

Computer Networks

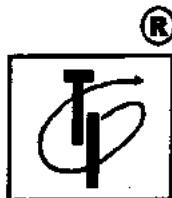
(Code : 310245)

Semester V – Computer Engineering
(Savitribai Phule Pune University)

**Strictly as per the New Credit System Syllabus (2015 Course)
Savitribai Phule Pune University w.e.f. academic year 2017-2018**

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



Tech-Max Publications, Pune
Innovation Throughout
Engineering Division

PO268A



Computer Networks (Code : 310245)

(Semester V, Computer Engineering, Savitribai Phule Pune University)

J. S. Katre.

Copyright © by Author. 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 : January 2001

First Edition as per New Syllabus : June 2017 (For Savitribai Phule Pune University)

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.

Printed at : Image Offset, Dugane Ind. Area Survey No. 28/25, Dhayari, Near Pari Company,
Pune - 41, Maharashtra State, India. E-mail : rahulshahimage@gmail.com

ISBN : 978-93-5224-597-0

Published by

Tech-Max Publications

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

Pune - 411009. Maharashtra State, India

Ph : 91-20-24225065, 91-20-24217965, **Fax** 020-24228978.

Email : info@techmaxbooks.com,

Website : www.techmaxbooks.com

(FID: TP407) [Book Code : PO268A]

Syllabus...

Savitribai Phule Pune University, Pune

Third Year of Computer Engineering (2015 Course)

(310245) Computer Networks

Teaching Scheme

Theory : 04 hrs/week

Examination Scheme

In-Sem(Paper) : 30 Marks

End-Sem (Paper) : 70 Marks

Course Objectives :

- To understand the fundamental concepts of networking standards, protocols and technologies.
- To learn different techniques for framing, error control, flow control and routing.
- To learn role of protocols at various layers in the protocol stacks.
- To learn network programming.
- To develop an understanding of modern network architectures from a design and performance perspective.

Course Outcomes :

On completion of the course, student will be able to :

- Analyze the requirements for a given organizational structure to select the most appropriate networking architecture, topologies, transmission mediums, and technologies.
- Demonstrate design issues, flow control and error control.
- Analyze data flow between TCP/IP model using Application, Transport and Network Layer Protocols.
- Illustrate applications of Computer Network capabilities, selection and usage for various sectors of user community.
- Illustrate Client-Server architectures and prototypes by the means of correct standards and technology.
- Demonstrate different routing and switching algorithms.

Course Contents

Unit I

Physical Layer :

Introduction of LAN ; MAN ; WAN ; PAN, Ad-hoc Network, Network Architectures : Client-Server ; Peer To Peer ; Distributed and SDN, OSI Model, TCP/IP Model, Topologies : Star and Hierarchical ; Design issues for Layers, Transmission Mediums : CAT5, 5e, 6, OFC and Radio Spectrum, Network Devices : Bridge, Switch, Router, Brouter and Access Point, Manchester and Differential Manchester Encodings ; IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS).
(Refer chapter 1)

Unit II

Logical Link Control :

Design Issues : Services to Network Layer, Framing, Error Control and Flow Control. Error Control: Parity Bits, Hamming Codes (11/12-bits) and CRC. Flow Control Protocols : Unrestricted Simplex, Stop and Wait, Sliding Window Protocol, WAN Connectivity : PPP and HDLC.
(Refer chapter 2)

Unit III

Medium Access Control :

Channel allocation : Static and Dynamic, Multiple Access Protocols : Pure and Slotted ALOHA, CSMA, WDMA, IEEE 802.3 Standards and Frame Formats, CSMA/CD, Binary Exponential Back-off algorithm, Fast Ethernet, Gigabit Ethernet, IEEE 802.11a/b/g/n and IEEE 802.15 and IEEE 802.16 Standards, Frame formats, CSMA/CA.

(Refer chapter 3)

Unit IV

Network Layer :

Switching techniques, IP Protocol, IPv4 and IPv6 addressing schemes, Subnetting, NAT, CIDR, ICMP, Routing Protocols: Distance Vector, Link State, Path Vector, Routing in Internet: RIP, OSPF, BGP, Congestion control and QoS, MPLS, Mobile IP, Routing in MANET : AODV, DSR.
(Refer chapters 4 and 5)

Unit V

Transport Layer :

Services, Berkley Sockets, Addressing, Connection establishment, Connection release, Flow control and buffering, Multiplexing, TCP, TCP Timer management, TCP Congestion Control, Real Time Transport protocol (RTP), Stream Control Transmission Protocol (SCTP), Quality of Service (QoS), Differentiated services, TCP and UDP for Wireless.
(Refer Chapter 6)

Unit VI

Application Layer :

Domain Name System (DNS), Hyper Text Transfer Protocol (HTTP), Email : SMTP, MIME, POP3, Webmail, FTP, TELNET, Dynamic Host Control Protocol (DHCP), Simple Network Management Protocol (SNMP).

(Refer chapter 7)

**Unit 1****Chapter 1 : Physical Layer** **1-1 to 1-87**

Syllabus : Introduction of LAN ; MAN ; WAN ; PAN, Ad-hoc Network, Network Architectures : Client-Server ; Peer To Peer; Distributed and SDN, OSI Model, TCP/IP Model, Topologies : Star and Hierarchical; Design issues for Layers, Transmission Mediums: CAT5, 5e, 6, OFC and Radio Spectrum, Network Devices : Bridge, Switch, Router, brouter and Access Point, Manchester and Differential Manchester Encodings ; IEEE802.11 : Frequency Hopping (FHSS) and Direct Sequence (DSSS).

1.1	Introduction.....	1-1
1.1.1	Introduction to Computer Networks.....	1-1
1.2	Network Topology Types.....	1-2
1.2.1	Bus Topology	1-2
1.2.2	Ring Topology	1-3
1.2.3	Star Topology	1-4
1.2.4	STAR LANs	1-4
1.2.5	Mesh Topology	1-5
1.2.6	Tree Topology	1-5
1.2.7	Logical Topology	1-6
1.2.8	Hybrid Topology	1-6
1.2.9	Hierarchical Topology.....	1-6
1.3	Uses of Computer Networks	1-7
1.3.1	Service Provided by the Network for Companies	1-7
1.3.2	Networks for People	1-8
1.4	Social Issues	1-8
1.5	Network Hardware.....	1-8
1.5.1	Types of Transmission Technology	1-9
1.6	Network Scale	1-9
1.7	Network Classification by their Geography	1-9
1.7.1	Local Area Networks (LAN).....	1-10
1.7.2	Ethernet.....	1-11
1.7.3	Metropolitan Area Network (MAN)	1-12
1.7.4	Wide Area Network (WAN).....	1-13
1.7.5	PAN (Personal Area Network)	1-14
1.7.6	CAN (Campus Area Network)	1-15
1.7.7	Wireless Networks.....	1-15
1.7.8	Internetworks.....	1-15
1.7.9	Comparison of LAN, WAN and MAN	1-16
1.8	Ad-Hoc Networks.....	1-16
1.9	Network Classification by their Component Role	1-16
1.10	Peer-to-Peer Networks.....	1-17
1.10.1	When to use Peer to Peer Networks ?	1-17
1.10.2	Advantages of Peer to Peer Networks	1-17
1.10.3	Disadvantages of Peer to Peer Networks	1-17

1.11	Client / Server Network (Server Based Network)	1-18
1.11.1	Communication in Client-Server Configuration	1-19
1.11.2	Advantages of Client-server Network	1-19
1.11.3	Disadvantages of Client-server Networks	1-19
1.11.4	Applications of Client-server Configuration	1-19
1.11.5	Comparison between Peer-to-Peer Network and Client-Server Network	1-19
1.11.6	Distributed Networking	1-20
1.11.7	SDN (Software Defined Network)	1-20
1.12	Layered Tasks	1-22
1.13	Network Software	1-23
1.13.1	Protocol Hierarchies (Layered Architecture)	1-23
1.13.2	Reasons for having Layered Protocols and its Benefits	1-23
1.13.3	Disadvantages of Layered Architecture	1-24
1.13.4	How does Data Transfer take Place ?	1-24
1.14	Network Architecture	1-24
1.14.1	Virtual Communication between Layers	1-24
1.15	Design Issues for the Layers	1-25
1.16	Interfaces and Services	1-27
1.16.1	Entities and Peer Entities	1-27
1.16.2	Service Provider and Service User	1-27
1.16.3	Service Access Points (SAPs)	1-27
1.16.4	Interface Data Unit (IDU)	1-28
1.16.5	Service Data Unit (SDU)	1-28
1.16.6	Protocol Data Unit (PDU)	1-28
1.17	Connection Oriented and Connectionless Services	1-28
1.17.1	Connection Oriented Service	1-28
1.17.2	Connectionless Service	1-28
1.17.3	Comparison of Connection Oriented and Connectionless Services	1-28
1.17.4	Quality of Service (QoS)	1-29
1.17.5	Service Primitives	1-29
1.18	Relationship of Services to Protocols	1-30
1.18.1	Service	1-30
1.18.2	Protocol	1-30
1.19	Reference Models	1-30
1.20	OSI Model	1-30
1.20.1	Functions of Different Layers	1-32
1.20.2	Exchange of Information using the OSI Model	1-33
1.20.3	Physical Layer	1-34
1.20.4	Data Link Layer	1-34
1.20.5	Network Layer	1-35
1.20.6	Transport Layer	1-37
1.20.7	The Session Layer	1-37
1.20.8	Presentation Layer	1-38
1.20.9	Application Layer	1-39
1.20.10	Merits of OSI Reference Model	1-40
1.20.11	Demerits of OSI Model	1-40



1.21	The TCP/IP Reference Model	1-40	1.28.2	Bands.....	1-56
1.21.1	Introduction to TCP/IP	1-40	1.28.3	EM Spectrum and Communication Applications	1-56
1.21.2	Overview of TCP/IP Architecture.....	1-40	1.28.4	Infrared Signals.....	1-57
1.21.3	Description of TCP/IP Model.....	1-41	1.28.5	Visible Light	1-57
1.21.4	Comparison of OSI and TCP/IP Models	1-42	1.29	Network Connecting Devices.....	1-57
1.22	Transmission Media	1-42	1.30	Hubs.....	1-58
1.22.1	Classification of Transmission Media.....	1-42	1.30.1	Passive Hubs.....	1-59
1.22.2	Comparison of Wired and Wireless Media.....	1-43	1.31	Repeaters	1-59
1.22.3	Types of Wired Media	1-44	1.31.1	Active Hubs.....	1-60
1.23	Twisted Pair Cables.....	1-44	1.31.2	Intelligent Hubs	1-60
1.23.1	Types of Twisted Pair Cables.....	1-44	1.32	Bridges.....	1-60
1.23.2	Categories (Cat) of UTP	1-45	1.32.1	Transparent Bridge.....	1-62
1.23.3	Category 3 and Category 5 (Cat 3 and Cat 5) UTP Cables	1-46	1.32.2	Source Routing Bridges.....	1-64
1.23.4	Category 6 (Cat 6) UTP.....	1-46	1.32.3	Comparison of Transparent and Source Routing Bridge	1-65
1.23.5	Category 7 (Cat 7) Shielded Screen Twisted Pair (SSTP).....	1-46	1.32.4	Remote Bridges	1-65
1.23.6	Applications of Twisted Pair Cables.....	1-46	1.32.5	Bridges Connecting Different LANs	1-65
1.23.7	Comparison of Twisted Pair Cables	1-46	1.33	Wireless Access Point (AP)	1-66
1.23.8	Connectors	1-47	1.33.1	Applications of AP	1-66
1.23.9	Connector for Twisted Pair Cable	1-47	1.33.2	Difference Between A.P. and Ad hoc Network	1-66
1.24	Co-axial Cables	1-47	1.33.3	Limitations of A.P.	1-66
1.24.1	Characteristics of a Co-Axial Cable	1-47	1.33.4	Security	1-66
1.24.2	Co-axial Cable Standards	1-48	1.33.5	Specialized APs	1-66
1.24.3	Applications of Co-axial Cables	1-48	1.34	Routers	1-66
1.24.4	Baseband Co-axial Cable	1-48	1.35	Gateways	1-68
1.24.5	Broadband Co-axial Cable	1-48	1.36	Switches	1-69
1.24.6	Connector for Co-axial Cable	1-48	1.36.1	Two Layer Switch	1-69
1.25	Optical Fiber Cables	1-49	1.36.2	Three Layer Switch	1-69
1.25.1	Light Sources for Fiber	1-49	1.36.3	Comparison of Hub and Switch	1-70
1.25.2	Principle of Light Propagation in a Fiber	1-49	1.36.4	Media Converters	1-70
1.25.3	Relation between Incident Angle and Emerging Angle	1-51	1.36.5	Comparison of Router and Bridge	1-70
1.25.4	Modes of Propagation	1-51	1.36.6	Comparison of Bridge, Switch and Hub	1-71
1.25.5	Single Mode Fibers	1-51	1.36.7	Comparison of Bridges, Routers and Switches	1-71
1.25.6	Multimode Fibers	1-51	1.36.8	Brouter	1-71
1.25.7	Characteristics of Optical Fiber Cables	1-53	1.37	Definition of Line Coding	1-72
1.26	Comparisons	1-53	1.37.1	Split Phase Manchester Format	1-72
1.26.1	Comparison of Step Index and Graded Index Fibers	1-53	1.37.2	Differential Manchester Code	1-72
1.26.2	Comparison of Single Mode and Multimode Fibers	1-53	1.38	Introduction to WLAN and WPAN	1-73
1.26.3	Comparison of Optical Fiber with Coaxial and Twisted Pair Cables	1-54	1.38.1	IEEE Standards	1-73
1.27	Advantages and Disadvantages of Fiber Optical Fibers	1-54	1.38.2	Wi-Fi	1-74
1.27.1	Advantages of Optical Fibers	1-54	1.39	Wireless LAN - 802.11 (Architecture)	1-74
1.27.2	Disadvantages of Optical Fibers	1-55	1.40	Components in a Typical IEEE 802.11 Network	1-76
1.27.3	Applications	1-55	1.40.1	Basic Service Set (BSS)	1-76
1.28	Unguided (Wireless) Media	1-55	1.40.2	Types of Stations in ESS	1-77
1.28.1	Unguided Media : Wireless	1-55	1.41	Introduction to Spread Spectrum	1-77
			1.41.1	How is the SS Signal Different from the Normal Signal ?	1-77



1.42	Applications of Spread Spectrum Modulation	1-78	2.4.3	Starting and Ending Character with Character Stuffing.....	2-4
1.43	Classification of the Spread Spectrum Modulation Techniques	1-78	2.4.4	Character Stuffing.....	2-4
1.44	Model of Spread Spectrum Digital Communication System.....	1-79	2.4.5	Starting and Ending Flags, with Bit Stuffing	2-5
1.45	Direct Sequence Spread Spectrum (DS-SS)	1-80	2.4.6	Physical Layer Coding Violations	2-6
1.45.1	Operation of the Encoder (Transmitter)	1-80	2.5	Error Control	2-7
1.45.2	Receiver	1-81	2.5.1	Function of a Timer.....	2-7
1.45.3	Features of DSSS	1-81	2.6	Error Detection and Correction.....	2-7
1.45.4	Applications of DS-SS System	1-81	2.6.1	Important Definitions Related to Codes.....	2-8
1.46	Frequency Hop Spread Spectrum (FH-SS) Signals.....	1-82	2.6.2	Error Detection.....	2-9
1.46.1	Types of Frequency Hopping	1-82	2.6.3	Error Detection Methods.....	2-10
1.47	Slow Frequency Hopping	1-82	2.6.4	Parity.....	2-10
1.47.1	Operation of the FH/MFSK Transmitter	1-83	2.6.5	Two Dimensional Parity Check.....	2-12
1.47.2	FH/MFSK Receiver	1-83	2.6.6	Cyclic Redundancy Check (CRC)	2-14
1.48	Fast Frequency Hopping	1-84	2.6.7	Error Correction	2-16
1.49	Advantages and Disadvantages of DS-SS and FH-SS Systems	1-85	2.6.8	Linear Block Codes.....	2-17
1.49.1	Advantages and Disadvantages of the DS-SS System	1-85	2.6.9	Hamming Codes.....	2-17
1.49.2	Advantages and Disadvantages of FH-SS System	1-86	2.6.10	Solved Examples	2-22
1.50	Comparisons	1-86	2.6.11	ARQ Technique	2-25
1.50.1	Comparison of Slow and Fast Frequency Hopping	1-86	2.7	Flow Control.....	2-26
1.50.2	Comparison of DS-SS and FH-SS Systems	1-86	2.8	Elementary Data Link Protocols	2-26
•	Review Questions.....	1-86	2.8.1	An Unrestricted Simplex Protocol	2-26
Unit 1					

Chapter 2 : Logical Link Control 2-1 to 2-50

Syllabus : Design Issues: Services to Network Layer, Framing, Error Control and Flow Control. Error Control: Parity Bits, Hamming Codes (11/12-bits) and CRC. Flow Control Protocols: Unrestricted Simplex, Stop and Wait, Sliding Window Protocol, WAN Connectivity : PPP and HDLC.

2.1	Introduction.....	2-1	2.1.1	Position of Data Link Layer	2-1
2.2	Data Link Layer Design Issues (Functions of Data Link Layer)	2-1	2.3	Services Provided to Network Layer	2-2
2.3	2.3.1 Types of Services Provided.....	2-3	2.3.2 Unacknowledged Connectionless Service.....	2-3	
2.3.3 Acknowledged Connectionless Service	2-3	2.3.4 Acknowledged Connection Oriented Service... 2-3			
2.4	Framing	2-3	2.4.1 Framing Methods	2-3	
2.4.2	Character Count.....	2-4	2.4.3 Starting and Ending Character with Character Stuffing.....	2-4	
			2.4.4 Character Stuffing.....	2-4	
			2.4.5 Starting and Ending Flags, with Bit Stuffing	2-5	
			2.4.6 Physical Layer Coding Violations	2-6	
			2.5	Error Control	2-7
			2.5.1	Function of a Timer.....	2-7
			2.6	Error Detection and Correction.....	2-7
			2.6.1	Important Definitions Related to Codes.....	2-8
			2.6.2	Error Detection.....	2-9
			2.6.3	Error Detection Methods.....	2-10
			2.6.4	Parity.....	2-10
			2.6.5	Two Dimensional Parity Check.....	2-12
			2.6.6	Cyclic Redundancy Check (CRC)	2-14
			2.6.7	Error Correction	2-16
			2.6.8	Linear Block Codes.....	2-17
			2.6.9	Hamming Codes.....	2-17
			2.6.10	Solved Examples	2-22
			2.6.11	ARQ Technique	2-25
2.7	Flow Control.....		2.7	Flow Control.....	2-26
2.8	Elementary Data Link Protocols		2.8.1	An Unrestricted Simplex Protocol	2-26
2.8.2	A Simplex Stop and Wait Protocol.....		2.8.2	A Simplex Stop and Wait Protocol.....	2-26
2.8.3	A Simplex Protocol for Noisy Channel.....		2.8.3	A Simplex Protocol for Noisy Channel.....	2-26
2.8.4	Piggybacking		2.8.4	Piggybacking	2-27
2.9	Sliding Window Protocols		2.9.1	A One Bit Sliding Window Protocol (Stop and Wait ARQ).....	2-31
2.9.2	A Protocol using GO Back n		2.9.2	A Protocol using GO Back n	2-34
2.9.3	Pipelining		2.9.3	Pipelining	2-36
2.9.4	Selective Repeat ARQ.....		2.9.4	Selective Repeat ARQ.....	2-37
2.9.5	Protocol Performance		2.9.5	Protocol Performance	2-38
2.10	Other Data Link Protocols.....		2.10	Other Data Link Protocols.....	2-39
2.11	High Level Data Link Control (HDLC) Protocol		2.11.1	Frame Structure in HDLC	2-40
2.11.2	Frame Types in HDLC		2.11.2	Frame Types in HDLC	2-41
2.11.3	Transparency in HDLC		2.11.3	Transparency in HDLC	2-42
2.11.4	Bit Stuffing		2.11.4	Bit Stuffing	2-42
2.12	Why is CRC in Data Link Protocols in Trailer and not in Header ?		2.12	Why is CRC in Data Link Protocols in Trailer and not in Header ?	2-43
2.13	Ways of Accessing the Internet		2.13	Ways of Accessing the Internet	2-43
2.14	SLIP-Serial Line IP.....		2.14	SLIP-Serial Line IP.....	2-44
2.15	Point-to-Point Protocol (PPP)		2.15.1	Services Provided by PPP	2-44
2.15.2	Frame Format of PPP		2.15.2	Frame Format of PPP	2-44
2.15.3	Transition Phases		2.15.3	Transition Phases	2-46
2.15.4	Multiplexing		2.15.4	Multiplexing	2-46
2.15.5	PPP Stack		2.15.5	PPP Stack	2-47
2.15.6	Link Control Protocol (LCP)		2.15.6	Link Control Protocol (LCP)	2-47



2.15.7	Authentication Protocols.....	2-48
2.15.8	Network Control Protocol (NCP)	2-48
2.15.9	Multilink PPP	2-48
2.15.10	Difference between SLIP and PPP	2-49
2.16	Solved Examples.....	2-49
	• Review Questions.....	2-50

Unit III**Chapter 3 : Medium Access Control** **3-1 to 3-62**

Syllabus : Channel allocation: Static and Dynamic, Multiple Access Protocols: Pure and Slotted ALOHA, CSMA, WDMA, IEEE 802.3, Standards and Frame Formats, CSMA/CD, Binary Exponential Back-off algorithm, Fast Ethernet, Gigabit Ethernet, IEEE 802.11a/b/g/n and IEEE 802.15 and IEEE 802.16 Standards, Frame formats, CSMA/CA.

3.8.3	Token Passing	3-16
3.9	Channelization	3-16
3.9.1	FDMA	3-17
3.9.2	TDMA	3-17
3.9.3	Code Division Multiple Access (CDMA)	3-17
3.9.4	Comparison of FDMA, TDMA and CDMA	3-18
3.10	Ethernet	3-18
3.10.1	Traditional Ethernet	3-19
3.10.2	Bridged Ethernet	3-19
3.10.3	Switched Ethernet	3-19
3.10.4	Full Duplex Ethernet	3-19
3.10.5	Fast Ethernet	3-19
3.10.6	Gigabit Ethernet	3-20
3.11	IEEE Standards	3-20
3.12	Traditional Ethernet (IEEE 802.3)	3-20
3.12.1	Traditional Ethernet Frame	3-20
3.12.2	Frame Length	3-21
3.12.3	Addressing	3-21
3.12.4	Types of Addresses	3-21
3.12.5	Physical Properties of Ethernet	3-22
3.12.6	Physical Layer Implementation of Traditional Ethernet	3-22
3.13	Changes in the Standards	3-23
3.14	Bridged Ethernet	3-23
3.15	Switched and Full Duplex Ethernet	3-24
3.15.1	Switched Ethernet	3-24
3.15.2	Full Duplex Ethernet	3-24
3.16	Fast Ethernet	3-25
3.16.1	Autonegotiation	3-25
3.16.2	Physical Layer Implementation	3-25
3.17	Gigabit Ethernet	3-26
3.17.1	Physical Layer Implementation	3-26
3.17.2	Ten Gigabit Ethernet	3-26
3.18	Token Bus : IEEE 802.4	3-27
3.19	Token Ring System [IEEE 802.5]	3-28
3.19.1	Comparison of Access Control Methods	3-30
3.19.2	Comparison of 802.3, 802.4 and 802.5 IEEE Standard	3-30
3.19.3	Why can't Ethernet and Token Ring be used in a WAN ?	3-31
3.20	Introduction to WLAN and WPAN	3-34
3.20.1	Wi-Fi	3-34
3.21	Infrastructure and Ad-Hoc Networks	3-34
3.21.1	The ISM Band	3-34
3.22	Fundamentals of WLANs	3-35
3.22.1	Wireless LAN Configuration	3-35
3.22.2	Applications of Wireless LAN	3-35
3.22.3	Wireless LAN - 802.11 (Architecture)	3-35
3.23	Technical Issues	3-37



3.23.1 Difference between Wireless and Wired Transmission.....	3-37	3.40.2 Bluetooth Security.....	3-55
3.23.2 Use of WLANs.....	3-37	3.40.3 Security Limitations in Bluetooth	3-55
3.24 Design Goals.....	3-37	3.40.4 Logical Link Control and Adaptation Protocol (L2CAP).....	3-55
3.25 Network Architecture	3-38	3.40.5 Host Controller Interface.....	3-55
3.25.1 Infrastructure Networks	3-38	3.41 Middleware Protocol Group	3-55
3.25.2 Ad-hoc LANs	3-38	3.42 Bluetooth Profiles.....	3-56
3.26 Components in a Typical IEEE 802.11 Network	3-39	3.42.1 Limitations.....	3-57
3.26.1 Basic Service Set (BSS).....	3-39	3.42.2 Bluetooth Advantages.....	3-57
3.26.2 Types of Stations in ESS.....	3-40	3.42.3 Comparison of Bluetooth and WLAN IEEE 802.11x.....	3-57
3.27 Services Offered by a Typical IEEE 802.11 Network	3-40	3.43 Applications of Bluetooth	3-57
3.27.1 AP Services.....	3-40	3.44 IEEE 802.16 (WMANs)	3-58
3.27.2 STA Services.....	3-40	3.44.1 The 802.16 Protocol Stack	3-59
3.28 IEEE 802.11 Standard.....	3-41	3.44.2 802.16 Frame Format.....	3-60
3.29 Physical Layer	3-41	3.44.3 Difference Between IEEE 802.11 and IEEE 802.16.....	3-60
3.29.1 802.11 Frame Format.....	3-42	3.44.4 Physical Layer (IEEE 802.16).....	3-60
3.29.2 IEEE 802.11 FHSS.....	3-42	3.44.5 Data Link Layer.....	3-61
3.29.3 IEEE 802.11 DSSS	3-43	• Review Questions.....	3-61
3.29.4 IEEE 802.11 a OFDM.....	3-43		
3.29.5 IEEE 802.11 b HR-DSSS.....	3-43		
3.29.6 IEEE 802.11g OFDM.....	3-43		
3.30 Basic MAC Layer Mechanisms	3-44		
3.30.1 Distributed Foundation Wireless Medium Access Control (DFWMAC).....	3-44		
3.30.2 Inter-Frame Spacing (IFS).....	3-44		
3.30.3 DCF and PCF in 802.11	3-45		
3.30.4 CSMA/CA Mechanism.....	3-45		
3.30.5 The Medium Access Mechanism	3-46		
3.30.6 RTS-CTS Mechanism	3-46		
3.31 Problems in Wireless LAN.....	3-47		
3.32 Comparison of Ethernet and Wireless Network	3-47		
3.33 Wireless LAN Protocols.....	3-48		
3.34 Advantages of WLAN	3-49		
3.34.1 Limitations of WLAN.....	3-49		
3.35 Bluetooth (WPAN)	3-49		
3.35.1 Applications of Bluetooth Technology	3-49		
3.35.2 Bluetooth Devices	3-49		
3.36 Bluetooth Specifications	3-50		
3.37 Transport Protocol Group.....	3-50		
3.37.1 Radio (Physical Layer)	3-50		
3.37.2 Physical Links in Bluetooth.....	3-50		
3.37.3 Baseband Layer	3-51		
3.37.4 TDMA	3-51		
3.37.5 Frame Format in Baseband Layer (Bluetooth Frame Format).....	3-52		
3.38 Piconets (Bluetooth Architecture)	3-53		
3.39 Scatternets (Bluetooth Architecture) and Issues.....	3-53		
3.40 Link Manager Protocol (LMP).....	3-54		
3.40.1 Power Management	3-54		

Unit - IV**Chapter 4 : Network Layer 4-1 to 4-47**

Syllabus : Switching techniques, Routing Protocols: Distance Vector, Link State, Path Vector, Congestion control.

4.1 Network Layer.....	4-1
4.1.1 Position of Network Layer.....	4-1
4.1.2 Network Layer Duties	4-1
4.2 Network Layer Design Issues	4-2
4.2.1 Store and Forward Packet Switching	4-2
4.2.2 Services Provided to the Transport Layer	4-3
4.2.3 Implementation of Connectionless Service	4-3
4.2.4 Implementation of Connection-Oriented Service	4-5
4.2.5 Internal Organization of the Network Layer	4-5
4.2.6 Comparison of Virtual Circuit and Datagram Subnets.....	4-5
4.3 Delivery	4-6
4.3.1 Direct Delivery	4-6
4.3.2 Indirect Delivery	4-6
4.4 Forwarding	4-7
4.4.1 Forwarding Techniques	4-7
4.4.2 Next Hop Method Versus Route Method	4-7
4.4.3 Network Specific Method Versus Host Specific Method	4-7
4.4.4 Default Method	4-8
4.4.5 Forwarding Process	4-8
4.5 Routers	4-9



4.5.1	Routing Tables	4-10	4.17.3	Link State Routing	4-34
4.6	Unicast Routing	4-10	4.17.4	Comparison of Link State Routing and Distance Vector Routing	4-34
4.6.1	Metric.....	4-11	4.18	Hierarchical Routing	4-35
4.6.2	Interior and Exterior Routing	4-11	4.19	Intra and Interdomain Routing	4-36
4.7	Broadcast Routing.....	4-11	4.20	Internetworking	4-37
4.8	Introduction to Switching	4-11	4.20.1	Why Internetworking ?	4-37
4.9	Switching Methods	4-12	4.20.2	The Problems in Internetworking	4-37
4.10	Circuit Switching Networks.....	4-12	4.20.3	Dealing with Incompatibility Issue	4-38
4.10.1	Three Phases	4-13	4.21	Fragmentation	4-39
4.10.2	Efficiency	4-13	4.21.1	Strategy - 1 for Fragmentation (Transparent Strategy)	4-40
4.10.3	Delay	4-14	4.21.2	Strategy - 2 for Fragmentation (Non-transparent Strategy)	4-40
4.10.4	Advantages	4-15	4.22	The Network Layer in the Internet	4-41
4.10.5	Disadvantages.....	4-15	4.23	Congestion	4-42
4.10.6	Circuit Switched Technology in Telephone Networks	4-15	4.23.1	Need of Congestion Control	4-42
4.11	Telegraph Networks and Message Switching	4-15	4.23.2	Causes of Congestion	4-42
4.11.1	Advantages	4-15	4.23.3	Difference between Congestion Control and Flow Control	4-43
4.11.2	Disadvantages.....	4-15	4.23.4	Principle of Congestion Control	4-43
4.12	Packet Switching.....	4-16	4.23.5	Congestion Prevention Policies	4-44
4.12.1	Datagram Packet Switching	4-16	4.23.6	Congestion Control in Virtual Circuit Subnets.....	4-46
4.12.2	Routing Table.....	4-17	4.24	Solved University Examples	4-47
4.12.3	Efficiency	4-17	•	Review Questions	4-46
4.12.4	Delay	4-17	4.25	University Questions and Answers	4-47
4.12.5	Advantages of Packet Switching.....	4-18		Unit IV	
4.12.6	Disadvantages of Packet Switching.....	4-18			
4.12.7	Datagram Networks in Internet	4-18			
4.13	Virtual Circuit Packet Switching.....	4-18			
4.13.1	Addressing	4-19			
4.13.2	Three Phases of Communication.....	4-19			
4.13.3	Efficiency	4-22			
4.13.4	Delay	4-22			
4.13.5	Circuit Switched Technology in WANs.....	4-23			
4.13.6	Advantages of Virtual Circuit Packet Switching	4-23			
4.13.7	Disadvantages of Virtual Circuit Packet Switching.....	4-23			
4.13.8	Comparison of Datagram and Virtual Circuits	4-23			
4.14	Multicast Routing.....	4-24			
4.15	Routing Algorithms	4-24			
4.15.1	Desired Properties of a Routing Algorithm....	4-24			
4.15.2	Types of Routing Algorithms	4-24			
4.15.3	Optimality Principle.....	4-25			
4.16	Static (Non adaptive) Algorithms	4-25			
4.16.1	Shortest Path Routing	4-25			
4.16.2	Dijkstra's Algorithm.....	4-25			
4.16.3	Flooding.....	4-29			
4.17	Dynamic Routing Algorithms	4-29			
4.17.1	Distance Vector Routing Algorithm	4-29			
4.17.2	Count to Infinity Problem	4-32			

Chapter 5 : Network Layer Protocols 5-1 to 5-59

Syllabus : IP Protocol, IPv4 and IPv6 addressing schemes, Subnetting, NAT, CIDR, ICMP, Routing in Internet : RIP, OSPF, BGP, MPLS, Mobile IP, Routing in MANET : AODV, DSR.

5.1	Introduction	5-1
5.1.1	Why IP Address ?	5-1
5.1.2	Logical Addresses (IP Addresses)	5-2
5.2	ARP (Address Resolution Protocol).....	5-2
5.2.1	Mapping of IP Address into a MAC Address	5-3
5.2.2	ARP Operation.....	5-3
5.2.3	ARP Cache Memory	5-4
5.2.4	ARP Packet Format	5-4
5.2.5	Encapsulation	5-4
5.2.6	Operation of ARP on Internet	5-4
5.2.7	Four Different Cases.....	5-5
5.2.8	Proxy ARP	5-5
5.3	Internet Protocol (IP).....	5-5
5.3.1	Datagram	5-6
5.3.2	Structure of IP Frame Header.....	5-6



5.3.3	Services Provided	5-7	5.10.4	RIP Operation	5-30
5.3.4	IPv4 Addresses	5-7	5.10.5	RIP Message Format	5-30
5.3.5	Network Address	5-9	5.10.6	Disadvantages of RIPv1	5-31
5.3.6	Special IP Addresses	5-10	5.10.7	RIP Version 2	5-31
5.3.7	Address Masks (Default Masks)	5-11	5.11	OSPF Routing Protocol	5-32
5.3.8	Limitations of IPv4	5-11	5.11.1	Features of OSPF	5-33
5.3.9	Subnetting in IP	5-12	5.11.2	Metric	5-34
5.3.10	Subnet Mask	5-12	5.11.3	Types of Links	5-34
5.3.11	Classless Addressing	5-13	5.11.4	Link State Advertisements (LSAs)	5-35
5.3.12	Supernetting	5-13	5.11.5	OSPF Packet Types	5-35
5.3.13	Who Decides the IP Addresses ?	5-13	5.11.6	Comparison between RIP and OSPF	5-36
5.3.14	Registered and Unregistered Addresses	5-13	5.12	Border Gateway Protocol	5-37
5.4	IPv6	5-14	5.12.1	Path Vector Routing	5-37
5.4.1	IPv6 Addresses	5-14	5.12.2	Path Vector Messages	5-37
5.4.2	Abbreviation	5-15	5.12.3	Loop Prevention	5-38
5.4.3	CIDR Notation	5-15	5.12.4	Path Attributes	5-38
5.4.4	Categories of Address	5-15	5.12.5	Types of Messages	5-38
5.4.5	IPv6 Packet Format	5-16	5.12.6	BGP Operation	5-39
5.4.6	NAT – Network Address Translation	5-16	5.12.7	BGP Routing	5-40
5.5	Extension Headers	5-17	5.12.8	How does BGP Solve the Count to Infinity Problem ?	5-41
5.5.1	Fragmentation	5-18	5.13	Solved Examples	5-41
5.5.2	Authentication and Privacy	5-18	5.14	MPLS (Multi-Protocol Label Switching)	5-49
5.5.3	Migrating to IPv6 (Compatibility to IPv4)	5-18	5.14.1	MPLS Header	5-49
5.5.4	Comparison between IPv4 and IPv6	5-18	5.14.2	How does MPLS Work ?	5-49
5.6	Mobile IP	5-19	5.14.3	Forwarding Table	5-50
5.6.1	Routing for Mobile Hosts	5-19	5.15	Routing in MANET	5-50
5.6.2	Mobile IP	5-20	5.15.1	Problems with Routing in Mobile Ad-hoc Networks (MANET)	5-50
5.7	Mapping Physical Address to Logical Address	5-20	5.15.2	Characteristics of the Routing Protocol for MANET	5-50
5.7.1	The Reverse Address Resolution (RARP) Protocol	5-20	5.15.3	Classification of Routing Protocols in MANETs	5-51
5.7.2	Solved Examples	5-21	5.16	Table Driven Routing Protocols (Proactive)	5-51
5.8	ICMP (Internet Control Message Protocol)	5-26	5.16.1	Destination Sequenced Distance Vector Routing Protocol (DSDV)	5-51
5.8.1	Types of Messages	5-27	5.17	On-demand Routing Protocol (Reactive)	5-53
5.8.2	Query	5-28	5.17.1	Dynamic Source Routing Protocol (DSR)	5-54
5.8.3	Different Types of Messages in ICMPv6	5-28			
5.9	Unicast Routing Protocols	5-29			
5.10	RIP (Routing Information Protocol)	5-29			
5.10.1	RIP Updating Algorithm	5-30			
5.10.2	Initializing the Routing Table	5-30			
5.10.3	Updating the Routing Table	5-30			

5.17.2 Ad-hoc on Demand Distance Vector Routing Protocol (AODV).....	5-56
• Review Questions.....	5-58
5.18 University Questions and Answers.....	5-58

Unit V

Chapter 6 : Transport Layer 6-1 to 6-61

Syllabus : Services, Berkley Sockets, Addressing, Connection establishment, Connection release, Flow control and buffering, Multiplexing, TCP, TCP Timer management, TCP Congestion Control, Real Time Transport protocol (RTP), Stream Control Transmission Protocol (SCTP), Quality of Service (QoS), Differentiated services, TCP and UDP for Wireless.

6.1 Introduction.....	6-1
6.2 Transport Layer Duties and Functionalities.....	6-1
6.2.1 Process-to-Process Delivery.....	6-2
6.2.2 Client Server Paradigm	6-3
6.2.3 Addressing in Transport Layer.....	6-3
6.2.4 Multiplexing and Demultiplexing.....	6-4
6.2.5 Connection Oriented Versus Connectionless Service	6-4
6.2.6 Reliability at Transport Layer Versus Reliability at DLL.....	6-5
6.3 The Transport Layer Services.....	6-6
6.3.1 Quality of Service (QoS).....	6-7
6.4 Transport Service Primitives	6-7
6.4.1 Nesting of TPDU's, Packets and Frames	6-8
6.5 Sockets and Their Programming.....	6-9
6.5.1 Socket Types.....	6-9
6.5.2 Berkeley Sockets.....	6-9
6.5.3 Steps Followed for Socket Programming.....	6-10
6.5.4 Connectionless Iterative Server (Datagram Socket)	6-10
6.5.5 Connection Oriented Concurrent Server (Stream Socket)	6-11
6.6 Elements of Transport Protocols.....	6-12
6.7 The Internet Transport Protocols (TCP and UDP).....	6-12
6.8 User Datagram Protocol (UDP).....	6-13
6.8.1 Well Known Ports for UDP	6-13

6.8.2 User Datagram	6-13
6.8.3 UDP Pseudo Header	6-14
6.8.4 UDP Operation	6-15
6.8.5 Applications of UDP	6-16
6.9 Transmission Control Protocol (TCP).....	6-16
6.9.1 Relationship Between TCP and IP	6-16
6.9.2 Ports and Sockets.....	6-17
6.10 Features of TCP.....	6-18
6.11 TCP Services.....	6-18
6.12 TCP Features.....	6-20
6.13 The TCP Protocol	6-21
6.13.1 TCP Segment	6-21
6.13.2 The TCP Segment Header	6-21
6.13.3 Checksum.....	6-23
6.14 TCP Connections.....	6-23
6.14.1 TCP Connection Establishment.....	6-23
6.14.2 Connection Termination Protocol [Connection Release]	6-23
6.14.3 TCP Connection Management	6-24
6.14.4 TCP Connection Release	6-24
6.15 TCP State Diagram.....	6-25
6.16 TCP Sliding Window (TCP Transmission Policy)	6-26
6.16.1 Nagle's Algorithm.....	6-27
6.16.2 Silly Window Syndrome	6-27
6.17 TCP Congestion Control	6-28
6.17.1 Slow Start Algorithm	6-29
6.17.2 Internet Congestion Control Algorithm	6-30
6.17.3 Congestion Avoidance (Additive Increase).....	6-31
6.17.4 Fast Retransmission	6-31
6.17.5 TCP Tahoe	6-31
6.17.6 Fast Recovery	6-32
6.18 TCP Timer Management	6-33
6.18.1 Jacobson's Algorithm.....	6-33
6.18.2 Karn's Algorithm	6-34
6.18.3 Other Timers in TCP	6-34
6.18.4 Comparison of UDP and TCP	6-34
6.19 Socket Programming with TCP.....	6-35
6.19.1 Socket Programming with TCP	6-35
6.19.2 Socket Programming with UDP	6-36
6.20 Protocols for Real Time Interactive Applications	6-37



6.20.1 RTP [Real Time Protocol].....	6-37	7.1 Application Layer	7-1
6.20.2 RTCP [RTP Control Protocol].....	6-38	7.1.1 Client Server Model	7-1
6.20.3 RTCP Packets.....	6-39	7.1.2 Addressing.....	7-3
6.21 Stream Control Transmission Protocol (SCTP).....	6-40	7.1.3 Applications	7-3
6.21.1 Introduction.....	6-40	7.1.4 Socket.....	7-3
6.21.2 Stream Control Transmission Protocol Message Format	6-40	7.2 Domain Name System (DNS).....	7-3
6.21.3 SCTP Compared to TCP.....	6-42	7.2.1 How does DNS Work ?.....	7-4
6.21.4 Message-Based Multi-Streaming.....	6-43	7.2.2 Name Space	7-4
6.21.5 SCTP Multihoming	6-45	7.2.3 Flat Name Space	7-4
6.22 Quality of Service (QoS).....	6-46	7.2.4 Hierarchical Name Space	7-4
6.22.1 Flow Characteristics.....	6-46	7.3 Domain Name Space.....	7-4
6.22.2 Techniques for Achieving Good QoS.....	6-46	7.4 Distribution of Name Space.....	7-6
6.22.3 Traffic Shaping	6-47	7.4.1 Hierarchy of Name Servers	7-6
6.22.4 Leaky Bucket Algorithm.....	6-47	7.5 DNS in the Internet	7-8
6.22.5 Token Bucket Algorithm	6-48	7.5.1 Generic Domains	7-8
6.22.6 Combination of Token Bucket and Leaky Bucket.....	6-49	7.5.2 Country Domain.....	7-8
6.22.7 Resource Reservation.....	6-49	7.5.3 Inverse Domain.....	7-8
6.23 Scheduling and Policing	6-49	7.6 Name Address Resolution	7-8
6.23.1 Link Scheduling Discipline	6-50	7.6.1 Recursive Resolution.....	7-9
6.24 Policing	6-51	7.6.2 Iterative Resolution	7-9
6.25 Integrated Services and Differentiated Services	6-53	7.6.3 The DNS Message Format	7-9
6.25.1 Intserv.....	6-53	7.6.4 Caching	7-10
6.25.2 Classes of Service.....	6-54	7.7 Electronic Mail	7-10
6.25.3 Differentiated Services (Diffserv)	6-55	7.7.1 E-mail Architecture and Services	7-10
6.26 RSVP	6-56	7.7.2 Message Formats	7-11
6.27 Wireless TCP and UDP	6-57	7.8 MIME – Multipurpose Internet Mail Extensions	7-12
6.27.1 Solution (Indirect TCP).....	6-57	7.8.1 Principle of MIME	7-12
6.27.2 Alternative Solution	6-58	7.9 Message Transfer Agent : SMTP	7-14
6.27.3 Wireless UDP	6-58	7.9.1 Commands and Responses	7-14
6.27.4 RPC (Remote Procedure Call).....	6-58	7.9.2 SMTP (Simple Mail Transfer Protocol) Operation	7-15
6.28 Solved Examples	6-59	7.9.3 Components of E-mail System	7-15
• Review Questions.....	6-60	7.9.4 SMTP Commands	7-16
		7.9.5 SMTP Operation	7-16
		7.10 E-mail Gateways	7-16
		7.11 Message Access Agent : POP and IMAP	7-17
		7.11.1 POP 3	7-17
		7.11.2 IMAP 4	7-18

UNIT VI**Chapter 7 : Application Layer 7-1 to 7-50**

Syllabus : Domain Name System (DNS), Hyper Text Transfer Protocol (HTTP), Email: SMTP, MIME, POP3, Webmail, FTP, TELNET, Dynamic Host Control Protocol (DHCP), Simple Network Management Protocol (SNMP).



7.11.3 Comparison of IMAP and POP 3	7-18	7.18.4 HTTP Messages.....	7-30
7.12 Web Based Mail	7-18	7.18.5 Request Message.....	7-30
7.13 File Transfer Protocol (FTP).....	7-18	7.18.6 Methods (Request Type)	7-31
7.13.1 Communication in FTP.....	7-19	7.18.7 Response Message	7-31
7.13.2 File Types.....	7-20	7.18.8 Headers	7-31
7.13.3 Data Structure	7-20	7.18.9 Comparison of HTTP and SMTP	7-32
7.13.4 Transmission Mode.....	7-20	7.19 Proxy Server	7-32
7.13.5 File Transfer	7-21	7.20 Performance Enhancement.....	7-33
7.13.6 FTP Commands.....	7-21	7.20.1 Content Delivery Networks	7-33
7.13.7 Anonymous FTP.....	7-21	7.20.2 DNS Records (Resource Records)	7-33
7.14 TFTP.....	7-21	7.21 P2P File Sharing	7-34
7.14.1 Comparison of FTP and TFTP	7-22	7.22 Remote Login : TELNET and SSH	7-34
7.15 World Wide Web (WWW).....	7-22	7.22.1 TELNET	7-34
7.15.1 Web from the Users Side	7-22	7.22.2 Network Virtual Terminal (NVT).....	7-36
7.15.2 Web from the Servers Side	7-24	7.22.3 Security Problems of TELNET	7-36
7.15.3 WWW Architecture	7-24	7.22.4 Secure Shell (SSH).....	7-36
7.16 Browser (Client).....	7-25	7.22.5 Port Forwarding	7-37
7.16.1 Server.....	7-25	7.22.6 SSH Packet Format	7-37
7.16.2 Uniform Resource Locator (URL).....	7-25	7.23 Host Configuration : DHCP	7-37
7.16.3 Cookies : User-Server Interaction	7-25	7.23.1 Previously used Protocols	7-37
7.17 Web Documents	7-26	7.23.2 Need for Dynamic Configuration	7-37
7.17.1 Static Documents	7-26	7.23.3 DHCP	7-38
7.17.2 HTML (Hypertext Markup Language).....	7-26	7.23.4 Advantages of DHCP	7-39
7.17.3 Dynamic Document	7-26	7.23.5 Components of DHCP	7-39
7.17.4 Common Gateway Interface (CGI).....	7-27	7.23.6 DHCP Operation	7-39
7.17.5 Active Documents	7-27	7.23.7 DHCP Operation on Different Networks	7-40
7.18 HTTP (Hypertext Transfer Protocol).....	7-28	7.23.8 Error Control	7-40
7.18.1 Principle of HTTP Operation	7-28	7.23.9 Optimizations In DHCP	7-40
7.18.2 The Web and HTTP	7-28		
7.18.3 Non-persistent and Persistent Connection....	7-29		



7.23.10 DHCP Message Format	7-41	7.25 Simple Network Management Protocol (SNMP)	7-47
7.24 Configuration	7-42	7.25.1 Concept	7-47
7.24.1 Static Address Allocation.....	7-42	7.25.2 Managers and Agents.....	7-47
7.24.2 Dynamic Address Allocation	7-42	7.25.3 Management Components	7-48
7.24.3 Transition States	7-42	7.25.4 Structure of Management Information (SMI) ..	7-48
7.24.3.1 Address Acquisition States.....	7-42	7.25.5 Management Information Base (MIB).....	7-49
7.24.3.2 Early Lease Termination	7-43	7.25.6 Simple Network Management Protocol (SNMP)	7-49
7.24.3.3 Lease Renewal States	7-43	• Review Questions	7-50
7.24.4 DHCP Architecture	7-44	7.26 University Questions and Answers	7-50
7.24.5 The DHCP Client.....	7-45		
7.24.6 DHCP Server.....	7-46		
7.24.7 BOOTP Relay Agents	7-47		





Unit I

Physical Layer

Syllabus :

Introduction of LAN ; MAN ; WAN ; PAN, Ad-hoc Network, Network Architectures : Client-Server ; Peer To Peer; Distributed and SDN, OSI Model, TCP/IP Model, Topologies : Star and Hierarchical; Design issues for Layers, Transmission Mediums: CAT5, 5e, 6, OFC and Radio Spectrum, Network Devices : Bridge, Switch, Router, brouter and Access Point, Manchester and Differential Manchester Encodings ; IEEE802.11 : Frequency Hopping (FHSS) and Direct Sequence (DSSS).

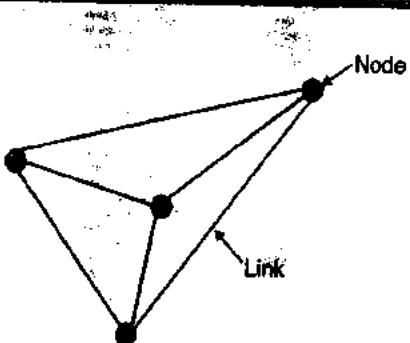
1.1 Introduction :

Network :

- Network is a broad term similar to "system". Network is a communication system which supports many users.
- In relation with the computers we can say that a "computer network" is a system which allows communication among the computers connected in the network.
- There are various ways of interconnecting the computers.

Protocol :

- For successful communication to occur, it is not enough for the "sender" to simply transmit the message and "assume" that the "receiver" will receive it properly.
- There are certain rules that must be followed to ensure proper communication.
- 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.
- **Node :** Each station in a communication network is called as a node. The nodes are connected in different way to each other to form a network.
- One of such networks is shown in Fig. 1.1.1.
- Many other forms of interconnections are possible. The most familiar network is the telephone system. It is the largest and most sophisticated network of all.



(G-13) Fig. 1.1.1 : A simple communication network

1.1.1 Introduction to Computer Networks :

- During 20th century the most important technology has been the information gathering, its processing and distribution.
- The computers and communication fields have been merged together and their merger has had a deep impact on the manner in which computer systems are organized.
- The old model in which a single computer used to serve all the computational needs of an organization has been replaced by a new one in which a large number of separate but interconnected computers do the job.
- Such systems are called as computer networks.
- Two computers are said to be interconnected if they interchange information. The connection between the separate computers can be done via a copper wire, fiber optics, microwaves or communication satellite.

Distributed system :

- A system with one control unit (master computer) and many slaves, or a large computer with remote printers and terminals is not called a computer network, it is called a **Distributed System**.
- In distributed system the existence of multiple autonomous computers is not visible to the user.
- With a computer network, the user has to consciously log onto a machine, submit jobs



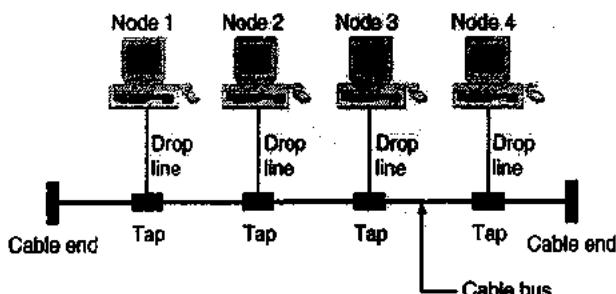
- remotely, move files around etc. in short handle all the network management personally.
- With a distributed system nothing of this needs to be done explicitly, it all happens automatically because the system takes care of it without the users knowledge.
- Basically a distributed system is a software system built on top of a network. The software gives it a high degree of cohesiveness, (homogeneity) and transparency to the system.

1.2 Network Topology Types :

- The word physical network topology is used to explain the manner in which a network is physically 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.
- The five basic network topologies are as shown in Fig. 1.2.1.
- These topologies can be classified into two types :
 - Peer to peer
 - 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.

1.2.1 Bus Topology :

- The bus topology is usually used when a network under consideration is small, simple or temporary as shown in Fig. 1.2.2.



(G-15) Fig. 1.2.2 : Bus topology

- On a typical bus network a simple cable is used without additional electronics to amplify the signal

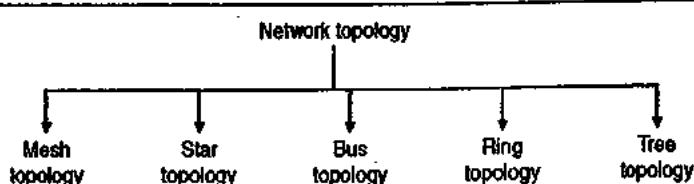
or pass it along from computer to computer. Therefore the bus is a passive topology.

- 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 impedance.
- The terminators absorb the electrical energy and avoid reflections.

Characteristics of the bus topology :

Following are some of the important characteristics of the bus topology :

- This is a multipoint configuration. There are more than two devices connected to the medium and they are capable of transmitting on the medium. Hence the Medium Access Control (MAC) is essential for the bus topology.
- The signal strength of the transmitted signal should be adequately high so as to meet the minimum signal strength requirements of the receiver.



(G-14) Fig. 1.2.1 : Classification of network topology

3. Adequate Signal to Noise Ratio (SNR) should be maintained for better quality reception.
4. The signal should not be too strong. This is necessary to avoid the overloading of transmitter and hence the possibility of signal distortion.
5. This is called as signal balancing which is not an easy task at all. Specially the signal balancing becomes increasingly difficult with increase in the number of stations.

Transmission media for bus LANs :

We can use the following transmission media for the bus LANs :

1. Twisted pair
2. Baseband co-axial cable
3. Broadband co-axial cable
4. Optical fiber

Advantages of bus topology :

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

Disadvantages of bus topology :

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

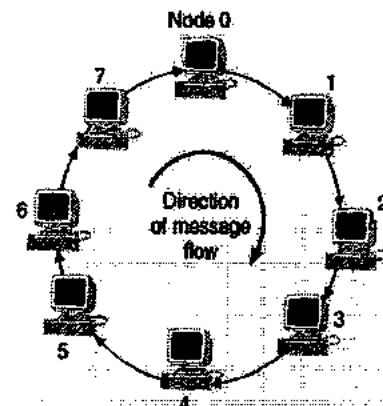
Ethernet 10 base 2, also known as thinnet, is an inexpensive network based on the bus topology.

A bus network behaves differently if it is not terminated or improperly terminated.

Token-bus networks are defined by the IEEE 802.4 standard.

1.2.2 Ring Topology :

- In a ring topology, each computer is connected to the next computer, with the last one connected to the first as shown in Fig. 1.2.3.
- 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.

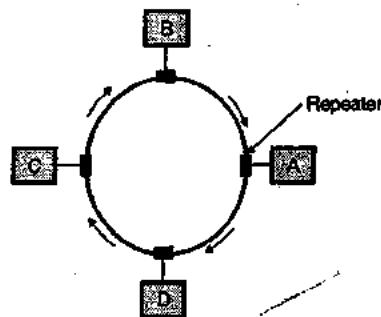


(G-16) Fig. 1.2.3 : Ring topology

- The messages flow around the ring in one direction. There is no termination because there is no end to the ring.
- 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 in sequence 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 originator indicating that the message has been received.
- The sending computer then creates another token and places it on the network, allowing another station to capture the token and begin transmitting.
- 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.

Characteristics of ring LANs :

- The basic ring LAN is shown in Fig. 1.2.4, which shows that along with the nodes A, B, C, D equal number of repeaters are used and that the transmission is unidirectional.



(G-17) Fig. 1.2.4 : Ring topology



- The data is travels in a sequential manner around the ring. Each repeater will receive regenerate and retransmit this data bit.

Problems faced in the ring topology :

- If any link breaks or if any repeater fails then the entire network will be disabled.
 - To install a new repeater for supporting a new device, it is necessary to have the identification of two nearby, topologically adjacent repeaters.
 - It is necessary to take preventive measures to deal with the time jitter.
 - Due to the closed nature of the ring topology it is necessary to remove the circulating packets.
- These problems except for the last one can be rectified by refinements of the ring topology.

Advantages of ring topology :

- Every computer gets an equal access to the token.
- There are no standing waves produced.

Disadvantages of ring topology :

- Failure of one computer on the ring can affect the whole network.
- It is difficult to trouble shoot the ring.
- Adding or removing the computers disturbs the network activity.

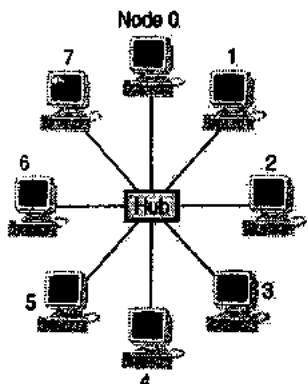
Note: Token ring networks are defined by the IEEE 802.5 standard.

Fibre Distributed Data Interface (FDDI) is a fast fibre-optic network based on the ring topology.

1.2.3 Star Topology :

In a star topology all the computers are connected via cables to a central location where they are all connected by a device called a hub as shown in Fig. 1.2.5. 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.

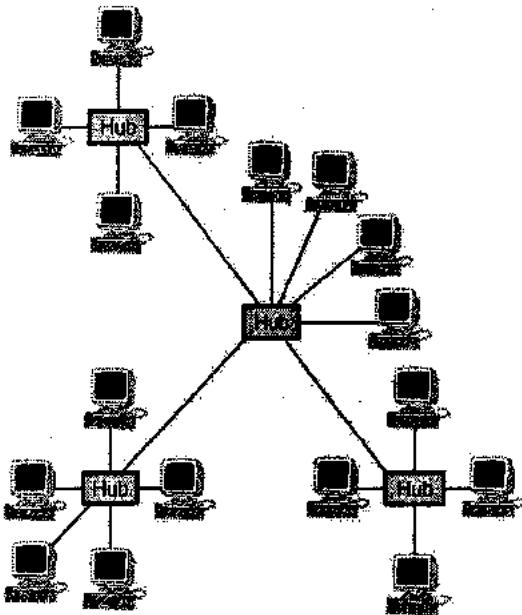


(G-18) Fig. 1.2.5 : Star topology

- Each computer on a star network communicates with a central hub. The hub then resends the message to

all the computers in a broadcast star network. It will resend the message only to the destination computer in a switched star network.

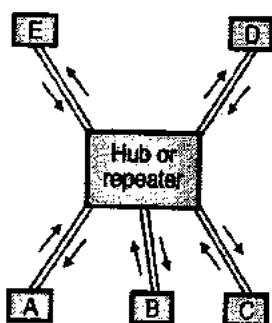
- The hub in a broadcast star network can be active or passive. An active hub generates the electrical signal and sends it to all the computers connected to it.
- This type of hub is usually called a multiport repeater. Active hubs require external power supply.
- A passive hub is a wiring panel or punch 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.
- A star network can be expanded by placing another star hub as shown in Fig. 1.2.6.
- This arrangement allows several more computers or hubs to be connected to that hub. This creates a hybrid star network.



(G-19) Fig. 1.2.6 : Expansion of star topology

1.2.4 STAR LANs :

- In the star type LANs, the Unshielded Twisted Pair (UTP) is used as the transmission medium.
- This is because the unshielded twisted pair is a telephone wire which is available in each and every office building. The other advantages of using twisted wires are as follows :
 - So no additional installation cost is required for the installation of LAN.
 - Since the telephone wires cover the entire building it is possible to spread the network in every part of each building.



(G-20) Fig. 1.2.7 : Single level star topology

- The basic star topology is as shown in Fig. 1.2.7. This is called as a single level star topology.
- As shown in Fig. 1.2.7, the central element of the star topology is an active element called hub or repeater.
- Each station (A, B, C, ...) is connected to the hub with the help of two links one for transmitting and the other for reception of the data.
- When a single station transmits, the hub repeats the signal and sends it to each station.
- Typically the length of each link is 100 m. If the twisted pair is used and the length may increase upto 500 m if the optical fibre is used as transmission medium.
- It is important to note that if two stations transmit simultaneously, then there will be a collision between their transmitted signals.

Disadvantages of star topology :

- If the central hub fails, the whole network fails to operate.
- Many star networks require a device at the central point to rebroadcast or switch the network traffic.
- 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.

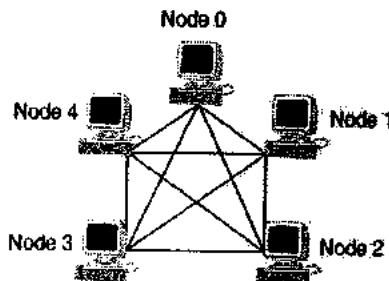
1.2.5 Mesh Topology :

In a mesh topology every device is physically connected to every other device with a point to point dedicated link as shown in Fig. 1.2.8.

- The term dedicated means that the link carries data only between two devices connected on it.
- 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.



(G-21) Fig. 1.2.8 : Mesh topology

Advantages :

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

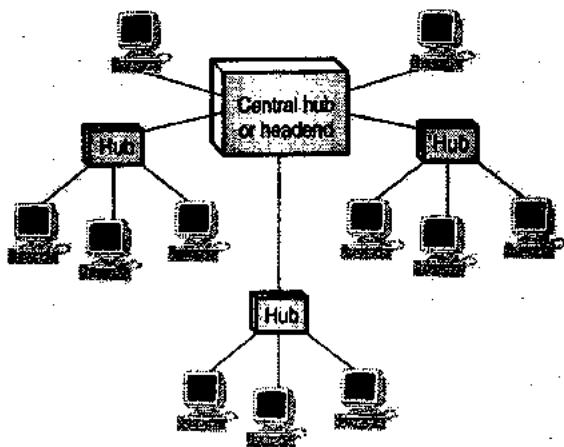
Disadvantages :

- Since every computer must be connected to every other computer installation and reconfiguration is difficult.
- Cabling cost is more.
- The hardware required to connect each link input/output and cable is expensive.

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

1.2.6 Tree Topology :

- A tree topology is a variation of a star. As in a star, nodes in a tree are connected to a central hub 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. 1.2.9.
- The central hub in the tree is an active hub which contains repeater. The repeater amplifies the signal and increases 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.



(G-22) Fig. 1.2.9 : Tree topology

Advantages :

1. It allows more devices to be attached to a single hub and can therefore increase the distance of 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 star topology.

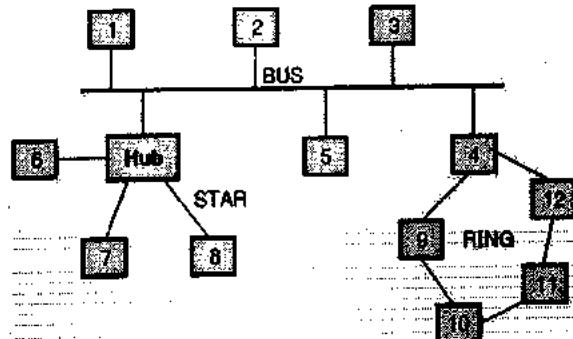
1.2.7 Logical Topology :

- 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.

1.2.8 Hybrid Topology :

- 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. 1.2.10 shows the hybrid topology in which bus, star and ring topologies are used simultaneously.
- In Fig. 1.2.10, 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.

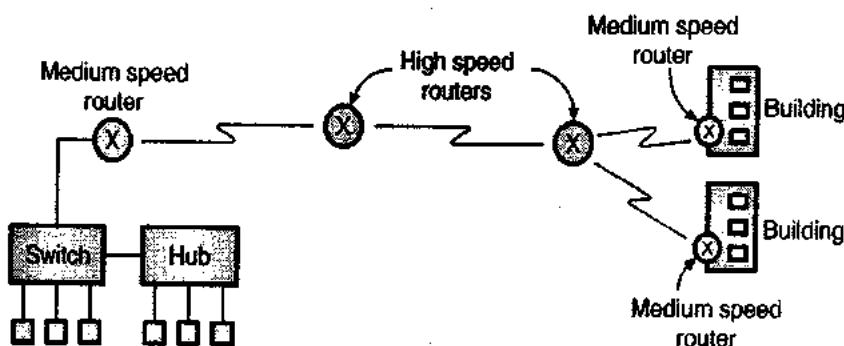


(G-23) Fig. 1.2.10 : Hybrid topology

- 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.

1.2.9 Hierarchical Topology :

- In the network design for the corporate world we need to meet customer's business and communication goals. For this you might need to recommend a network topology consisting of many pieces and parts.
- We can simplify this task by breaking things down and develop the design in pieces or layers.
- The hierarchical network design model helps us to develop a network topology in separate layers with each layer focusing on specific function. This helps us to choose right equipment and features for the layer.
- Fig. 1.2.11 shows an example of hierarchical design using routers for core, switches for distribution and hubs for access.



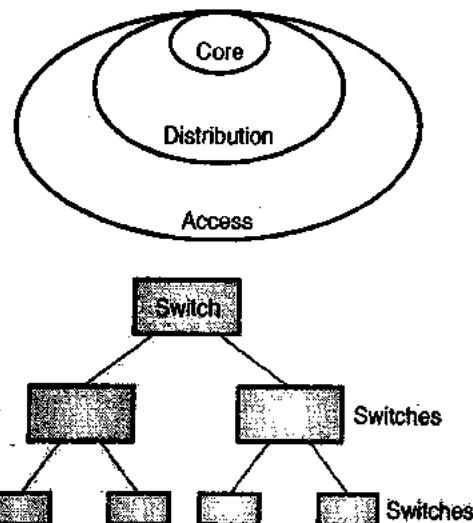
(G-1941) Fig. 1.2.11 : Hierarchical design using routers, switches and hubs

- In Fig. 1.2.11, the high speed WAN routers carry the traffic along the enterprise backbone. Then medium speed routers connect buildings at each campus whereas switches and hubs connect the user devices and the servers within buildings.
- Networks growing in an unplanned way tend to develop an unstructured format. Such networks are called as fur-ball networks.
- We can use the hierarchical topology for such fur ball networks so as to minimize the network costs because now we can buy the appropriate networking devices for each layer of hierarchy.
- It is also possible to accurately plan the network capacity at within each layer of hierarchy. This would reduce the wastage of bandwidth.
- It is possible to apply network management responsibility and network management systems to different layers to control costs.
- Hierarchical topology to keep design and testing process simple. Fault isolation is improved.
- This topology makes it possible to change the network environment.

Hierarchical switch network :

- A general hierarchical model of a network is made of three pieces or layers as shown in Fig. 1.2.12.
- The hierarchical topology is preferred because it is a scalable network. It is easy to expand the hierarchical network.
- In Fig. 1.2.12, the core layer is a high speed switching and routing backbone and it should be designed to pass network traffic as fast as possible.
- The distribution layer defines the network boundaries and at this layer the packet manipulation takes place. The network security is also provided at this layer.
- At the access layer the local end users are allowed into the network.
- The layer 3 switches (corresponding to the core) are the smartest because they have to perform the routing functions calculating the best path to send traffic to destination. These switches read the network address.

- The layer 2 switches are less smart and slow as compared to layer 3 switches. They can only read the data link layer (MAC) address. Layer 3 switches can read both MAC and network addresses.



(G-1942) Fig. 1.2.12 : Hierarchical topology using switches

1.3 Uses of Computer Networks :

The computer networks are playing an important role in providing services to large organizations as well as to the individual common man.

1.3.1 Service Provided by the Network for Companies :

- Many organisations have a large number of computers in operation. These computers may be within the same building, campus, city or different cities.
- Even though the computers are located in different locations, the organisations want to keep track of inventories, monitor productivity, do the ordering and billing etc.



- The computer networks are useful to the organisations in the following ways :

1. Resource sharing :

It allows all programs, equipments and data available to anyone on the network irrespective of the physical location of the resource and the user.

2. High reliability due to alternative sources of data :

- It provides high reliability by having alternative sources of data. For e.g. all files could be replicated on more than one machines, so if one of them is unavailable due to hardware failure or any other reason, the other copies can be used.
- The aspect of high reliability is very important for military, banking, air traffic control, nuclear reactor safety and many other applications where continuous operations is a must even if there are hardware or software failures.

3. Cost :

- Computer networking is an important financial aspect for organisations because it saves money.
- Organisations can use separate personal computer one per user instead of using mainframe computer which are expensive.
- The organisations can use the workgroup model (peer to peer) in which all the PCs are networked together and each one can have the access to the other for communicating or sharing purpose.
- The organisation, if it wants security for its operation it can go in for the domain model in which there is a server and clients. All the clients can communicate and access data through the server.

4. Communication medium :

- A computer network provides a powerful communication medium among widely separated employees.
- Using network it is easy for two or more employees, who are separated by geographical locations to work on a report, document or R and D simultaneously i.e. on-line.

1.3.2 Networks for People :

The computer networks offer the following services to an individual person :

- Access to remote information
- Person to person communication
- E-commerce
- Interactive entertainment.

1. Access to remote information :

Access to remote information involves interaction between a person and a remote database. Access to remote information comes in many forms like :

- Home shopping, paying telephone, electricity bills, e-banking, on line share market etc.
- Newspaper is on-line and is personalised, digital library consisting of books, magazines, scientific journals etc.
- World wide web which contains information about the arts, business, cooking, government, health, history, hobbies, recreation, science, sports etc.

2. Person to person communication :

Person to person communication includes :

- Electronic-mail (e-mail)
- Real time e-mail i.e. video conferencing allows remote users to communicate with no delay by seeing and hearing each other. Video-conferencing is being used for remote school, getting medical opinion from distant specialists etc.
- Worldwide newsgroups in which one person posts a message and all other subscribers to the newsgroup can read it or give their feedbacks.

3. Interactive entertainment :

Interactive entertainment includes :

- Multiperson real-time simulation games.
- Video on demand.
- Participation in live TV programmes likes quiz, contest, discussions etc.

1.4 Social Issues :

- New social, ethical and political problems have been faced as the computer networks have expanded in size.
- A popular feature of many networks is newsgroups or bulletin boards. Here people can exchange messages their views about a topic.
- But trouble comes when newsgroups discuss sensitive topics such as religion, politics or sex.
- There are many such social issues associated with the computer networks.

1.5 Network Hardware :

- Now let us discuss the technical issues involved in the network design.
- Two important dimensions of a computer network are :
 - Transmission technology and
 - Scale.



1.5.1 Types of Transmission Technology :

The transmission technology can be categorised broadly into two types :

1. Broadcast networks and
2. Point-to-point networks.

1. Broadcast networks :

- In a broadcast networks all the machines on the network use or share communication channel that is shared or used by all the machines on the network. Short messages called packets sent by any machine are received by all the others.
- Broadcast systems generally use a special code in the address field for addressing a packet to all the concerned computers. This mode of operation is called broadcasting.
- Some broadcast systems also support transmission to only a group of few machines known as multicasting.
- When a packet is received, a machine checks the address field. If the packet is addressed to it then the packet is processed, otherwise the packet is ignored.

2. Point-to-point networks :

- In point to point networks there exist of many connections between individual pairs of machines. To go from the source to the destination a packet on this types of network may have to go through intermediate computers before they reach the desired computer.
- The packets emerging from the same source have to follow multiple routes, of different lengths.
- Hence properly designed routing algorithms are very important in the point-to-point networks.
- An important general rule is as follows :

Small, localized networks (e.g. LAN) tend to use the broadcasting, whereas networks located over wide geographical areas (such as WAN) use point-to-point transmission.

1.6 Network Scale :

- This is an alternative criterion for classification of networks.

- Fig. 1.6.1 gives the network classification based on their physical size. All these systems are multiprocessor systems.

Interprocessor distance	Processors are located in	Example of network
0.1 m	Same circuit board	Data flow machine
1 m	Same system	Multicomputer
10 m	Same room	LAN
100 m	Same building	LAN
1 km	Same campus	LAN
10 km	Same city	MAN
100 km	Same state	WAN
1,000 km	Same continent	WAN
10,000 km	Same planet	Internet

Fig. 1.6.1 : Network classification according to scale

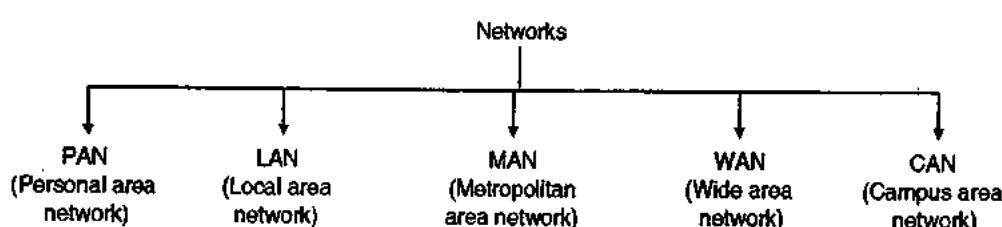
- Beyond the multicomputers are the true networks, in which the computers communicate by exchanging messages over long cables.
- Such networks are divided into following categories :
 1. Local area networks
 2. Metropolitan networks and
 3. Wide area networks.

Internetwork :

- The connection of two or more networks is called as an internetwork.
- The best example of internetwork is the Internet.

1.7 Network Classification by their Geography :

- Computer network can be classified based on the geographical area they cover, i.e. the area over which the network is spread.
- Such a classification is shown in Fig. 1.7.1.
- In this section, we will discuss the following categories of networks :



(G-1400)Fig. 1.7.1 : Network categories



1.7.1 Local Area Networks (LAN) :

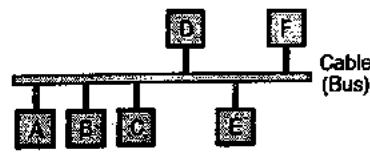
- The Local Area Network (LAN) is a network which is designed to operate over a small physical area such as an office, factory or a group of buildings. LANs are very widely used in a variety of applications.
- LANs are easy to design and troubleshoot. The personal computers and workstations in the offices are interconnected via LAN.
- The exchange of information and sharing of resources becomes easy because of LAN.
- In LAN all the machines are connected to a single cable. Different types of topologies such as Bus, Ring, Star, Tree etc. are used for LANs.
- LAN uses a layered architecture and they are capable of operating at hundreds of Mbits/sec.
- A Local Area Network (LAN) is usually a privately owned and links the devices in a single office, building or campus of upto a few kilometres in size as shown in Fig. 1.7.1.
- Depending on the needs of an organisation and the type of technology used, a LAN can be as simple as a few computers and a printer at home or it can contain many computers in a company and include voice, sound and video peripherals.
- LANs are widely used to allow resources to be shared between personal computers or workstations. The resources to be shared can be hardware like a printer or softwares or data.
- In a LAN one of the computer can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- LAN's are also distinguished from MAN's and WAN's based on the transmission media they use and topology. In general a given LAN will use only one type of transmission medium. The most common networking topologies used are bus, ring and star.
- The data rates for LAN can now range from 10 Mbps to 16 Gbps.

Important characteristics of LAN :

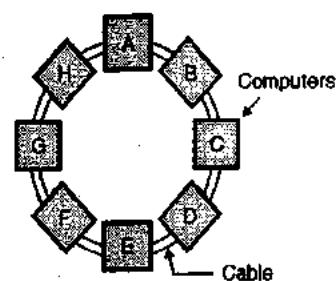
1. Very high degree of interconnection between the computers.
2. High rate of data transmission.
3. Physical connection of computers in a LAN is easy.
4. Every computer in the LAN can communicate with every other computer.
5. The medium used for data transmission is inexpensive.

LAN topologies :

Various topologies are possible for the broadcast LANs such as bus topology or ring topology as shown in Fig. 1.7.2.



(a) Bus topology



(b) Ring topology

(G-32) Fig. 1.7.2 : LAN topologies

Static and Dynamic broadcast networks :

- The broadcast networks are further classified into two types namely :
 1. Static networks and
 2. Dynamic networks.
- This classification is based on how the common channel is allocated.
- In static allocation, each machine is allowed to broadcast only in its allotted time slot.
- But static allocation wastes the channel capacity when a machine does not want to transmit in its allotted time slot.
- Hence most of the systems try to allocate the channel dynamically i.e. on demand.

LAN components :

Some of the important LAN components are as follows :

1. Workstations.
2. File servers.
3. Gateway.
4. Network interfacing unit.
5. Active and passive hubs.
6. LAN cables or communication channels.

Workstation :

Workstation refers to the individual, single computer. A communication capability is added to enable it for networking.

File server :

File server is a computer that allows the sharing of data, software and hardware resources by running special softwares.

Gateway :

It assists the transfer of data from one LAN to the other LAN.

Network Interfacing Unit (NIU) :

It is a unit which consists of hardware as well as software. It uses microprocessor to control the access and communication in a network.

LAN cables or communication channel :

A cable is used for connecting the computers in a LAN. The communication from one computer to others takes place over the cables. So cables are called communication channels. The twisted pair, coaxial cables or optical fiber cables are used in LANs.

Advantages of LAN :

1. High reliability. Failure of individual computers does not affect the entire LAN.
2. It is possible to add a new computer easily.
3. The transmission of data is at a very high rate.
4. Sharing of peripheral devices such as printer is possible.

Applications of LAN :

1. File transfer and file access.
2. Personal computing.
3. Office automation.
4. Distributed computing.
5. Word and text processing.
6. Document distribution.
7. Remote access to database.
8. Electronic message handling.

1.7.2 Ethernet :

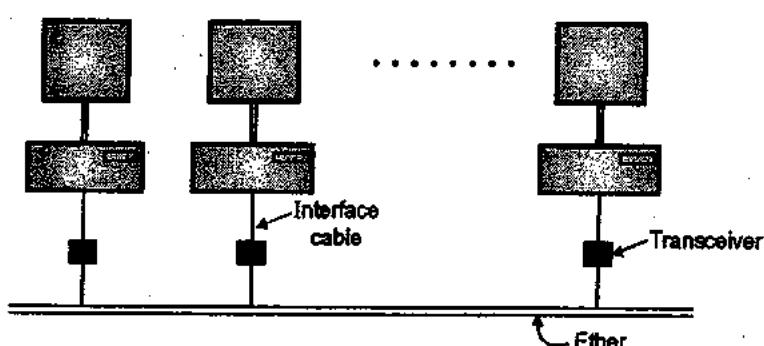
- Both Internet and ATM (Asynchronous Transfer Mode) were designed for wide area networking. But

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)
- Traditional Ethernet was created in 1976 and has a data rate of 10 Mbps.
- The fast Ethernet is its next version and has a data rate of 100 Mbps.
- The Gigabit Ethernet operates at the data rate of 1000 Mbps or 1 Gbps.

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.



(G-23)Fig. 1.7.2(c) : Architecture of original Ethernet

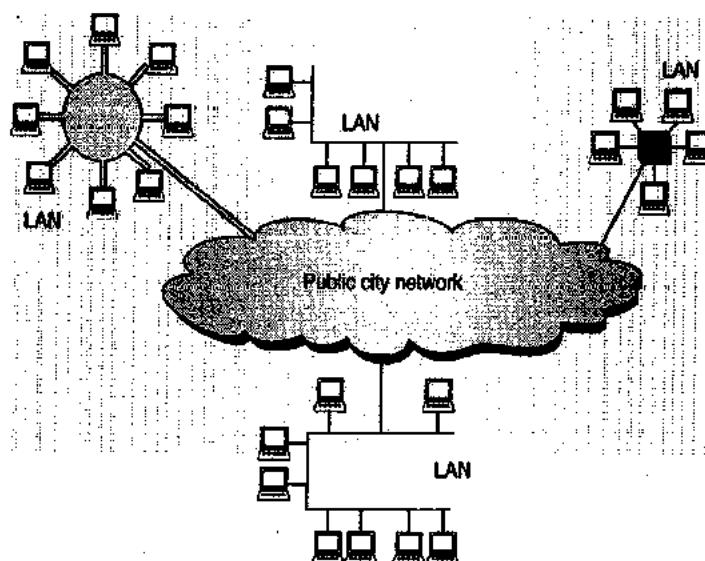
Transmission medium :

- 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.
- The architecture of the original Ethernet is shown in Fig. 1.7.2(c).
- 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.

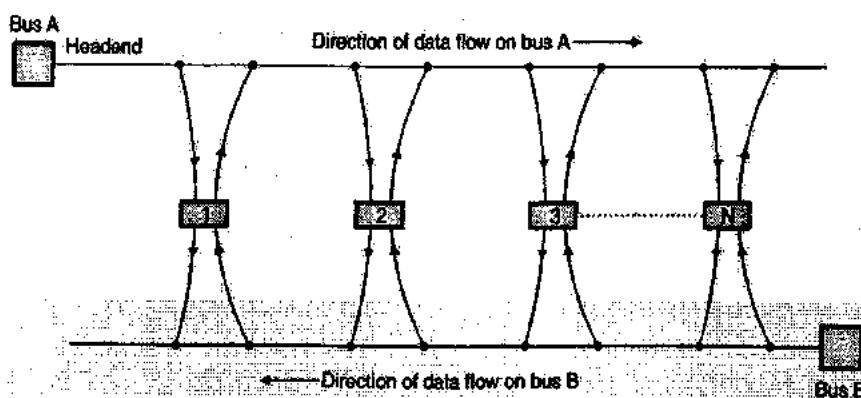
1.7.3 Metropolitan Area Network (MAN) :

- A MAN is basically a bigger version of a LAN and normally uses similar technology. It is designed to extend over a larger area such as an entire city.

- The MAN can be in the form of a single network such as a cable network or it can be a combination of multiple LANs as shown in Fig. 1.7.3.
- A MAN may be wholly owned and operated by a private company or it may be a service provided by a public company, such as a local telephone company (telco).
- A MAN is distinguished by the IEEE 802.6 standard or it is also known as Distributed Queue Dual Bus (DQDB).
- The DQDB consists of two unidirectional cables (buses) to which all the computers are connected as shown in Fig. 1.7.4.
- Each bus has a device which initiates the transmission activity called as the head-end.
- Traffic that is destined for a computer to the right of the sender uses the upper bus and to the left uses the lower bus as shown in Fig. 1.7.4.



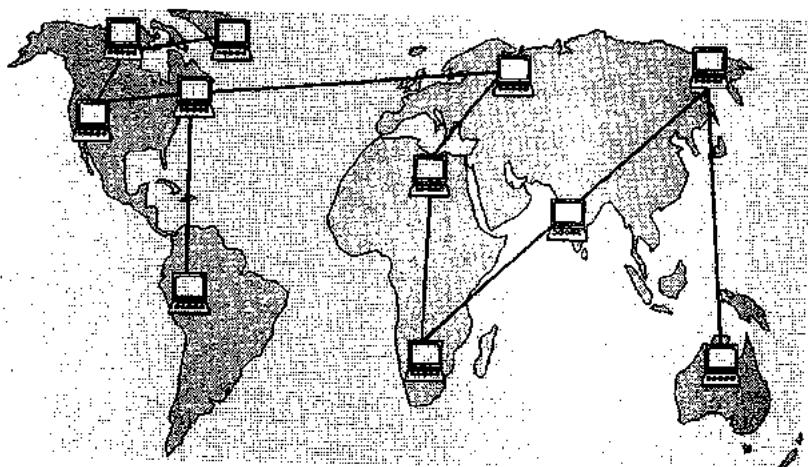
(G-33)Fig. 1.7.3 : Metropolitan area network



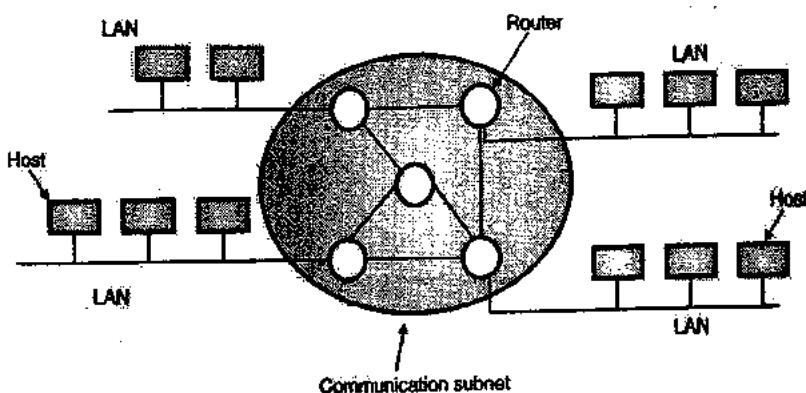
(G-34)Fig. 1.7.4 : Distributed queue dual bus architecture(DQDB)

1.7.4 Wide Area Network (WAN) :

- When a network spans a large distance or when the computers to be connected to each other are at widely separated locations a local area network cannot be used.
- For such situations a Wide Area Network (WAN) must be installed. The communication between different users of "WAN" is established using leased telephone lines or satellite links and similar channels.
- It is cheaper and more efficient to use the phone network for the links.
- Most wide area networks are used for transferring large blocks of data between its users. As the data is from existing records or files, the exact time taken for this data transfer is not a critical parameter.
- An example of WAN is an airline reservation system. Terminals are located all over the country through which the reservations can be made.
- It is important to note here that all the terminals use the same centralized common data provided by the central reservation computer.
- Because of the large distances involved in the wide area networks, the propagation delays and variable signal travel times are major problems.
- Therefore most wide area networks are not used for time critical applications. As explained earlier they are more suitable for transfer of data from one user to the other which is not a time critical application. Wide area networks are basically packet switching networks.
- A WAN provides long distance transmission of data, voice image and video information over large geographical areas that may comprise a country, a continent or even the whole world as shown in Fig. 1.7.5.
- WAN contains a collection of machines used for running user (i.e. application) programs. All the machines called hosts are connected by a communication subnet as shown in Fig. 1.7.6.
- The function of the subnet is to carry messages from host to host. The subnet consists of two important components; transmission lines and switching elements.
- Transmission lines move bits from one machine to another. The switching elements are specialised computers used to connect two or more transmission lines. When data arrive on an incoming line, the switching element has to choose an outgoing line on which it is to be forwarded.



(G-35)Fig. 1.7.5 : Wide area network

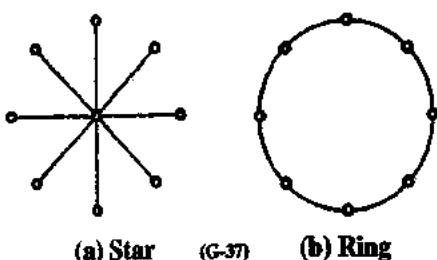


(G-36) Fig. 1.7.6 : Communication subnet and hosts

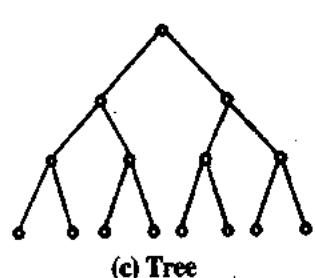
- The switching elements are either called as packet switching nodes, intermediate systems, data switching exchanges or routers.
- When a packet is sent from one router to another via one or more intermediate routers, the packet is received at intermediate router. It is stored in the routers until the required output line is free and then forwarded. A subnet using this principle is called a point to point, store-forward or packet switched subnet.
- WAN's may use public, leased or private communication devices, and can spread over a wide geographical area. A WAN that is wholly owned and used by a single company is often called as an enterprise network.
- In most WANs the network contains a large number of cables or telephone lines each one connecting a pair of routers.
- If two routers which are not connected to each other via a cable want to communicate, then they have to do it indirectly via other routers.

Router interconnection topologies :

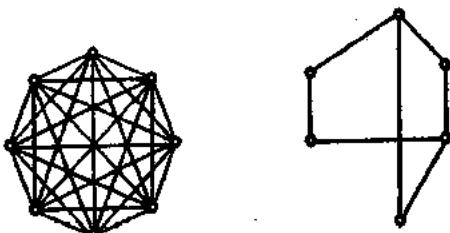
- Fig. 1.7.7 shows some of the possible router interconnection topologies in a point to point subnet.



(G-37) (a) Star (b) Ring



(G-37) Fig. 1.7.7 (Contd..)



(G-38) Fig. 1.7.7 : Router interconnection topologies

- The LANs have a symmetric topology while WANs have irregular topologies.
- The WANs can also be formed using satellite or ground radio system. Satellite networks are inherently broadcast type so they are useful when the broadcast property is important.

Characteristics of WAN :

Following are some of the important characteristics of WAN :

- Remote data entry and access is possible.
- Communication facility is provided.
- Centralized information is created and used.

1.7.5 PAN (Personal Area Network) :

- A Personal Area Network (PAN) is a computer network designed for and organized around an individual person.
- A PAN generally consists of a mobile computer such as a laptop, a cell phone and /or a Personal Digital Assistant (PDA). PAN will allow the communication to take place among these devices.
- PAN can also be used for communication among personal devices themselves (intrapersonal communication) or for connecting to a higher level network and internet (This is called as an uplink).



- The PANs can be constructed using cables or it can be wireless. The wireless PANs typically use Bluetooth or sometimes use the infrared connections.
- The PANs generally cover a range upto 10 meters. PAN can be considered as a special type of Local Area Network (LAN), which is designed for one person instead of a group.

1.7.6 CAN (Campus Area Network) :

- The Campus Area Network (CAN) is made up of an interconnection of LAN within a limited geographical area.
- The network equipments such as switches, routers and the transmission media i.e. optical fiber etc. are almost entirely owned by the campus owner (i.e. a company, university, government etc.)
- For example, a university CAN would connect different buildings in its campus, such as various departments, library, student hall to each other.
- CAN could also be thought of as a special case of WAN.

1.7.7 Wireless Networks :

- The fastest growing segment of the computer industry is the mobile computers such as notebook computers and Personal Digital Assistant (PDAs).
- The wireless networks are becoming increasingly important because the wired connection is not possible in cars or aeroplanes.
- Wireless networks can have many applications. A very common example is the portable office.
- People travelling on road often want to make use of their portable electronic equipment for telephone calls, e-mails, faxes, read remote files etc.

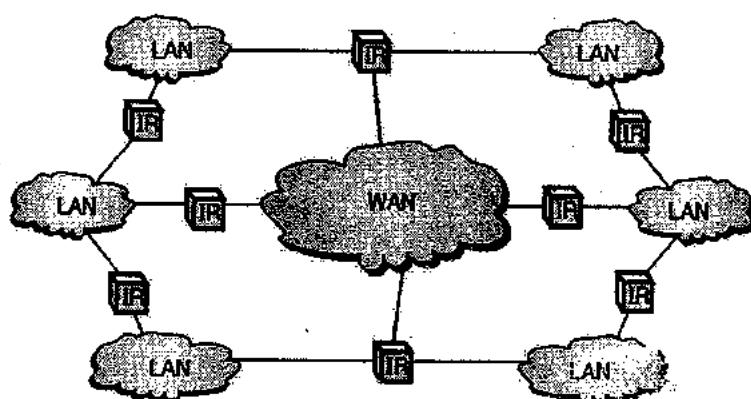
- Wireless networks can exist on trucks, buses, taxies, aeroplanes etc. They are used where the telephone systems are destroyed in the event of disasters such as fires, floods and earthquakes etc.
- The wireless networks are important for military.
- Wireless networks and mobile computing are related but they are not identical because portable computers are sometimes wired and some wireless computers are not portable.
- But some applications are truly mobile wireless applications such as a portable office, inventories being handled by PDAs, etc.
- Wireless LAN is another example of wireless network. Direct digital cellular service CDPD (Cellular Digital Packet Data) is now becoming available.
- It is possible to have combinations of wired and wireless networking.

1.7.8 Internetworks :

- When two or more networks are connected together they are called as internetwork or internet as shown in Fig. 1.7.8.
- Individual networks are joined into internetworks by the use of internetworking devices like bridges, routers and gateways.
- Fig. 1.7.8 shows a general form of internet. It is the collection of number of LANs which are interconnected via a WAN.

What is the difference between a subnet and WAN ?

If the system within a closed periphery contains only routers then it is called as a subnet. But if it contains routers as well as hosts then it is a WAN.



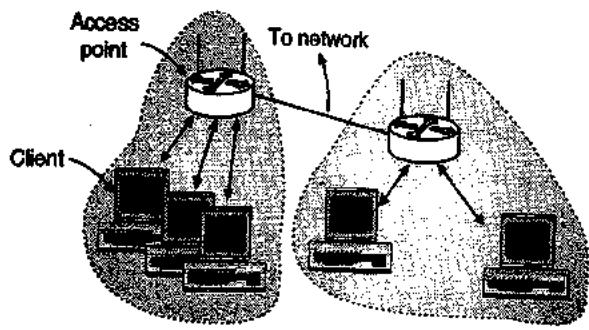


1.7.9 Comparison of LAN, WAN and MAN :

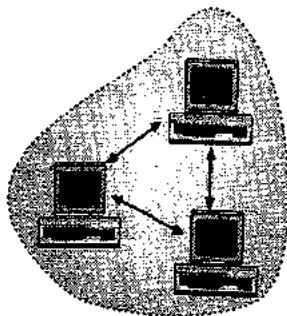
Sr. No.	Parameter	LAN	WAN	MAN
1.	Ownership of network	Private	Private or public	Private or public
2.	Geographical Area covered	Small	Very large (states or countries)	Moderate (city)
3.	Design and maintenance	Easy	Not easy	Not easy
4.	Communication medium	Coaxial cable	PSTN or satellite links	Coaxial cables, PSTN, optical fiber cables, wireless.
5.	Data rates (speed)	High	low	Moderate
6.	Mode of communication	Each station can transmit and receive	Each station cannot transmit	Each station can transmit or receive.
7.	Principle	Operates on the principle of broadcasting	Switching	Both
8.	Propagation delay	Short	Long	Moderate
9.	Bandwidth	Low	High	Moderate

1.8 Ad-Hoc Networks :

- 802.11 networks can be used in two possible modes :
 - Infrastructure mode
 - Ad-hoc mode.



(a) Infrastructure mode



(b) Ad-hoc mode

(G-1527) Fig. 1.8.1 : Types of 802.11 networks

- The other mode of operation is ad-hoc networks as shown in Fig. 1.8.1(b). In this mode a group of computers can communicate to each other directly without any Access Point (AP) in between.

- The infrastructure mode is as shown in Fig. 1.8.1(a). The client such as laptop or a smart phone is connected to another network such as company Internet.
- In this mode the client is associated with an Access Point (AP) which is in turn connected to the other network as shown.
- The client sends and receives its packets via AP. Many such APs are connected together to form an extended 802.11 network.

1.9 Network Classification by their Component Role :

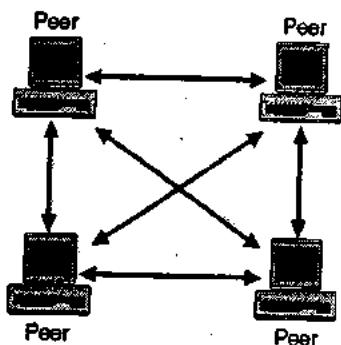
- The local area networks are classified into two types :
 - Peer to peer networks.
 - Client server networks.
- The relationship between each PC or device on the network with the others in terms of control will be dependent on the choice of network type.
- For these two types, the special software is required for controlling the flow of information between the users.
- The Network Operating System (NOS) is installed on each PC depending on the type of network. NOS monitors the data exchange, flow of files, and other information.
- The network operating systems are different for the peer to peer and client server networks.
- A peer-to-peer network is analogous to a company that uses decentralized management, where decision are made locally.



- A client-server network is similar to company that works on the principle of centralized management, where decisions are made in a central location.

1.10 Peer-to-Peer Networks :

- Fig. 1.10.1 shows the structure of the peer-to-peer network. In this type of network, each computer is responsible for making its own resources available to other computers on the network.
- Each computer is responsible for setting up and maintaining its own security for its resources.
- Also each computer is responsible for accessing the required network resources from peer-to-peer relationships.
- Peer to peer network is useful for a small network containing less than 10 computers on a single LAN. Each computer maintains its own accounts and their security settings.
- In peer-to-peer network, every computer can function as both a client and server. Windows 2000 comes in both server and professional versions, but it's still a peer-to-peer operating system.
- Peer to peer networks do not have a central control system. There are no servers in peer networks.
- In this type of network users simply share disk space and resources, such as printers and faxes.
- Peer networks are organised into workgroups. Workgroups have very little security. There is no central login process.
- If the user has logged into one peer on the network he can use any resources on the network that are not controlled by a specific password.



(G-40) Fig. 1.10.1 : Peer-to-peer network relationship

- Access to individual resources can be controlled if the user who shared the resources installs a password to access it.

- Since there is no central security, the user will have to know individual password for each secured shared resource which he wants to access.
- Peer to peer networks are relatively simple. Each computer in the network can act as client as well as server as per requirement.
- This eliminates the need of expensive server.
- No additional software is necessary in order to set up the peer to peer network.

1.10.1 When to use Peer to Peer Networks ?

The peer to peer networks are suitable for the following working conditions :

- If network security is not an important issue.
- If the number of users is less than 10 (small network).
- If all the users are situated in the same area.
- If the possibility of future expansion is less.

1.10.2 Advantages of Peer to Peer Networks :

Peer networks have many advantages, especially for small business houses that cannot afford to buy expensive server hardware and software.

- No extra investment in server hardware or software is required.
- Use less expensive computer hardware :** In peer-to-peer network, the resources are distributed over many computers, so there is no need for higher-end-server computer.
- Easy to administer :** In peer-to-peer network each machine performs its own administration.
- No NOS required :** Peer-to-peer network does not require a Network Operating System (NOS).
- More built-in-redundancy :** If you have a small network, with 10-20 workstations and each one with some important data on it, and one fails you still have most of your shared resources available.

Peer-to-peer network achieves more redundancy because of smaller possibility of single point of failure.

- Easy setup and lower cost for small networks.
- Users can control resource sharing.
- A user is not dependent on other computers for its operation.

1.10.3 Disadvantages of Peer to Peer Networks :

There are several disadvantages of peer-to-peer network, particularly for larger networks as follows :



1. Individual performance is affected : If some workstations have frequently used resources on them, then the use of these resources by other computer might adversely affects the person using this particular workstation.
2. Less security : A peer-to-peer network operates on the most common desktop operating systems like windows which are not very secure operating systems.
3. Backup is difficult : In peer-to-peer network there is no centralized server. Hence data is scattered over many workstations. So it is difficult to backup all data in an organized manner.
4. Hard to maintain version control : In peer-to-peer network, files are stored on number of different workstations. So it is difficult to manage different document versions or files.
5. As there is no centralized management it makes large peer networks hard to manage and find data easily.
6. Users are supposed to manage their own computers.
7. It is not possible to save important data in a centralized manner.
8. Additional load on computer because of resource sharing and absence of server.

1.11 Client / Server Network (Server Based Network) :

- In client-server network relationships, certain computers act as server and others act as clients. A server is simply a computer that makes the network resources available and provides service to other computers when they request it. A client is the computer running a program that requests services from a server.

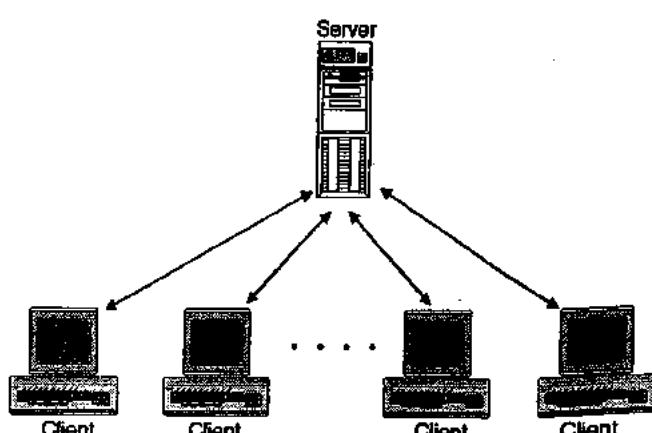
- Local Area Networking (LAN) is based on the client-server network relationship. You can construct a client server network by using one or more powerful networked computers as servers and the rest of as clients. Client-server network typically uses a directory service to store information about the network and its users.
- A client-server network is one in which all available network resources such as files, directories, applications and shared devices, are centrally managed, stored and then accessed by client.
- Fig. 1.11.1 shows client-server network relationship.
- In the client server networks the servers provide security and administration of the entire network.
- In client-server networks the processing tasks are divided between clients and servers. Clients request services such as file storage and printing and servers deliver them.

Client :

The individual workstations in the network are called as the clients.

Server :

- The central computer which is more powerful than the clients and which allows the clients to access its softwares and database is called as the server.
- Server computers typically are more powerful than client computers or are optimised to function as servers.
- No user can access the resources of the servers until he has been authenticated (permitted) by the server to do so.



(G-4)Fig. 1.11.1 : Client server network relationship

1.11.1 Communication in Client-Server Configuration :

- Fig. 1.11.2 explains the principle of communication in the client server configuration.
- The client places a request on the server machine when he wants an access to the centralised resources.



(c-42)Fig. 1.11.2 : Client/server communication

- The server responds to this request and sends the signal accordingly to the client as shown in Fig. 1.11.2.
- The software run at the client computer is called as client program. This software configures that particular computer to act as a client.
- Similarly the software run on the server computer is called as server program. It configures that particular computer to act as a server.

1.11.2 Advantages of Client-server Network :

The advantages of client-server network are as follows :

1. The network is secure :

In client-server network's high security is because of several things :

- Shared resources are located in a centralized area and they are administered centrally.
- The servers are physically placed in secure location such as lockable separate server room.
- The operating system runs on client-server are designed to provide better security to network.
- Better security to network due to good administration.

2. Better performance :

The dedicated server computers are more expensive than standard computer workstations, but they also offer considerably better performance.

3. Centralized backup :

Backing up company's important data is much easier when it is located on a centralized server. Centralized backup is much faster too.

4. Higher reliability :

In client server network centralized dedicated server provide more reliability. It has built-in redundancy.

5. Central file storage, which allows all users to work from the same of data.

6. Reduces cost because of sharing of hardware and software.

7. Increased speed due to dedicated server for sharing resources.

8. Single password allows access to all shared resources.

- Central organisation which keeps data from getting lost among computers and easy manageability of large number of users.
- The individual users don't have to manage or share resources.

1.11.3 Disadvantages of Client-server Networks :

- Professional administration is required :** Client-server networks usually need professional administration. You can hire a network administrator or you can use a company which provides professional network administration services.
- We have to use a high speed server computer with lots of memory and disk space.
- It requires a special network operating system and a number of client licenses.
- Expensive dedicated hardware needs to be used.

1.11.4 Applications of Client-server Configuration :

Some of the important applications are as follows :

- E-mail clients.
- Web browsers.
- FTP (file transfer) clients.

1.11.5 Comparison between Peer-to-Peer Network and Client-Server Network :

Sr. No.	Peer-to-peer	Client-server
1.	It is much like company uses decentralized management.	It is much like company using centralized management.
2.	In this each machine has same power.	In this server has more power and client has less power.
3.	Uses less expensive computer hardware.	It has to use expensive hardware.
4.	Easy to setup and administer.	Complex to setup and require professional administrator.
5.	Less secure.	Very secure.
6.	Decentralized backup i.e. difficult to backup.	Centralized backup i.e. easy to backup.
7.	Network O.S. not required.	Network O.S. required.
8.	It has built-in redundancy.	Not built-in redundancy.
9.	It is suitable for small network.	It is suitable for large network.
10.	Poor performance.	Better performance.

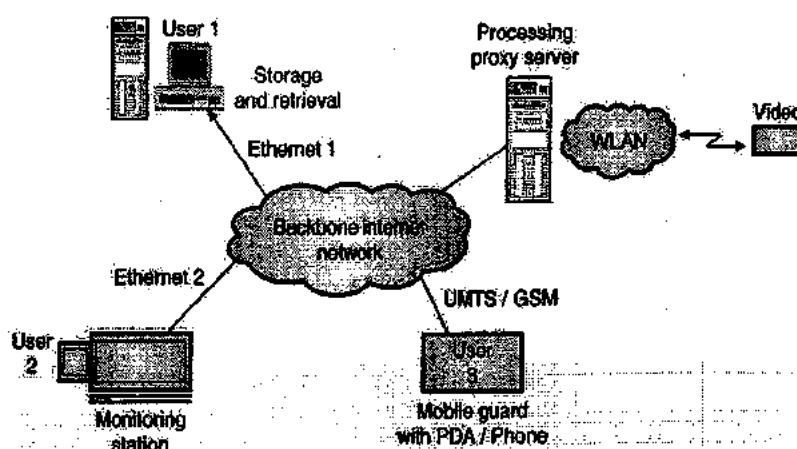


1.11.6 Distributed Networking :

- Distributed networking is a distributed computing network system. It is said to be distributed when the computer programming and the data to be worked on are spread out across more than one computer.
- Usually the distributed networking is implemented over a computer network.
- Prior to the emergence of low cost desk tops, the computing was generally centralized to one computer.
- Although such centers still exist, the distributed networking applications operate more efficiently.
- A popular example of distributed networking is the client server network.
- However very large enterprises find it extremely difficult to manage their distributed network using the traditional client server approach. So the recent development in the field of cloud computing has opened up new possibilities.
- We may define the distributed network as a type of computer network that is spread over different networks. This provides a single data communication network, which can be managed jointly or separately by each network.
- Besides shared communication within the network a distributed network often uses the distributed processing.
- Distributed networks are part of distributed computing architecture, in which enterprise IT infrastructure resources are divided over a number of networks, processes and intermediary devices.
- A distributed network is powered by a network management software, which manages and monitors data routing combining and allocating network bandwidth, access control and other important networking processes.
- Fig. 1.11.3 shows the simplified Distributed Network Architecture (DNA).

1.11.7 SDN (Software Defined Network) :

- In the recent years, there has been a tremendous increase in carrier network traffic. This is basically due to the explosive growth in the use of online applications and in the mobile connected devices.
- Now a days the network operators need to cope up with a vast variety of data formats, service types and online devices.
- They need to do so while ensuring security, quality and availability without increasing the costs.
- However the existing network architectures and their management tools are not designed to cope up with such highly elastic demands.
- The Software Defined Network (SDN) is the industry's response to meet all the challenges mentioned above.
- SDN allows the networks to react dynamically to the changes such as usage patterns and availability of network resources.
- It is possible to instantly adjust the network architecture in response to user or application request so that services can be introduced very easily, quickly and at lower costs.
- In SDN a separation is provided between the control plane (controller) and data plane (switch) functions of networks with the help of a protocol that modifies the forwarding tables in network switches.
- Due to this the networks can be easily optimized so that they can respond quickly to the changes in the network usage, without manually reconfiguring the existing infrastructure or hardware.
- SDN also provides an entity i.e. the controller with which the switches and applications can communicate in real time.
- Due to the controller it is possible for the networks to interact with applications. This allows the applications to implement multiple logical network topologies on a single network fabric.



(G-1938) Fig. 1.11.3 : A distributed video surveillance network

Open flow :

- It is a multivendor standard defined by the Open Networking Foundation (ONF) for implementing SDN in networking equipment.
- The open flow protocol defines the interface between an open flow controller and an open flow switch.
- The open flow protocol allows the controller to instruct the switch about handling of incoming data packets.

How does SDN work ?

- SDN provides a wide range of competing architectures but at its most simple, the SDN method centralizes control of network by separating the control logic to off device computer resources.
- All SDN models have some version of an SDN controller as well as southbound APIs and north bound APIs.

1. Controllers :

Controller is the brain of SDN networks. It offers a centralized view of the overall network and enables the network administrator to dictate the underlying systems (such as switches or routers) about the traffic handling.

2. Southbound APIs :

- SDN uses southbound APIs to relay information to the switches and routers "below". Southbound API is one of the most common protocols. "Open Flow" considered as the first standard in SDN was the first southbound API.
- Some people consider open flow and SDN as one and the same. But actually open flow is one piece of SDN.

3. Northbound APIs :

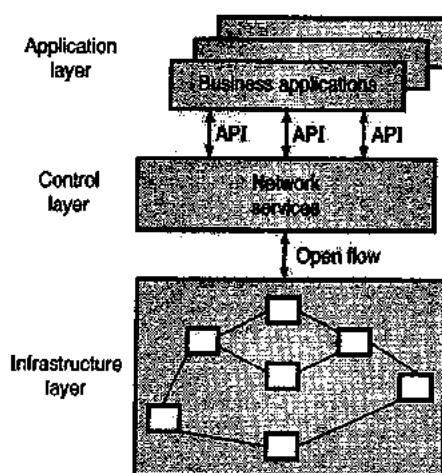
- SDN uses northbound APIs to communicate with the applications and business logic "above".
- This helps the network administrators to shape traffic and deploy services.

The SDN frame work :

Fig. 1.11.4 shows the typical SDN framework. The SDN architecture has the following important features.

Features :

1. Directly programmable
2. Agile
3. Centrally managed
4. Programmatically configured
5. Open standard based
6. Vendor neutral



(G-1939) Fig. 1.11.4 : SDN framework

1. Directly programmable :

In SDN the network control is directly programmable because it is decoupled from the forwarding functions.

2. Agile :

As the control is decoupled from forwarding the administrators dynamically adjust network-wide traffic flow to meet the changing needs.

3. Centrally managed :

In SDN controllers the network intelligence is centralized which maintains a global view of the network. It appears to the applications and policy engineers as a single logical switch.

4. Programmatically configured :

SDN allows the network managers to configure, manage, secure and optimize the network resources very quickly with the help of dynamic, automated SDN programs.

5. Open-standard based and vendor neutral :

As SDN is implemented through open standards, the network design and operation get simplified.

SDN is not same as open flow :

- Many a times people consider open flow same as SDN. But it is not true. As shown in Fig. 1.11.4, open flow is just one element of the SDN architecture.
- Actually open flow is an open standard for communications protocols that enable the control plane to interact with the forwarding plane.
- Note that open flow is not the only protocol available for SDN.

**Benefits of SDN :**

1. It is directly programmable.
2. It has a centralized management.
3. Delivers agility and flexibility.
4. Enables innovation.
5. It is dynamic and manageable.
6. It is cost effective.
7. It is ideal for high bandwidth, dynamic applications.

SDN applications :

1. Software Defined Mobile Networking (SDMN).
2. SD-WAN : It is a WAN managed using the principle of SDN.
3. SD-LAN : It is a LAN that works on the principle of SDN.

1.12 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. 1.12.1 shows the steps involved in this process.
- In Fig. 1.12.1, 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 :**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.

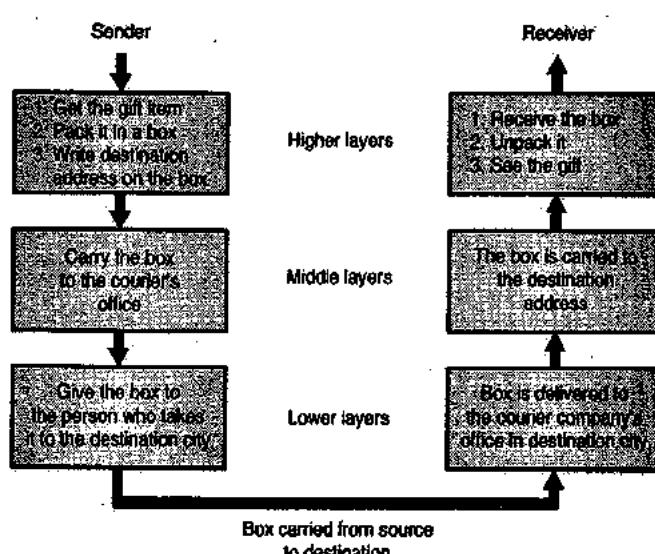
Middle layers : The box is carried by another person to the destination address and the box is delivered.

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.



(G-1546) Fig. 1.12.1 : Layered tasks



1.13 Network Software :

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

1.13.1 Protocol Hierarchies (Layered Architecture) :

- Most networks are organized in the form of a series of layers or levels as shown in Fig. 1.13.1.
- This 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.
- 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. 1.13.1. 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. 1.13.1 show the virtual communication and physical communication is shown by solid lines.

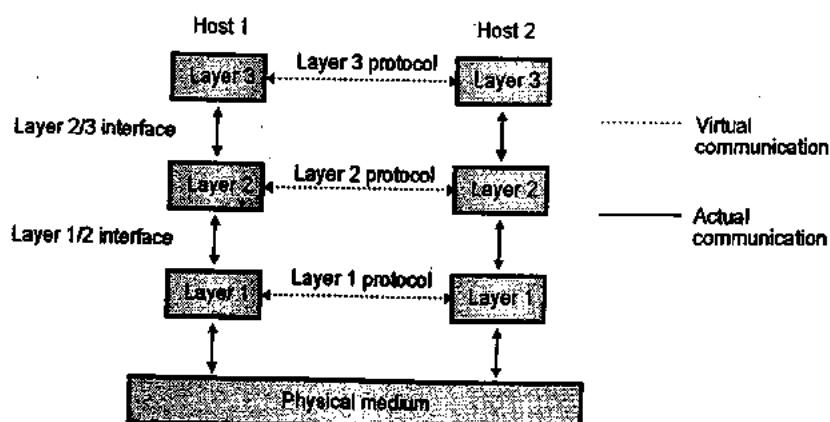
1.13.2 Reasons for having Layered Protocols and Its Benefits :

SPPU : May 10, May 11

University Questions

- Q. 1 What are the reason for using layered protocol ?
(May 10, May 11, 8 Marks)

- 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 :
- It simplifies the design process as the functions of each layers and their interactions are well defined.
 - The layered architecture provides flexibility to modify and develop network services.
 - 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.
 - The concept of layered architecture in a new way of looking at the networks.
 - Addition of new services and management of network infrastructure becomes easy.
 - Due to segmentation (layered structure), it is possible to break difficult problems into smaller and more manageable tasks.
 - Logical segmentation allows parallel working by different teams on different tasks simultaneously.



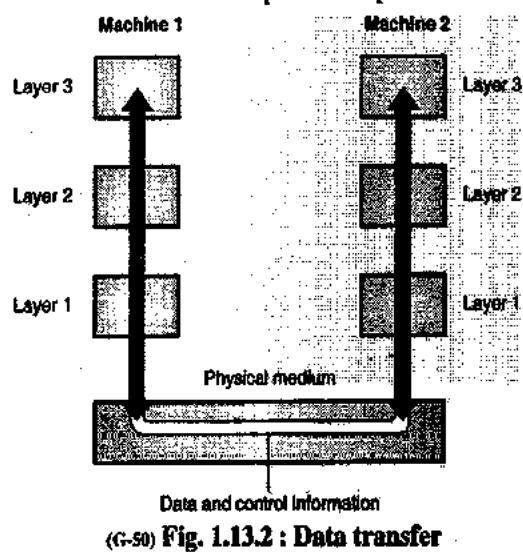
(G-49) Fig. 1.13.1 : Layers, protocols and interfaces

1.13.3 Disadvantages of Layered Architecture :

1. The problem associated with the layered protocols is that we lose touch with the reality.
2. Layering is a kind of hiding information.
3. Layered architecture can sometimes result in poor performance.

1.13.4 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.



(G-50) Fig. 1.13.2 : Data transfer

- 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. 1.13.2.

Interface :

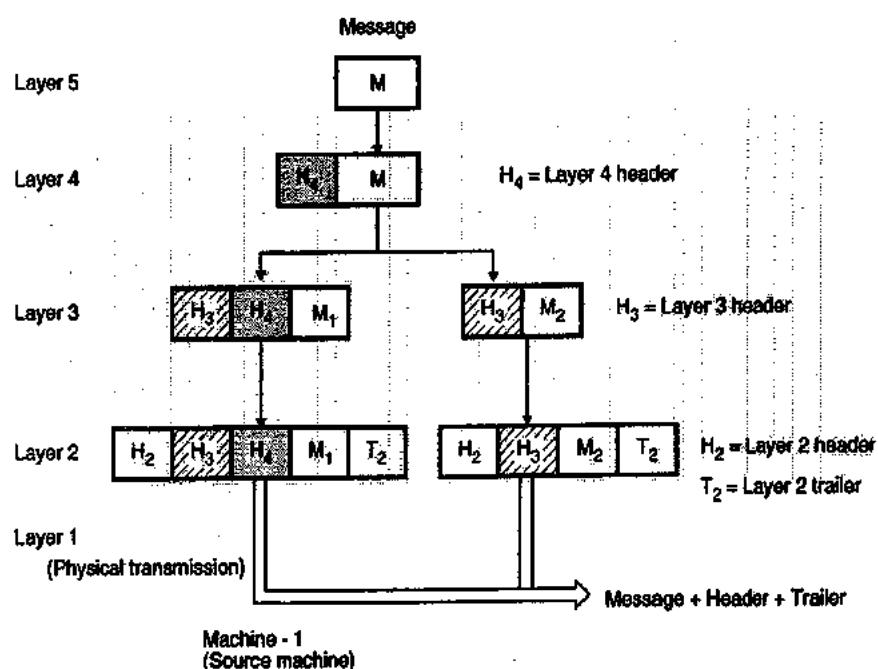
- An interface defines the operations and services offered by lower layer to the upper layer.
- There is an interface between each pair of adjacent layers.

1.14 Network Architecture :

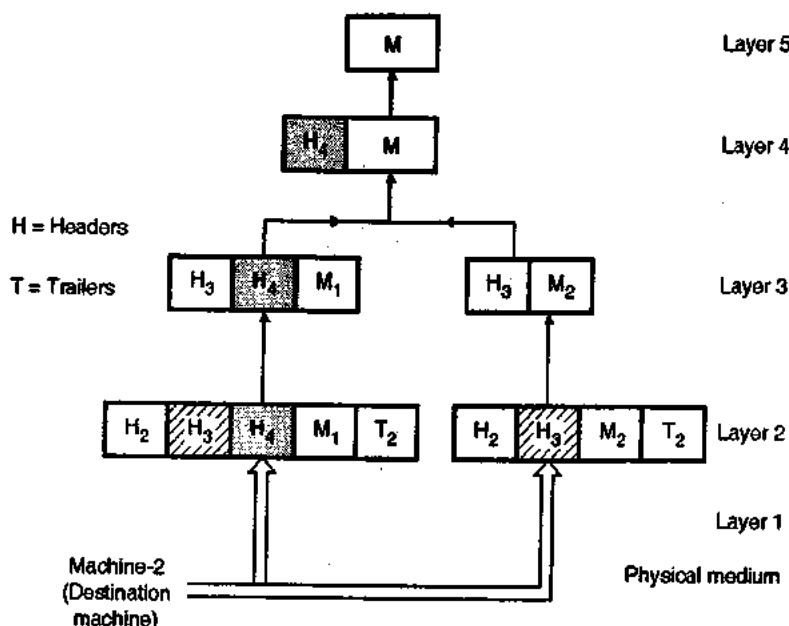
- A set of layers and protocols is called as network architecture.
- Protocol stack is defined as a list of protocols used for a certain system, one protocol per layer.

1.14.1 Virtual Communication between Layers :

- Let us now go into technical details of the communication between say layer 5 of two machines.



(G-51) Fig. 1.14.1 : Information flow for virtual communication between layers 5



(G-52) Fig. 1.14.2

- Refer Fig. 1.14.1 and go through the steps given below to understand the communication.

- Step 1:** A message M is produced by layer 5 of machine 1 and given to layer 4 for transmission.
- Step 2:** Layer 4 adds a header H_4 in front of the message so as to identify the message and passes the (header + message) to layer 3.
- A header includes the control information and it allows a layer 4 in machine 2 to deliver the messages in right order.
- Step 3:** Layer 3 breaks up the incoming messages into small units, packets and appends a layer 3 header to each packet M_1 and M_2 as shown in Fig. 1.14.1 and passes these packets to layer 2.
- Step 4:** Layer 2 adds header as well as trailer to each packet obtained from layer 3 and hands over the resultant unit to layer 1 for physical transmission.

- This sequence of operation taking place at machine 1 is shown in Fig. 1.14.1.
- The control information placed in headers is used at the destination machine (machine 2) to convey the message to layer 5 as shown in Fig. 1.14.2.

1.15 Design Issues for the Layers :

In this section we are going to discuss some of the important design issues that are related to computer networking.

1. Addressing :

- For every layer, it is necessary to identify senders and receivers. Some mechanism needs to be used for the same.
- Since there are many possible destinations for a packet, some form of addressing is needed in order to specify a specific destination.

2. Direction of Transmission :

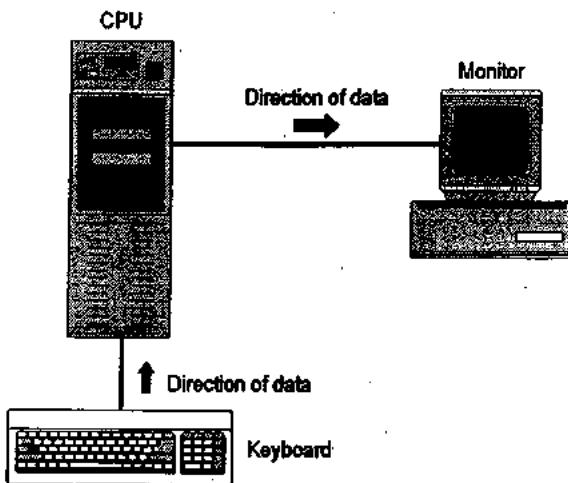
- Another important design issue is the direction of data transfer.
- Depending on the ability of a system to communicate only in one direction or both the directions, the communication systems are classified as :
 - Simplex systems.
 - Half duplex systems.
 - Full duplex systems.

Simplex systems :

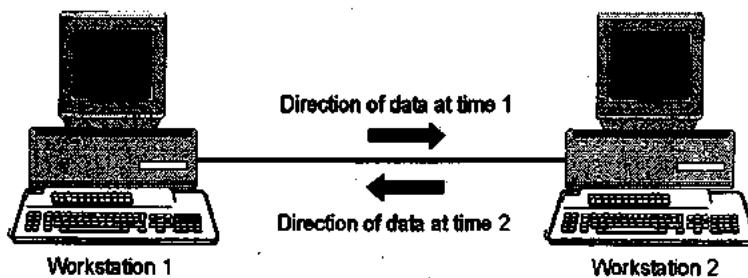
- In these systems the information is communicated in only one direction. For example the radio or TV broadcasting systems can only transmit. They cannot receive.
- In data communication system the simplex communication takes place as shown in Fig. 1.15.1.
- The communication from CPU to monitor or keyboard to CPU is unidirectional.
- Keyboard and traditional monitors are examples of simplex devices.

Half duplex systems :

- These systems are bi-directional, i.e. they can transmit as well as receive but not simultaneously.
- At a time these systems can either transmit or receive, for example a transceiver or walky talky set. Thus the direction of communication will keep changing itself.
- A data communication system working in the half duplex mode is shown in Fig. 1.15.2.
- Each station can transmit and receive, but not at the same time. When one device is sending the other one is receiving and vice versa.
- In half duplex transmission, the entire capacity of the channel is utilized by the transmitting (sending) systems.



(G-53) Fig. 1.15.1 : Simplex mode of data transmission



(G-54) Fig. 1.15.2 : Half duplex system



(G-55) Fig. 1.15.3 : Full duplex mode

Full duplex systems :

- These are truly bi-directional systems as they allow the communication to take place in both the directions simultaneously.
- These systems can transmit as well as receive simultaneously, for example the telephone systems.
- A full duplex data communication system is shown in Fig. 1.15.3. Each station can transmit and receive simultaneously.
- In full duplex mode, signals going in either direction share the full capacity of link.
- The link may contain two physically separate transmission paths one for sending and another for receiving.
- Otherwise the capacity of channel is divided between signals travelling in both directions.

- Many networks provide atleast two logical channels per connection, one for the normal data and the other for urgent data.

3. Error control :

- Another important issue is the error control because physical communication channels can introduce errors in the data travelling on them.
- Error detection and correction both are essential.
- Many error detecting and correcting codes are known out of which those which are agreed upon and receiver should be used.
- The receiver should be able to tell the sender by some means, that it has received a correct message or a wrong message.



4. Avoid loss of sequencing :

- All the communication channels cannot preserve the order in which messages are sent on it.
- So there is a possibility of loss of sequencing. That means messages are not received serially at the receiver.
- To avoid this, all the packets of a message should be numbered so that they can be put back together at the receiver in the appropriate sequence.

5. Ability of receiving long messages :

- At several levels, one more problem needs to be solved, which is inability of all processes to accept arbitrarily long messages.
- So a mechanism needs to be developed to deassemble (break into small messages), transmit and then reassemble messages.

To use multiplexing and demultiplexing :

- Multiplexing and demultiplexing is to be used to share the same channel by many sources simultaneously.
- It can be used for any layer. Multiplexing is needed at the physical layer level.

Interfaces and Services :

The basic function of each layer in the layered structure is to provide service to the layer above it.

- Now we will discuss exactly what service does it provide. But before that, let us define some important terms.

1.16.1 Entities and Peer Entities :

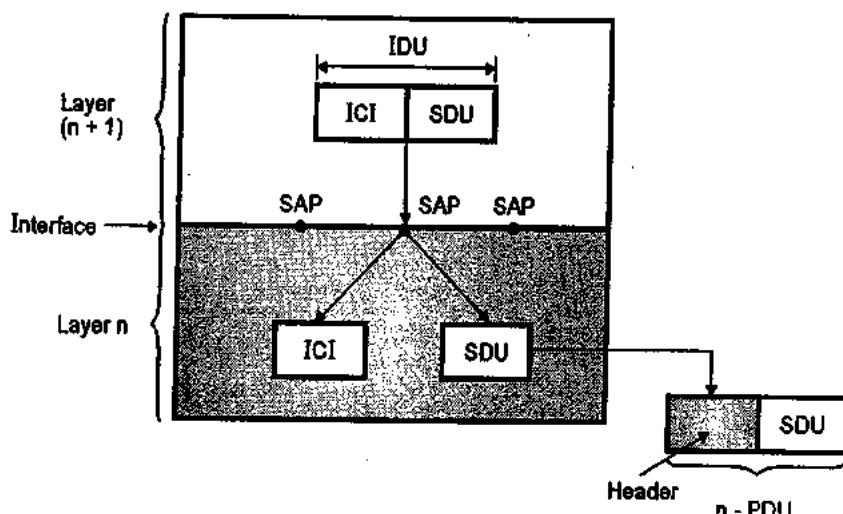
- An entity is defined as the active element in each layer. An entity can be either a software entity or a hardware entity.
- The example of software entity is a process and that of a hardware entity is an intelligent I/O chip.
- Entities in the same layer but on different machines are called as peer entities.

1.16.2 Service Provider and Service User :

- The entities at layer n implement services for the layer $(n + 1)$ which is above the n^{th} layer.
- So layer n which provides service is called as service provider and layer $(n + 1)$ which takes this service is called as service user.

1.16.3 Service Access Points (SAPs) :

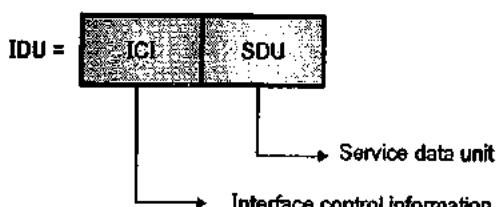
- Refer Fig. 1.16.1 to understand the definition of SAPs.
- The long form of SAP is service access point. They are available at the interface of n and $n + 1$ layer as shown in Fig. 1.16.1.
- Services are available at SAPs. That means the layer n SAPs are those places at the interface where layer $(n + 1)$ can access the services being offered.
- Each SAP has a unique address for its identification.



(G-59) Fig. 1.16.1 : Relation between layers at an interface

1.16.4 Interface Data Unit (IDU) :

- For successful exchange of information between two layers, a set of rules about the interface should be present.
- As shown in Fig. 1.16.2, the layer (n + 1) entity passes an IDU (interface data unit) to the layer n entity through the SAP.



(G-57) Fig. 1.16.2 : IDU

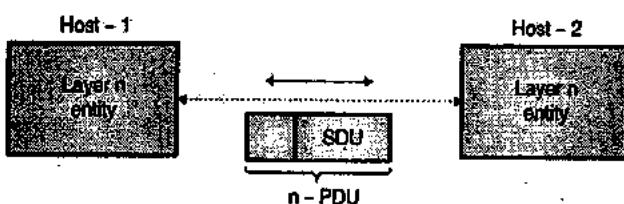
- An IDU consists of two parts namely SDU (Service Data Unit) and ICI (Interface Control Information).

1.16.5 Service Data Unit (SDU) :

- SDU is a part of IDU. The SDU is the information passed across the network to the peer entity and then upto layer (n + 1).
- ICI contains the control information which is necessary to help the lower layer (n) to do the necessary job.

1.16.6 Protocol Data Unit (PDU) :

- In order to transfer the SDU, the layer (n) entity has to divide it into many smaller pieces.
- Each piece is given a header and sent as a separate PDU (Protocol Data Unit) such as a packet.



(G-58) Fig. 1.16.3 : Layer (n) entities exchange n-PDUs in their layer (n) protocol

- The PDU headers are used by the peer entities to carry out their peer protocol.
- Some PDUs contain data while other PDUs contain the control information. The PDU headers will identify or differentiate between different types of PDUs.
- They also provide sequence numbers and counts.

1.17 Connection Oriented and Connectionless Services :

- Any layers can offer two types of services to the layer above it :
 - Connection oriented service
 - Connectionless service.

1.17.1 Connection Oriented Service :

SPPU : May 08

University Questions

- Q. 1 Explain connection oriented service in details. What are the principle differences between connectionless communication and connection oriented communication ?
(May 08, 8 Marks)

- The connection oriented service is similar to the one provided in the telephone system.
- The service users of the connection oriented service undergo the following sequence of operation :
 - Establish a connection.
 - Use the connection.
 - Release the connection.
- The connection acts like a tube. The sender pushes bits from one end of the tube and the receiver takes them out from the other end.
- The order is generally preserved. That means the order in which the bits are sent is same as the order in which they are received.
- Sometimes after establishing a connection, the sender and receiver can discuss and negotiate about parameters to be used such as maximum message size, quality of service and some other issues.

1.17.2 Connectionless Service :

- The connectionless service is similar to the postal service.
- Each message (analogous to a letter) carries the full address of the destination. Each message is routed independently from source to destination through the system.
- It is possible that the order in which the messages are sent and the order in which they are received may be different.

1.17.3 Comparison of Connection Oriented and Connectionless Services :

SPPU : May 08, May 11

University Questions

- Q. 1 Explain connection oriented service in details. What are the principle differences between connectionless communication and connection oriented communication ?
(May 08, 8 Marks)

- Q. 2 What is the principle difference between connection oriented and connectionless communication ?
(May 11, 8 Marks)

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

- One more type of service is the request-reply service. In this type, the sender transmits a single datagram which contains a request and the receiver send a reply to it.
- Table 1.17.1 lists various types of services and their examples.

Table 1.17.1 : Six different types of services

Sr. No.	Service	Type	Example
1.	Reliable message stream.	Connection oriented	Sequence of pages.
2.	Reliable byte stream.	Connection oriented	Remote login.
3.	Unreliable connection.	Connection oriented	Digitized voice.
4.	Unreliable datagram.	Connectionless	Electronic mail.
5.	Acknowledged datagram.	Connectionless	Registered e-mail.
6.	Request-Reply.	Connectionless	Database query.

- The unreliable service is used only if the reliable service is not available or is too costly to afford.

1.17.4 Quality of Service (QoS) :

- Each service can be judged by its quality of service.
- Services can be of two types :
 1. Reliable
 2. Unreliable.
- Reliable services are those which never lose data. In the reliable services a receiver sends acknowledgements of the received messages to the sender.
- But due to acknowledgements the overheads and delays increase which are sometimes undesirable.
- Applications such as electronic mail do not require any connections. The cost associated, complexity and overheads of reliable services is not required here.
- Such applications require high reliability of message arrival but no guarantee i.e. unreliable service will be acceptable for this application.
- The services in which acknowledgements are not sent to sender are unreliable connectionless services. Such services are called as datagram service which is similar to telegram service.
- However note that acknowledged datagram service can also be provided.

1.17.5 Service Primitives :

- Primitive means operation. A service is specified by a set of primitives i.e. a set of operations. A user process can access these primitives to access the service.
- Primitives of connection oriented service are different from those of connectionless service.
- The service primitives required for implementation of a reliable byte stream in a client server environment are given in Table 1.17.2.

Table 1.17.2 : Service primitives

Sr. No.	Name	Meaning
1.	LISTEN	Block waiting for an incoming connection
2.	CONNECT	Establish a connection
3.	RECEIVE	Block waits for a message
4.	SEND	Send the message
5.	DISCONNCT	Terminate the connection



1.18 Relationship of Services to Protocols :

- Services and protocols are two completely different concepts and should not be mixed up.

1.18.1 Service :

- It is defined as a set of operations that a layer can provide to the layer above it.
- A service defines or states the operations a layer is ready to perform. But it does not say anything about how these operations would be implemented.

1.18.2 Protocol :

- A protocol is a set of rules. The format and meaning of frames, packets or messages that are being sent and received by the communicating peer entities is governed by the protocols.
- The entities use protocols so as to implement their services. Once their predecided services are ensured, they are free to change the protocol.

1.19 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.

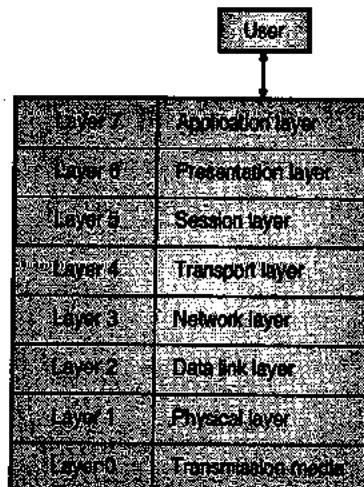
1.20 OSI Model :

SPPU : May 06, May 08, Dec. 08

University Questions

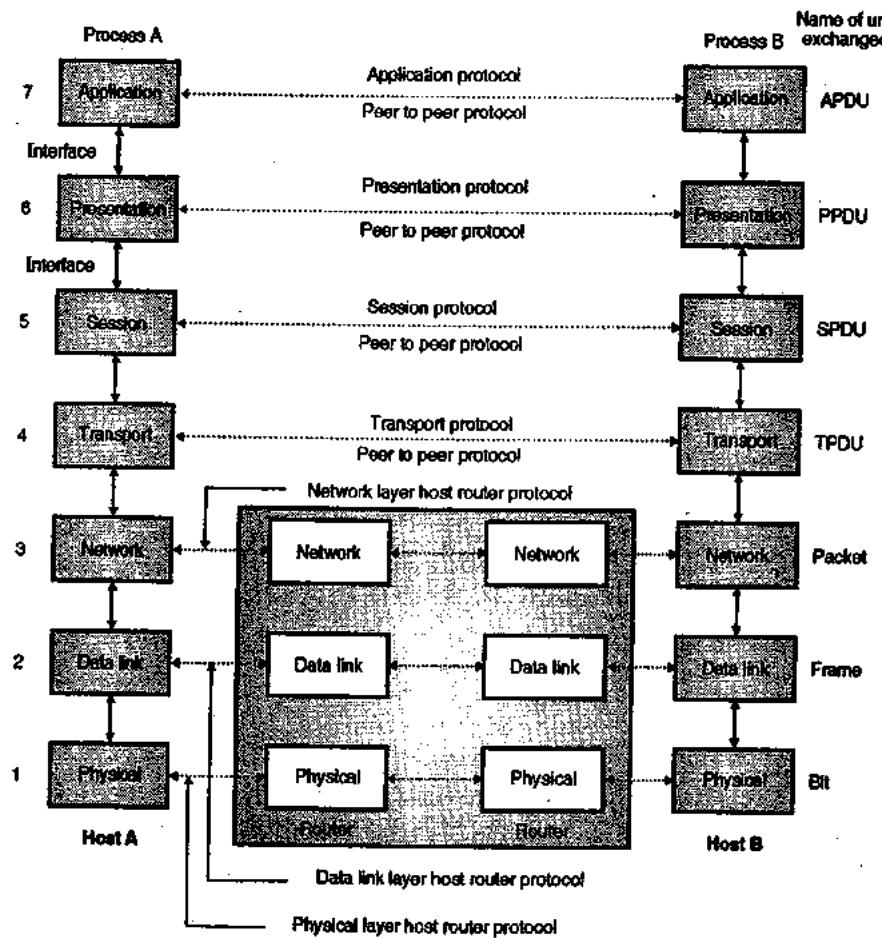
- Q. 1 Explain the OSI Reference model ?** (May 06, 8 Marks)
- Q. 2 What is OSI model ? Explain the functions of different layers in OSI model.** (May 08, 8 Marks)
- Q. 3 What OSI model defines about network devices, transmission media, network transmission and data flow?** (Dec. 08, 8 Marks)

- 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".



(G-59) Fig. 1.20.1 : A seven layer ISO-OSI reference model

- Fig. 1.20.1 shows the seven layer architecture of 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.
- A more detailed OSI reference model is shown in Fig. 1.20.2.



(G-6) Fig. 1.20.2 : The OSI reference model

- The OSI model shown in Fig. 1.20.2 does not contain the physical medium.
- This model is based on a proposal developed by the International Standards Organization (ISO).
- It is called as ISO-OSI (Open System Interconnection) reference model because it is designed to deal with open systems i.e. the systems which are open for communication with other systems.
- Table 1.20.1 shows various layers and its functions.

Table 1.20.1 : 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.

Level	Name of the Layer	Functions
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	Re-transferring files of information, LOGIN, password checking etc.

- All the applications need not use all the seven layers shown in Fig. 1.20.1.
- 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.

1.20.1 Functions of Different Layers :

SPPU : May 08, Dec. 09

University Questions

- Q.1** What is OSI model? Explain the functions of different layers in OSI model. (May 08, 8 Marks)
- Q.2** Which of the OSI layer handle each of the following?
- Dividing the transmitted bit stream into frames
 - Determine which route through the subnet to use. (Dec. 09, 8 Marks)

Layer 1 : The physical layer :

Functions of the physical layer are as follows :

- To activate, maintain and deactivate the physical connection.
- To define voltages and data rates needed for transmission.
- To convert the digital data bits into electrical signal.
- To decide whether the transmission is simplex, half duplex or full duplex.
- A physical layer does not perform the following operations :
 - It does not detect or correct errors.
 - 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 :

- To route the signals through various channels to the other end.
- To act as the network controller by deciding which route data should take.
- 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 :

- It decides if the data transmission should take place on parallel paths or single path.
- It does the functions such as multiplexing, splitting or segmenting on the data.
- Transport layer guarantees transmission of data from one end to the other.
- 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 :

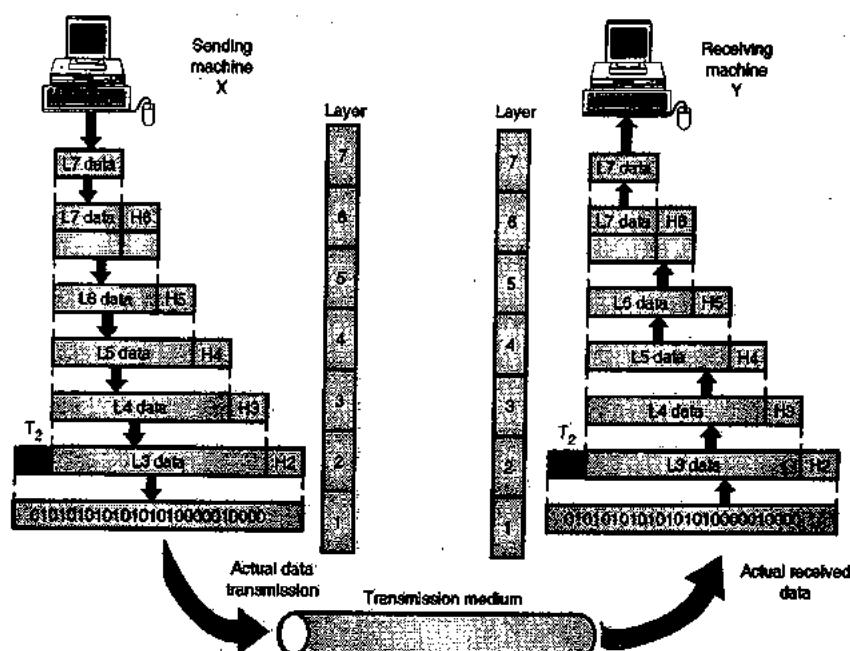
- Application layer is at the top of all as shown in Fig. 1.20.1. It provides different services such as manipulation of information in various ways, re-transferring the files of information, distributing the results etc. to the user who is sitting above this layer.
- The functions such as LOGIN, or password checking are also performed by the application layer.
- Let us now go into the details of each and every layer.

1.20.2 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. 1.20.3.
- 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.



(G-6) Fig. 1.20.3 : An exchange using the OSI model

1.20.3 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. 1.20.4.

Following are the functions of the physical layer :

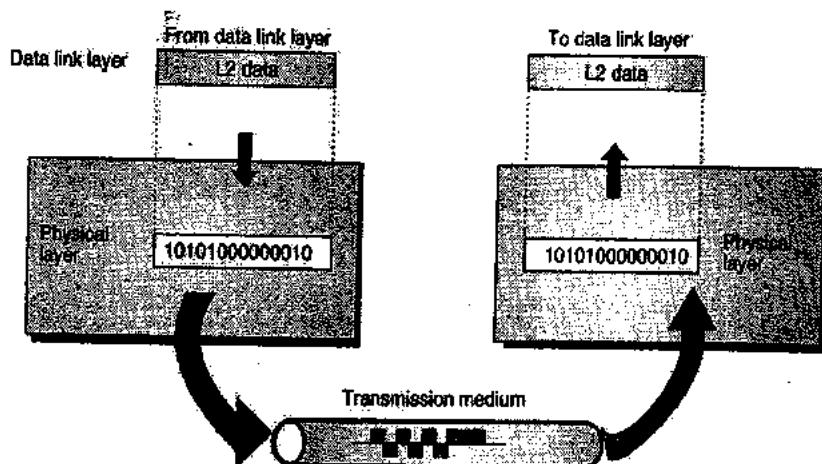
- To define the type of encoding i.e. how 0's and 1's are changed to signals.
- To define the transmission rate i.e. the number of bits transmitted per second.
- To deal with the synchronization of the transmitter and receiver.

- To deal with network connection types, including multipoint and point-to-point connections.
- To deal with physical topologies i.e. bus, star, ring, or mesh.
- To deal with the media bandwidth i.e. baseband and broadband transmission.
- Multiplexing which deals with combining several data channels into one.
- To define the characteristics between the device and the transmission medium.
- To define the transmission mode between two devices i.e. whether it should be simplex, half duplex or full duplex.

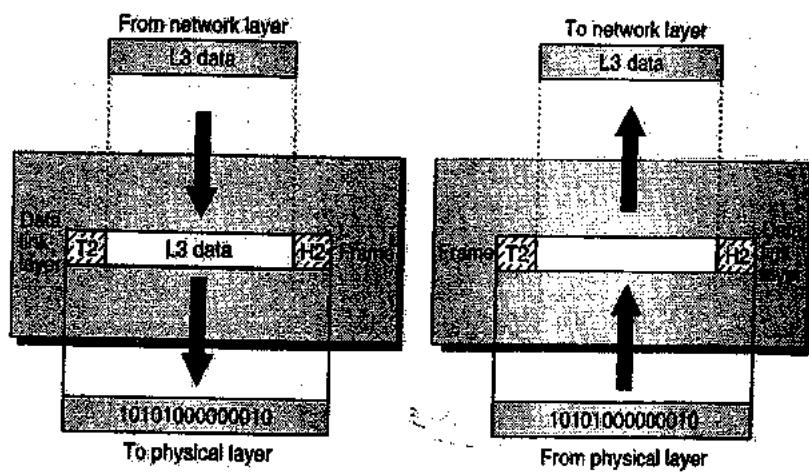
Note : Passive hubs, simple active hubs, terminators, couplers, cable and cabling, connectors, repeaters, multiplexers, transmitters, receivers, transceivers are associated with the physical layer.

1.20.4 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. 1.20.5.



(G-62) Fig. 1.20.4 : Physical layer



(G-63) Fig. 1.20.5 : Data link layer



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 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) :

It establishes and maintains links between the communicating devices.

2. Media Access Control (MAC) :

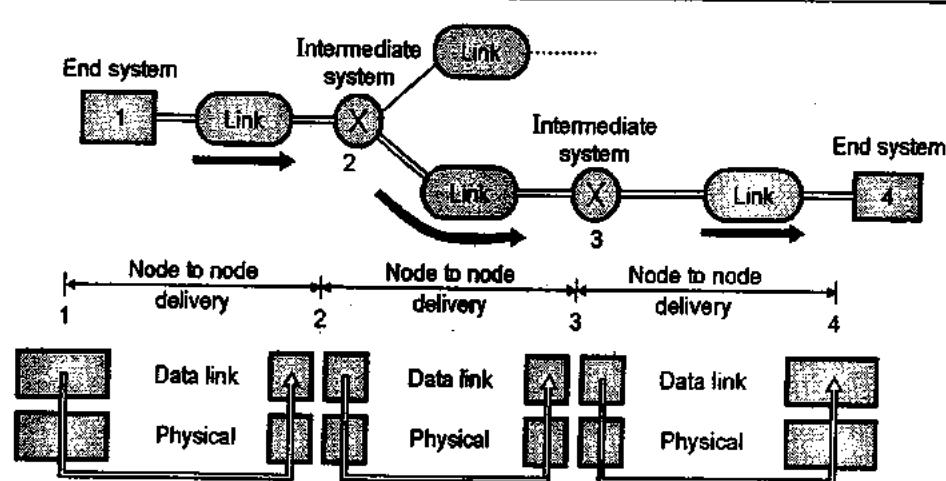
- It controls the way multiple devices share the same media channel.
- The logical link control sub-layer provides Service Access Points (SAPs) that the other

computers can refer to and use to transfer information from LLC to the network layer.

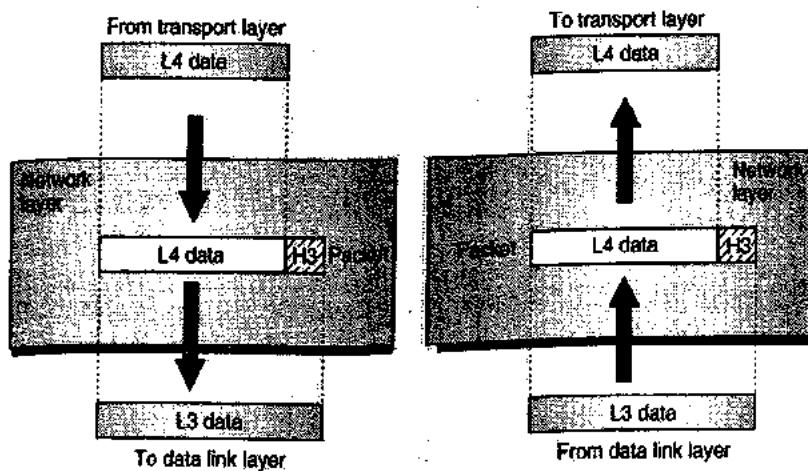
- The MAC sub-layer provides for shared access to the network adapter and communicates directly with the network interface cards.
- Network interface cards (NIC) have a unique 12-digit hexadecimal MAC address assigned before they leave the factory where they are manufactured.
- The MAC addresses are 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. 1.20.6 shows the node delivery by the data link layer.
- Fig. 1.20.6 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.

1.20.5 Network Layer :

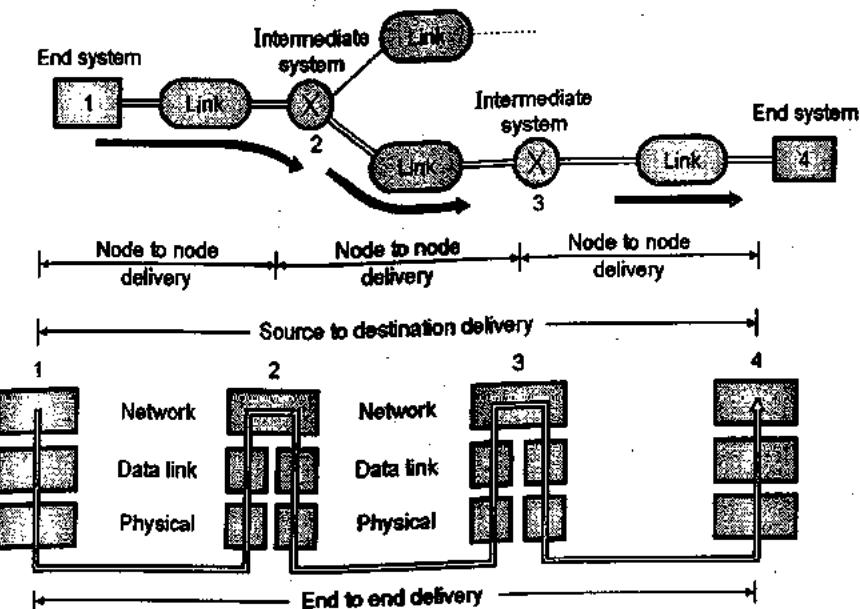
- The main function of this layer is to deliver packets from source to destination across multiple networks (links).
- If two systems are connected on the same link, then the network layer may not be needed.
- The relationship of the network layer to the data link and transport layer is shown in Fig. 1.20.7.



(G-60) Fig. 1.20.6 : Node to node delivery



(G-65) Fig. 1.20.7 : Network layer



(G-66) Fig. 1.20.8 : End to end delivery

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. 1.20.8.
 - 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 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.

1.20.6 Transport Layer :

- The function of the transport layer is the process to process delivery of 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. 1.20.9 shows the relationship of the transport layer to the network layer and session layer.

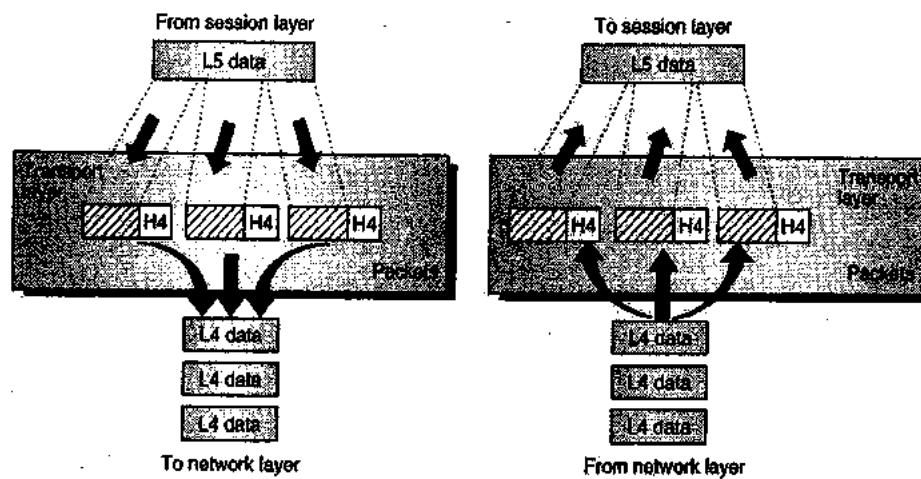
Functions of transport layer :

The transport layer performs the following functions :

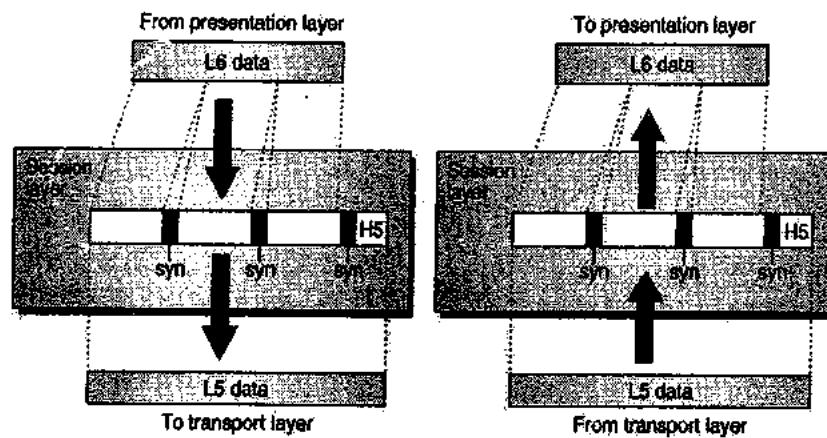
1. It divides each message into packets at the source and re-assembles them at the destination.
2. The transport layer header H4 includes a service point address to deliver a specific process from source to a specific process at the destination.
3. The transport layer is capable of either connectionless 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.

1.20.7 The Session Layer :

- The main functions of this layer are to establish, maintain and synchronise the communication between interested systems.
- Fig. 1.20.10 shows the relationship of the session layer to the transport layer and the presentation layer.



(G-67) Fig. 1.20.9 : Transport layer



(G-68) Fig. 1.20.10 : Session 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 :

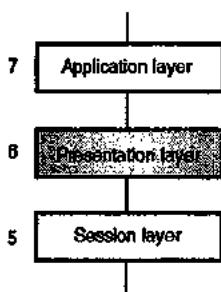
Dialog control is the means by which a sending and receiving systems initiate a dialog, exchange messages and finally end the dialog.

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.

1.20.8 Presentation Layer :

- The presentation layer is the 6th layer the OSI model as shown in Fig. 1.20.11.
- Above it there is the application layer and below it there is the sessions layer.



(G-707) Fig. 1.20.11 : Position of presentation 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 :

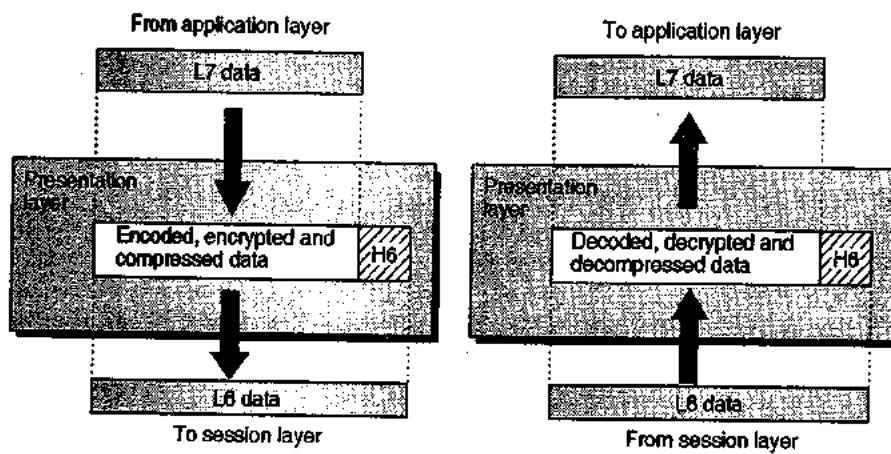
- For ensuring the security and privacy of the information that is being communicated, a process called data encryption is essential.
- Encryption is carried out at the sending end. In the encryption process, the sender transforms the original information to another form, and sends the transformed information.
- 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 :

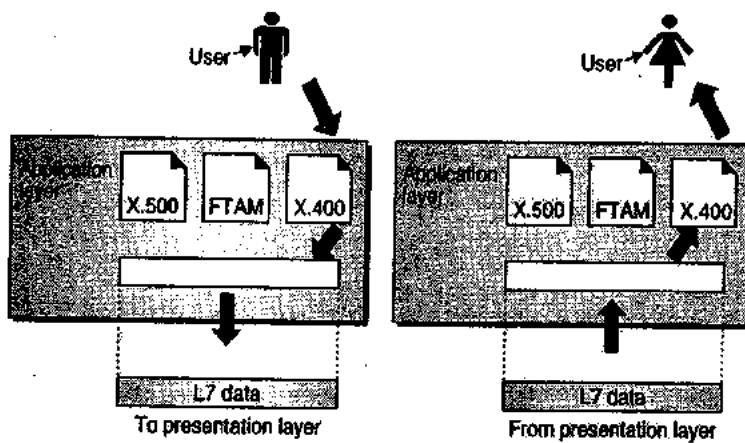
- The data compression technique is used for reducing the number of bits required to send an information.
- Data compression is essential for transmission of multimedia such as text, audio and video.

Relation with application and session layers :

- The main function of the presentation layer takes care of the syntax and semantics of the data exchanged between two communication systems.
- The relation of presentation layer with the application layer and session layer is illustrated in Fig. 1.20.12.



(G-69) Fig. 1.20.12 : Relation of presentation layer with the application layer and session layer



(G-70) Fig. 1.20.13 : 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).

1.20.9 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. 1.20.13.

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.



1.20.10 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.

1.20.11 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.

1.21 The TCP/IP Reference Model :

SPPU : May 07, Dec. 11

University Questions

- Q.1** Explain TCP/IP Model and compare TCP/IP and OSI Model. (May 07, 8 Marks)
Q.2 Consider you are accessing a web page. Explain what different things happen at client and server side at each layer. Assume that both are using TCP/IP protocol stack. (Dec. 11, 8 Marks)

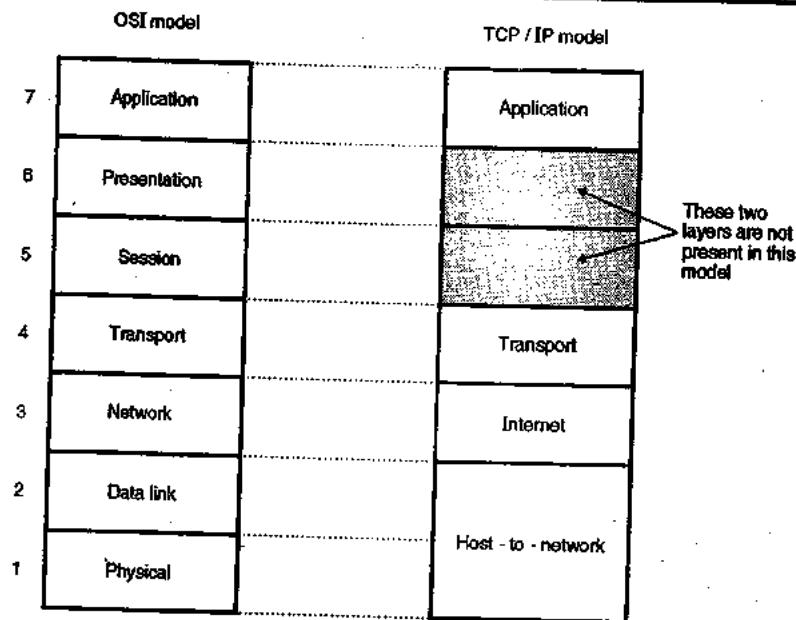
- This is the other reference model which was used earlier by ARPANET and then it is being used in the Internet.
- TCP/IP is a short form of transmission control protocol and internet protocol.
- ARPANET was a research network sponsored by the U.S. department of Defence.
- It included many universities and government installations using the leased telephone lines. Later on the satellites and radio networks were added to it.
- This inclusion could not be handled by the existing protocols at that time. So a new reference architecture was needed.
- This new architecture is known as TCP/IP reference model due to the use of the two protocols TCP and IP.
- While designing the new model certain goals were to be achieved. Some of them were as follows :
 1. First design goal was to have an ability to connect multiple networks together in a seamless way.
 2. Another goal was that the network should be able to survive loss of subnet hardware with existing conversation not being broken.
 3. Next, a flexible architecture was needed to deal successfully with the divergent requirements of various applications.

1.21.1 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.
- Since the development of the ARPANET, 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.

1.21.2 Overview of TCP/IP Architecture :

- 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.
- ARPA originally created TCP/IP 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 diverse networks.



(G-71) Fig. 1.21.1 : TCP/IP reference model

- 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. 1.21.1 shows the TCP/IP reference model along with the OSI model used for comparison.

1.21.3 Description of TCP/IP Model :

As shown in Fig. 1.21.1, the TCP/IP model has only four layers.

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. 1.21.1.

Transport layer :

- This is the layer above the internet layer. Its functions are same as those of a transport layer in OSI layer.
- 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. 1.21.2.
- Many other protocols have been added to these, over the years such as Domain Name Service (DNS), NNTP and HTTP etc.



Application layer	TELNET, FTP, SMTP, DNS, HTTP, NNTP
Transport	TCP UDP
Internet (Network)	IP
Host-to-network	ARPANET, SATNET LAN, packet radio

Fig. 1.21.2

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.

1.21.4 Comparison of OSI and TCP/IP Models :

SPPU : Dec. 06, May 07, Dec. 07, May 09, Dec. 09

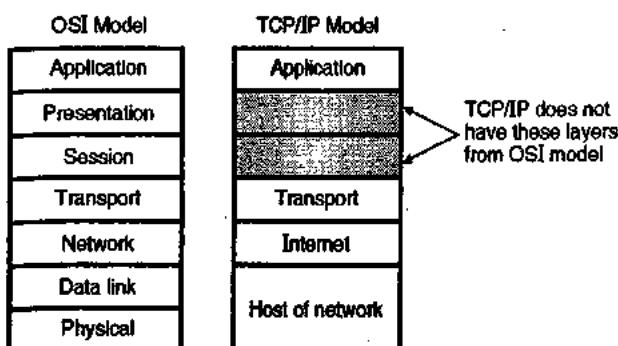
University Questions

- Q. 1** Compare TCP/IP and OSI reference model. (Dec. 06, Dec. 09, 8 Marks)
- Q. 2** Explain TCP/IP Model and compare TCP/IP and OSI Model. (May 07, 8 Marks)
- Q. 3** List two ways in which the OSI and TCP/IP reference model are the same. Now list two ways in which they differ from each other. (Dec. 07, May 09, 8 Marks)

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. 1.21.3 and Table 1.21.1 for the comparison of the two reference models.



(G-73) Fig. 1.21.3 : Relationship between OSI and TCP/IP models

Table 1.21.1 : Difference between OSI and TCP/IP model

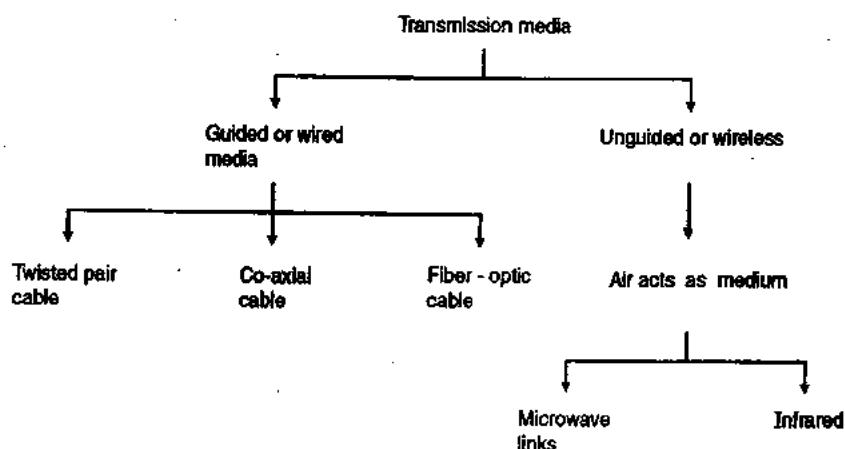
OSI	TCP/IP
Has 7 layers	Has 4 layers
Transport layer guarantees delivery of packets.	Transport layer does not guarantee delivery of packets.
Horizontal approach.	Vertical approach.
Separate session layer.	No session layer, characteristics are provided by transport layer.
Separate presentation layer.	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.

1.22 Transmission Media :

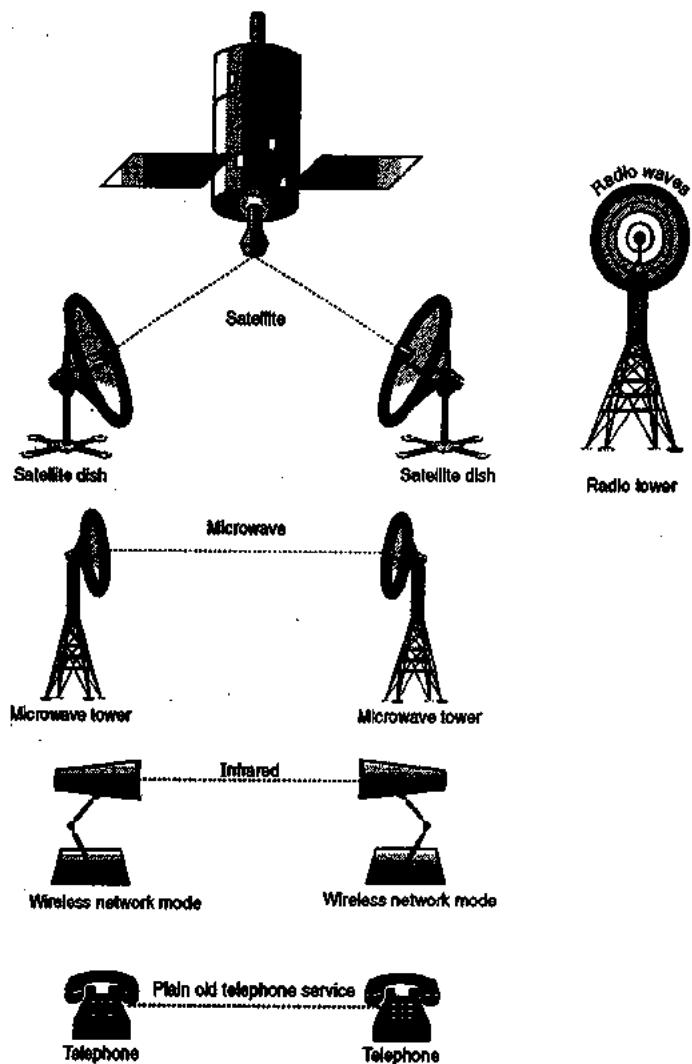
- Media are what the message is transmitted over. In other words a communication channel is also called as a medium.
- Different media have different properties and used in different environments for different purposes.
- The purpose of the physical layer is to transport a raw bit stream from one computer to another.

1.22.1 Classification of Transmission Media :

- We can classify the transmission media as shown in Fig. 1.22.1 into two categories.
- Media are roughly grouped into two classes :
 1. Guided media 2. Unguided media
- 1. **Guided media** : Guided media is a communication medium which allows the data to get guided along it. For this the media need to have a point to point physical connection.
- 2. **Unguided media** : The wireless media is also called as an unguided media.



(L-57) Fig. 1.22.1 : Classification of transmission media



(L-57) Fig. 1.22.2 : Transmission medias

- The examples of guided media are copper wires and fiber-optics, whereas radio and lasers through the air are examples of unguided media as shown in Fig. 1.22.2.

1.22.2 Comparison of Wired and Wireless Media :

Comparison of wired and wireless media is given in Table 1.22.1.



Table 1.22.1 : Comparison of wired and wireless media

Sr. No.	Wired media	Wireless media
1.	The signal energy is contained and guided within a solid medium.	The signal energy propagates in the form of unguided electromagnetic waves.
2.	Twisted pair wires, coaxial cable, optical fiber cables are the examples of wired media	Radio and infrared light are the examples of wireless media.
3.	Used for point to point communication.	Used for radio broadcasting in all directions.
4.	Wired media lead to discrete network topologies.	Wireless media leads to continuous network topologies.
5.	Additional transmission capacity can be procured by adding more wires.	It is not possible procure additional capacity.
6.	Installation is costly, time consuming and complicated.	Installation needs less time and money.
7.	Attenuation depends exponentially on the distance.	Attenuation is proportional to square of the distance.

1.22.3 Types of Wired Media :

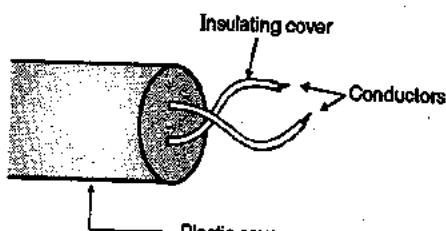
The most commonly used networking media are :

1. Co-axial cable
2. Twisted pair cable
3. Optical fiber cable.

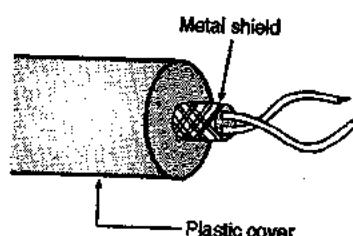
The selection of networking media depends on various factors such as cost, connectivity, bandwidth, performance in presence of noise, geographical coverage etc.

1.23 Twisted Pair Cables :

- The construction of twisted pair cable is as shown in Fig. 1.23.1. This is a very commonly used medium and it is cheaper than the co-axial cable or optical fiber cable.
- The construction of twisted pair cable is as shown in Fig. 1.23.1. This is a very commonly used medium and it is cheaper than the co-axial cable or optical fiber cable.
- Twisted pairs can be used for either analog or digital transmission. The bandwidth supported by the wire depends on the thickness of the wire and the distance to be travelled by a signal on it.
- Twisted pairs support several megabits/sec for a few kilometres and are less costly.



(a) UTP



(b) STP

(a-s74) Fig. 1.23.1 : Construction of twisted pair cables

1.23.1 Types of Twisted Pair Cables :

- The two commonly used types of twisted pair cables are as follows :
 1. Unshielded Twisted Pair (UTP)
 2. Shielded Twisted Pair (STP)
- The construction of UTP and STP cables is shown in Fig. 1.23.1.

UTP :

- A twisted pair consists of two insulated conductors twisted together in the shape of a spiral as shown in Fig. 1.23.1. It can be shielded or unshielded.
- The unshielded twisted pair cables are very cheap and easy to install. But they are badly affected by the electromagnetic noise interference.

STP :

- STP cable as shown in Fig. 1.23.1(b) has a metal foil or braided mesh included in order to cover each pair of twisted insulating conductors.
- This is known as the metal shield which is normally connected to ground so as to reduce the interference of the noise. But this makes the cable bulky and expensive.
- So practically UTP is more used than STP. The STP was developed by IBM and is used primarily for the IBM company only.
- Applications of the twisted pair cables are in point to point and point to multipoint communications, telephone systems etc.

- Twisted pairs support several megabits/sec for a few kilometres and are less costly.



Why to twist the wires ?

- Twisting of wires will reduce the effect of noise or external interference. The induced emf into the two wires due to interference tends to cancel each other due to twisting.
- Number of twists per unit length will determine the quality of cable. More twists means better quality.

1.23.2 Categories (Cat) of UTP :

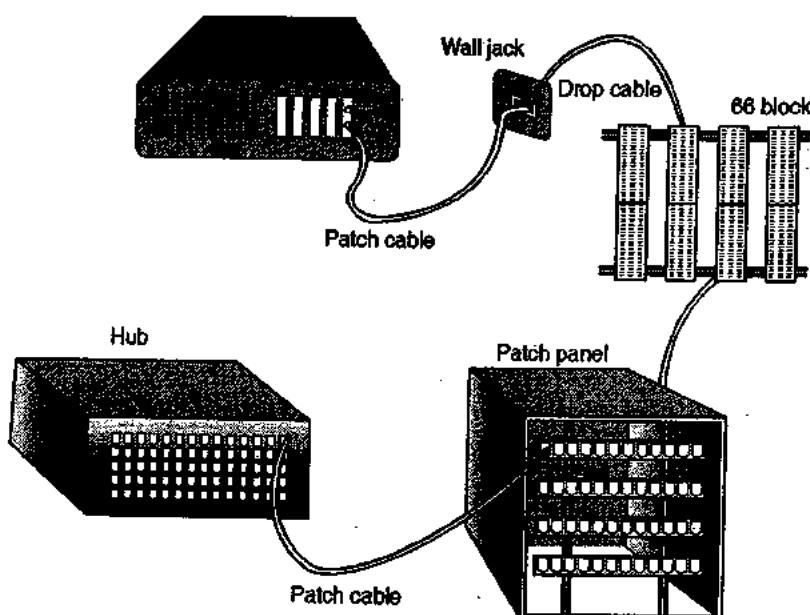
- Table 1.23.1 shows various categories of the unshielded twisted pair cables.
- These categories are decided by EIA i.e. electronic industries association. Different category cables are used for different applications.

Table 1.23.1 : Categories of UTP cables

Category	Data rate	Bandwidth	Application
1.	Extremely low upto 100 kbps	Low	Analog applications, telephony.
2.	Moderate upto 2 Mbps.	Moderate upto 2 MHz.	Analog and digital telephony

Category	Data rate	Bandwidth	Application
3.	Upto 10 Mbps	Upto 10 MHz	Local Area Networks (LANs)
4.	Upto 20 Mbps	Upto 20 MHz	Local Area Networks (LANs)
5.	Upto 100 Mbps	Upto 100 MHz	Local Area Networks (LANs)
6.	Upto 200 Mbps	Upto 200 MHz	Local Area Networks (LANs)
7.	Upto 600 Mbps	Upto 600 MHz	Local Area Networks (LANs)

- These cables ensure less crosstalk and a higher quality of signal over longer distances. Therefore these cables are popularly used for high speed computer communication.
- A connection diagram using the UTP is shown in Fig. 1.23.2.



(L-575) Fig. 1.23.2 : A common UTP installation



1.23.3 Category 3 and Category 5 (Cat 3 and Cat 5) UTP Cables :

- Most office buildings have been wired with twisted pair cable for telephones which is commonly called as voice grade UTP.
- Because these cables are already in place we can use them easily as LAN medium. The disadvantage of these voice grade twisted pair cables are low data rates and limited distances.
- Hence in 1991 the EIA published a new standard called EIA-568 in order to specify the use of voice grade unshielded twisted pair as well as shielded twisted pair for the in-building data applications.
- These standards were specified for the data rates upto 16 Mbps for LAN. But in the subsequent years, the LANS became faster with a data rate upto 100 Mbps.
- Hence a new standard EIA-568 A was published in 1995. EIA-568 A defined three categories of UTP cabling as follows :
 - Category 3 :** Characteristics of UTP cables and associated connecting hardware are specified upto 16 MHz.
 - Category 4 :** Under this category, the characteristics of UTP cables and associated connecting hardware have been specified for the data rates upto 20 MHz.
 - Category 5 :** Under this category, the characteristics of UTP cables and associated connecting hardware were specified for the data rates upto 100 MHz.
- The cat 3 and cat 5 cables were the most popular cables for LAN applications. Cat 3 cables are popularly used for the office building applications.
- The data rates upto 16 Mbps can be achieved by cat-3 cables provided that it is well designed and used over a limited distance.
- Cat-5 is a data-grade cable that can be used for data rates upto 100 Mbps if the distance is limited.

1.23.4 Category 6 (Cat 6) UTP :

Construction :

- Cat 6 UTP cable consists of 4-pairs of copper conductors, i.e. total 8-conductors. The jacket is made of thermoplastic polyolefin or Fluorinated Ethylene Propylene (FEP).
- The material used for outside sheath of this cable can be of PVC, a fire retardant polyolefin or flubropolymers.
- The design and manufacturing is done by taking a lot of care. Advanced connector design is essential.
- It is the best available UTP.
- Cat-6 that can operate upto 200 MHz and further increase is possible in the near future.

1.23.5 Category 7 (Cat 7) Shielded Screen Twisted Pair (SSTP) :

Construction :

- It is also called as PiMF (Pairs in Metal Foil) SSTP of 4 pairs of 22-23 copper conductors. The jacket is made of thermoplastic polyolefin or Fluorinated Ethylene Propylene (FEP).
- A separate and improved shielding has been provided to each pair of conductors. Thus shielding has been improved.

Expected performance :

Cat-7 cable has a very large bandwidth between 6000 to 1200 MHz.

1.23.6 Applications of Twisted Pair Cables :

Some of the applications of twisted pair cables are as follows :

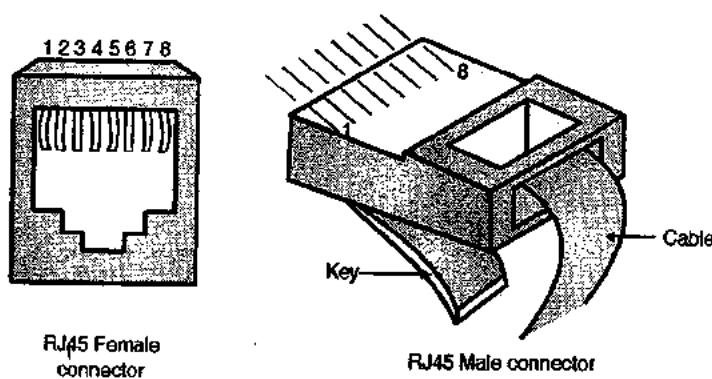
- Local area networks for connecting computers to each other.
- In the ISDN (Integrated Services Digital Network).
- In the Digital Subscriber Line (DSL).
- In the analog telephony (conventional telephone line) to carry voice and data signals.
- In digital telephony system (T_1 system)

Note :

- A modular RJ-45 telephone connector is used to connect a four-pair cable.
- A modular RJ-11 telephone connector is used to connect a two pair cable.
- Shielded twisted pair (STP) cables were introduced by IBM corporation.

1.23.7 Comparison of Twisted Pair Cables :

Specification	Category 5	UTP	SSTP
1. Bandwidth	1 – 155 Mbps (typically 10 Mbps)	1 – 155 Mbps (typically 16 Mbps)	
2. Number of nodes connected per segment		2	2
3. Attenuation	High	High	
4. Electromagnetic interference	Very high	High	
5. Ease of Installation	Easy	Fairly easy	
6. Cost	Lowest	Moderate	



(G-340) Fig. 1.23.3 : UTP RJ45 connector

1.23.8 Connectors :

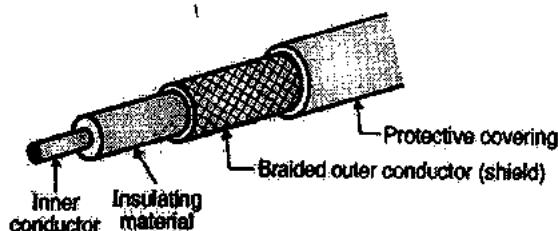
- For connecting one computer to the other, we need to use some transmission medium such as a cable.
- The cables are of different types such as twisted pair cables, coaxial cables or fiber optic cables.
- For connecting these cables between two computers we have to use connectors on both ends of a cable.
- Generally the connectors are male-female type to ensure reliable connection.

1.23.9 Connector for Twisted Pair Cable :

- The Unshielded Twisted Pair (UTP) cable is the most commonly used cable in computer communication.
- RJ45 is the most commonly used UTP where RJ is the short form of Registered Jack. It is a male-female type keyed connector as shown in Fig. 1.23.3.
- This connector can be inserted in only one way.

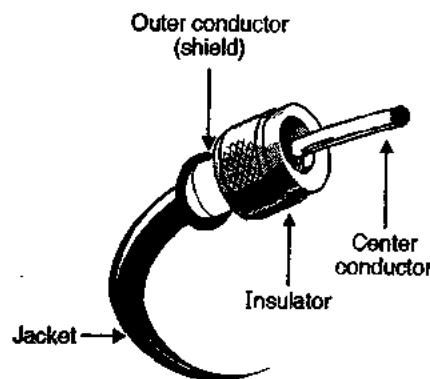
1.24 Co-axial Cables :

- The construction of co-axial cable is as shown in Fig. 1.24.1. It consists of two concentric conductors namely an inner conductor and a braided outer conductor separated by a dielectric material.
- The external conductor is in the form of metallic braid and used for the purpose of shielding. The co-axial cable may contain one or more co-axial pairs.



(L-577) Fig. 1.24.1 : Construction of a co-axial cable

- The construction of a co-axial cable with other accessories such as connector, jacket etc. is shown in Fig. 1.24.2.



(L-577) Fig. L.24.2 : Co-axial cable

- The wire mesh (braided conductor) protects the inner conductor from Electromagnetic Interference (EMI). It is often called a shield.
- A tough plastic jacket forms the cover of the cable as shown in Fig. 1.24.2 providing insulation and protection.
- The co-axial cable was initially developed for analog telephone networks. A single co-axial cable would be used to carry more than 10,000 voice channels at a time.
- The digital transmission systems using the co-axial cable were developed in 1970s. These systems operated in the range of 8.5 Mb/s to 565 Mb/s.
- The most popular application of a co-axial cable is in the cable TV system. The existing co-axial cable system has a range from 54 MHz to 500 MHz.
- Other important application is cable modem, with the cable modem termination system (CMTS).
- One more application is Ethernet LAN using the co-axial cable. The co-axial cable is used for its large bandwidth and high noise immunity.

1.24.1 Characteristics of a Co-Axial Cable :

The important characteristics of a co-axial cable are as follows :

- Two types of cables having 75Ω and 50Ω impedance are available.
- Due to the shield provided, this cable has excellent noise immunity.



- It has a large bandwidth and low losses.
- This cable is suitable for point to point or point to multipoint applications. In fact this is the most widely used medium for local area networks.
- These cables are costlier than twisted pair cables but they are cheaper than the optical fiber cables.
- It has a data rate of 10 Mbps which can be increased with the increase in diameter of the inner conductor.
- The specified maximum number of nodes is upto 100.
- The attenuation is less as compared to the twisted pair cable.
- Co-axial cables are easy to install.
- Co-axial cables are relatively inexpensive (as compared to the optical fiber cable).

1.24.2 Co-axial Cable Standards :

Table 1.24.1 shows the co-axial cable standards. The co-axial cables are categorised by their RG ratings where RG stands for Radio Government.

Table 1.24.1 : Categories of co-axial cables

Category	Impedance	Application
RG-11	50 Ω	LAN
RG 58	50 Ω	LAN
RG 59	75 Ω	Cable TV.

1.24.3 Applications of Co-axial Cables :

1. Analog telephone networks.
2. Digital telephone network.
3. Cable TV
4. Traditional Ethernet LANs
5. Digital transmission
6. Fast Ethernet

1.24.4 Baseband Co-axial Cable :

The baseband co-axial cable is the one that makes use of digital signalling. The original Ethernet scheme makes use of baseband co-axial cable.

Characteristics of baseband co-axial cable :

- The baseband co-axial cables are used to allow digital signaling for the data.
- The digital signal used for data transfer on these cables is encoded using Manchester or Differential Manchester coding.
- The digital signals need larger bandwidth. Hence the entire frequency spectrum of the cable is consumed. So it is not possible to transmit multiple channel using FDM.
- The transmission of digital signal on the cable is bi-directional.

- The baseband co-axial cable was originally used for the Ethernet system that operates at 10 Mbps.
- These cables have a characteristic impedance of 50Ω rather than 75Ω of the cable TV co-axial cables.
- The maximum length of baseband co-axial cable between two repeaters is dependent on the data rates.
- Lower the data rate longer is the cable. The length has to be reduced with increased data rates so as to reduce the probability of errors getting introduced.
- There are two baseband coaxial cable used in bus LANs namely 10 BASE 5 and 10 BASE 2 which are compared based on various factors in Table 1.24.2.

Table 1.24.2 : IEEE 802.3 specifications for 10 Mbps baseband co-axial cable Bus LAN

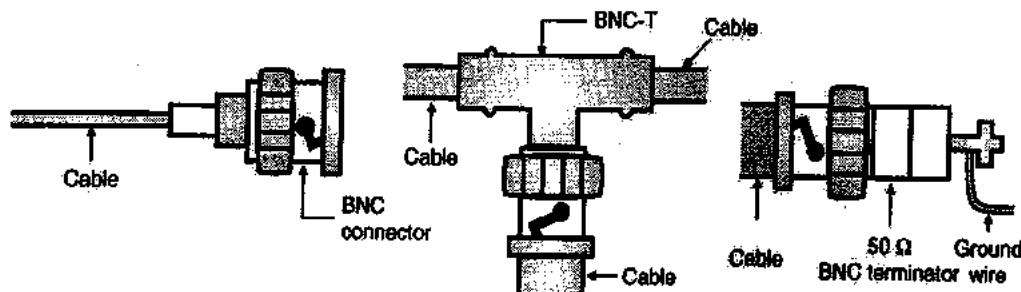
Sl. No.	Parameter	10 BASE 5	10 BASE 2
1.	Data rate	10 Mbps	10 Mbps
2.	Maximum segment length	500 m	185 m
3.	Network span	2500 m	1000 m
4.	Nodes per segment	100	30
5.	Node spacing	2.5 m	0.5 m
6.	Cable diameter	1 cm	0.5 cm

1.24.5 Broadband Co-axial Cable :

- This is the co-axial cable which is used in the cable TV system. It has higher bandwidth compared to the baseband cable.
- The type of signalling is analog at radio frequencies.
- This cable has certain disadvantages such as it is more expensive, more difficult to install and maintain as compared to the baseband co-axial cable.
- IEEE 802.3 standards have specified this as an option but practically the broadband co-axial cables are not popular.

1.24.6 Connector for Co-axial Cable :

- Coaxial cable is another important type of guided transmission media. It has higher bandwidth as compared to that of twisted pair cable.
- The coaxial cable connectors are required for connecting a coaxial cable to a computer or any other device.
- The most popular connector used for coaxial cables is the Bayonet-Neill-Concelman or BNC connectors.
- Fig. 1.24.3 shows the various types of BNC connectors. The BNC connectors are available in three different types :
 1. BNC connector
 2. BNC-T connector
 3. BNC terminator.

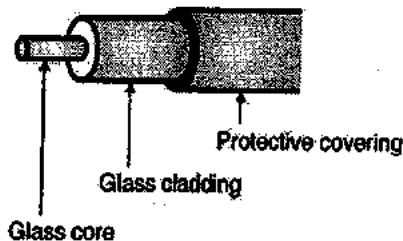


(G-34) Fig. 1.24.3 : BNC connectors of different types

1.25 Optical Fiber Cables :

Construction :

- The construction of an optical fiber cable is as shown in Fig. 1.25.1.
- It consists of an inner glass core surrounded by a glass cladding which has a lower refractive index and a protective covering.
- Digital signals are transmitted in the form of intensity - modulated light signal.



(G-16) Fig. 1.25.1 : Construction of optical fiber cable

- Light is launched into the fiber at one end using a light source such as a Light Emitting Diode (LED) or laser.
- It is detected on the other side using a photo detector such as a phototransistor or photodiode.

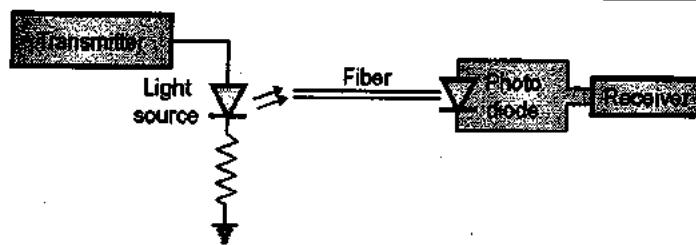
- The optical fiber cables are costlier than the other two types but they have many advantages over the other two types.

1.25.1 Light Sources for Fiber :

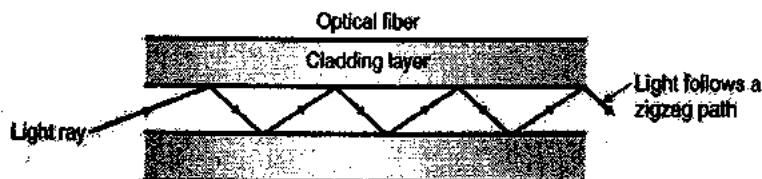
- For data transmission to take place, the sending device that is the transmitter must be capable of inducing data bits 0 to 1 into the light source. At the receiver a photodiode is used to translate this light back into data bits as shown in Fig. 1.25.2.
- The two light sources which are used popularly are :
 1. LED (Light Emitting Diode)
 2. Injection Laser Diode (ILD)
- The LED is cheaper but has a disadvantage that it provides an unfocussed light which hits the core boundaries and gets diffused.
- So LED is preferred only for short distances.
- The laser diode can provide a very focused beam which can be used for a long distance communication.

1.25.2 Principle of Light Propagation In a Fiber :

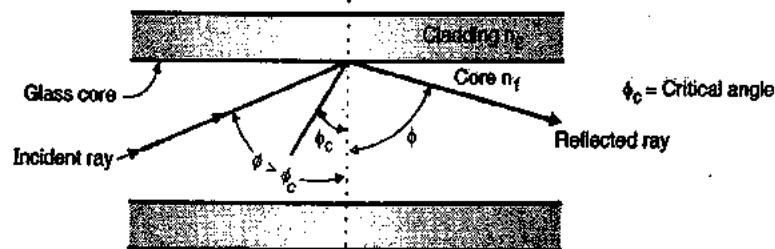
The light enters into a glass fiber from one end, and gets reflected within the fiber. It follows a zigzag path along the length of the fiber as shown in Fig. 1.25.3(a).



(G-16) Fig. 1.25.2

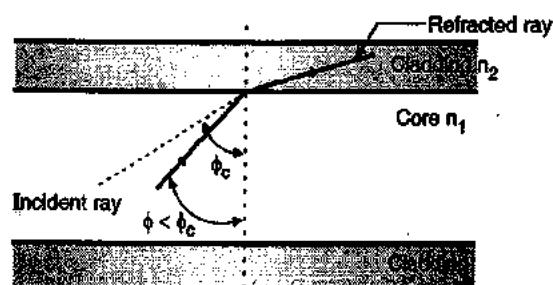
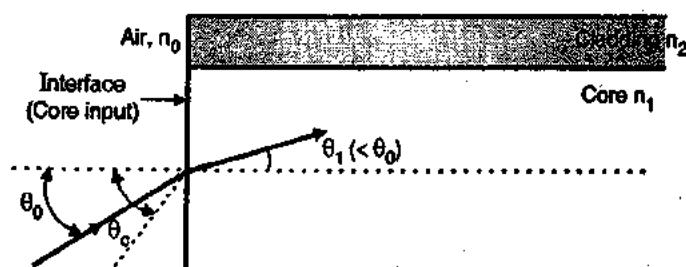


(a) Light follows a zigzag path within the optical fiber



(b) Reflection at the interface of core and cladding

(G-105) Fig. 1.25.3

(G-106) Fig. 1.25.4 : Refraction takes place at the core cladding interface if $\phi < \phi_c$ 

(G-107) Fig. 1.25.5 : Refraction at the interface

- Fig. 1.25.3(b) illustrates the principle of light travel through the optical fiber.
- When the light enters into a glass fiber from one end, most of it propagates along the length of the fiber and comes out from the far end.
- A small portion of the incident light escapes through the side walls of the fiber.
- The light which travels from one end to the other end of the glass fiber is said to have "guided" through the fiber.
- The light stays inside the fiber and does not escape through the walls because of the "total internal reflection" taking place inside the fiber.
- This total internal reflection can take place only if the following two conditions are satisfied :
 1. The glass fiber core must have a refractive index which is higher than the refractive index of the cladding around the core ($n_1 > n_2$).
 2. The angle of incidence of the light entering the fiber must be greater than the critical angle, " ϕ_c ".

$$\sin \phi_c = \frac{n_2}{n_1}$$

This is as shown in Fig. 1.25.3.

Observations from Fig. 1.25.3(b) :

Some of the important observations from Fig. 1.25.3(b) are as follows :

1. The angle of incidence (angle made by the incident ray) i.e. ϕ is greater than the critical angle ϕ_c . Therefore the incident light ray will be reflected within the core totally. The reflected ray is at same angle as that of the incident ray.
2. If the incident light makes an angle which is less than the critical angle ϕ_c then it gets refracted as shown in Fig. 1.25.4. The refracted ray enters into the cladding and gets lost.

1.25.3 Relation between Incident Angle and Emerging Angle :

Let us obtain the relation between the incident angle θ_0 and the emerging angle θ_1 by referring to Fig. 1.25.5.

- Assume that the refractive index of air is " n_0 " and that of the fiber core is " n_1 " such that $n_1 < n_0$.
- As shown in Fig. 1.25.5 the light ray enters the fiber core at an angle θ_0 , through the air-core interface. The angle θ_0 is measured between the light ray and the dotted line which is normal to the air-core interface.
- When the incident light ray enters the core of refractive index n_1 , it undergoes refraction and makes an angle θ_1 with the dotted line normal to the air-core interface as shown in Fig. 1.25.5. This angle θ_1 is called as the emerging angle.
- The relation between the incident angle θ_0 and emerging angle θ_1 is given by "Snell's relationship" which states that,

$$n_0 \sin \theta_0 = n_1 \sin \theta_1 \quad \dots(1.25.1)$$

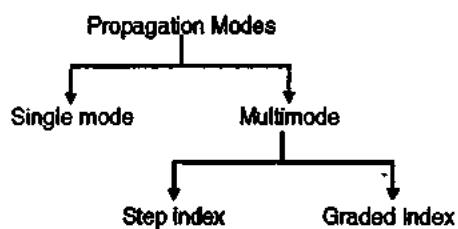
- Therefore the emerging angle θ_1 is given by,

$$\sin \theta_1 = \frac{n_0}{n_1} \sin \theta_0 \quad \dots(1.25.2)$$

- As $n_0 > n_1$, $\frac{n_0}{n_1} < 1$ therefore the emerging angle will be less than the angle of incidence θ_0 .

1.25.4 Modes of Propagation :

- The number of paths followed by light rays inside the optical cable is called as modes.
- Fig. 1.25.6 shows different modes of operation of an optical fiber.
- There are two types namely single mode and multimode fibers.

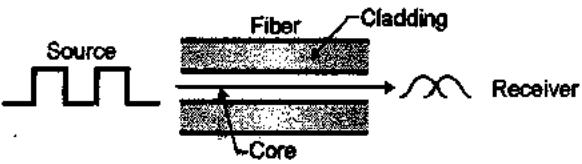


(G-108) Fig. 1.25.6 : Propagation modes in optical fibers

- In single mode light follows a single path through the core whereas in multimode, the light takes more than one paths through the core.

1.25.5 Single Mode Fibers :

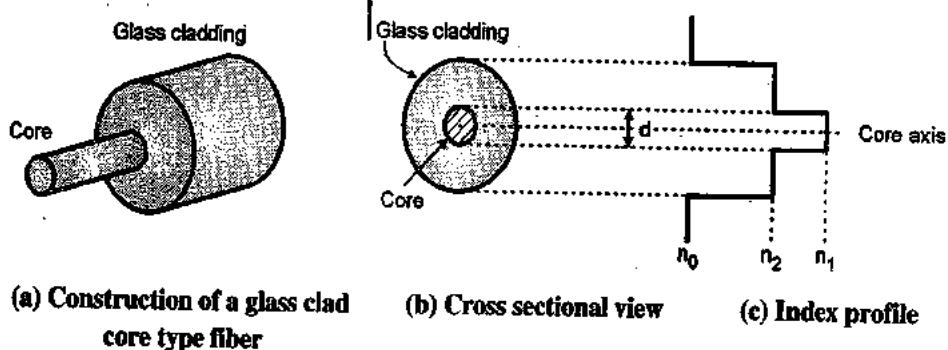
- These are called as single mode fibers because they support only one mode of propagation (TE, TM or TEM).
- The optical signal travelling inside this fiber has only one group velocity.
- Due to single mode travelling, the amount of dispersion is less than that introduced in multimode fibers.
- These fibers can have either step index or graded index profile. They are high quality fibers used for wideband long haul communication and they are fabricated from doped silica to reduce internal attenuation.
- The light travel in a single mode fiber is shown in Fig. 1.25.7. This beam travels almost horizontally and follows only one path from source to destination, as shown in Fig. 1.25.7. The critical angle of incident highly focused light beam is nearly equal to 90°.
- In the single mode fibers the delays are negligible and the signal reconstruction at the receiver is easier which results in almost no signal distortion.



(G-109) Fig. 1.25.7 : Single mode fiber

1.25.6 Multimode Fibers :

- These are called as multimode fibers because they support simultaneous propagation of many modes and the incident light follows different paths from the source to destination.
- Each mode has its own group velocity and each mode will follow its own path while travelling from the transmitter to receiver.
- Due to presence of more than one modes, the intermodal dispersion will exist.
- Multimode fibers can have the step index or graded index profile and they are fabricated using the multicomponent glasses or doped silica.

**Step index fibers :**

(G-110) Fig. 1.25.8

- The construction of an optical fiber with a core and glass cladding is as shown in Fig. 1.25.8(a).
- The refractive index of the core is n_1 and that of the glass cladding is n_2 , with $n_1 > n_2$. Therefore the index profile of glass clad core fiber is as shown in Fig. 1.25.8(c).
- Due to the sudden change in refractive index at the boundary of core and cladding, this fiber is called **step index fiber**.
- Fig. 1.25.9 illustrates the propagation of light over a step index fiber.
- Multiple beams will follow different zigzag paths as shown in Fig. 1.25.9. The number of reflections that a beam undergoes, depends on the angle of incidence of that beam.

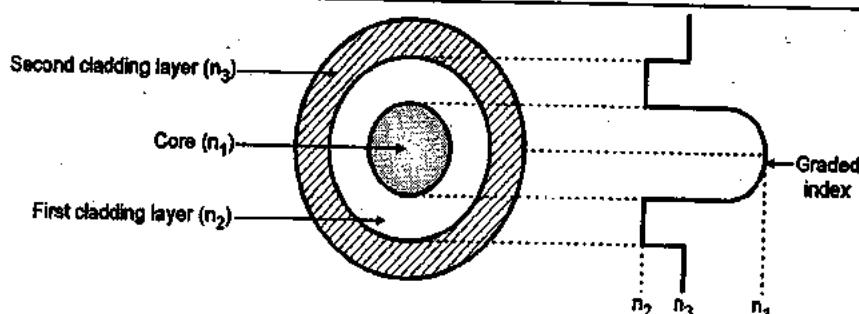


(G-111) Fig. 1.25.9 : Multimode step index fiber

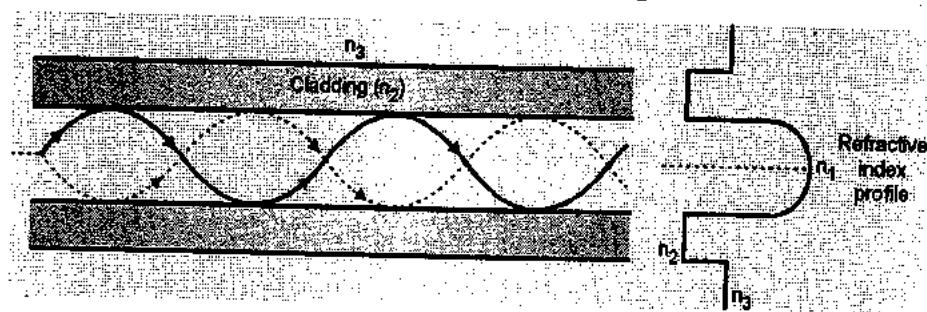
- Hence, at the destination, all the beams do not reach simultaneously. This leads to diffusion of signal at the receiver.

Graded index fibers :

- The step index multimode fibers are therefore not used for long distance communications.
- As shown in Fig. 1.25.10, the refractive index of the fiber core does not remain constant throughout its bulk.
- Instead it is maximum at the center of the core and reduces gradually towards the walls of the core. In order to get this type of index profile the material in the fiber core is modified.
- Due to the modification in the index profile, the light gets refracted inside the fiber core and does not travel in straight line as shown in Fig. 1.25.11.
- Instead the light rays are curved towards the center of the core.
- These rays have been launched into the core within the acceptance cone. The acceptance cone of a graded index core is larger than that of the step index core.
- In graded index fibers as well different beams result in different curves or waveforms.



(G-112) Fig. 1.25.10 : Refractive index profile of a graded index fiber



(G-113) Fig. 1.25.11 : Propagation of light in a graded index fiber

1.25.7 Characteristics of Optical Fiber Cables :

Fiber optic cables have the following characteristics :

1. Fiber optic cabling can provide extremely high bandwidths in the range from 100 Mbps to 2 Gbps because light has a much higher frequency than electricity.
2. The number of nodes which a fiber optic can support does not depend on its length but on the hub or hubs that connect cables together.
3. Fiber optic cable has much lower attenuation and can carry signal to longer distances without using amplifiers and repeaters in between.
4. Fiber optic cable is not affected by EMI effects and can be used in areas where high voltages are passing by.
5. The cost of fiber optic cable is more as compared to twisted pair and co-axial.
6. The installation of fiber optic cables is difficult and tedious.

Note :

- Three wavelength bands are used for fiber optic communication respectively 850 nanometer, 1300 nanometer, 1550 nanometer.
- Single mode fiber devices are more expensive and more difficult to install than multi-mode devices.
- Fiber optic cable connectors and splice (joint) attenuate the signals.
- Fiber optic cable supports 75 nodes in an Ethernet network.
- Single mode fiber optic cable are used to provide network links of several hundred kilometres in length.
- Fiber optic cable does not leak signals so it is immune to eves dropping (tapping of signals).
- Fiber optic cable does not require a ground hence it is not affected by potential shifts in the electrical ground nor does it produce static.

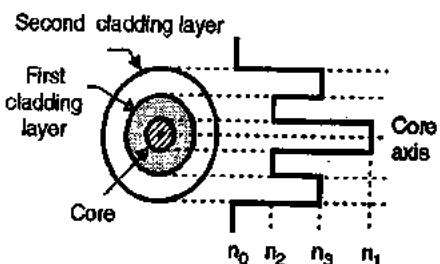
1.26 Comparisons :

1.26.1 Comparison of Step Index and Graded Index Fibers :

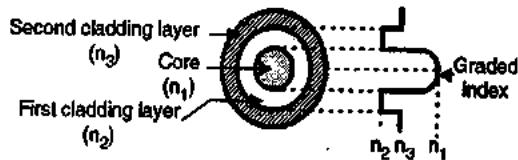
Table 1.26.1 : Comparison of step index and graded index fibers

Sr. No.	Step index fibers	Graded index fibers
1.	The refractive index changes in steps or abruptly.	The refractive index changes gradually.

Sr. No.	Step index fibers	Graded index fibers
2.	The light rays travel in straight line through the step index fibers.	The light rays do not travel in straight line through the graded index fibers.
3.	Index profile Refer Fig. A	Index profile Refer Fig. B
4.	The light rays travel in a straight line due to constant refractive index of the fiber throughout the bulk of the core.	The light rays do not travel in straight line due to the continuous refraction. This is due to the continuously changing refractive index throughout the core bulk.
5.	Acceptance cone of these fibers is smaller than that of the graded index fiber.	Acceptance cone of these fibers is larger than that of the step index fiber.



(L-595) Fig. A



(L-595) Fig. B

1.26.2 Comparison of Single Mode and Multimode Fibers :

Table 1.26.2 : Comparison of single mode and multimode fibers

Sr. No.	Single mode fiber	Multimode fiber
1.	These fibers support only one mode of propagation (TE or TM or TEM)	These fibers support the propagation of many modes.
2.	The travelling signal inside the fiber has only one group velocity.	The different modes have different group velocities and each mode will follow its own path between the transmitter and receiver.



Sr. No.	Single mode fiber	Multimode fiber
3.	The amount of dispersion introduced is less than that introduced in the multimode fibers.	The intermodal dispersion exists due to different group velocities of various modes.
4.	These fibers can have either a step index or graded index profile.	These fibers can have either step index or graded index profile.
5.	These are high quality fiber for wideband long haul transmission and are fabricated from doped silica for reducing the attenuation.	These are fabricated using the multicomponent glasses or doped silica.

1.26.3 Comparison of Optical Fiber with Coaxial and Twisted Pair Cables :

Sr. No.	Twisted pair cable	Co-axial cable	Optical fiber
1.	Transmission of signals takes place in the electrical form over the metallic conducting wires.	Transmission of signals takes place in the electrical form over the inner conductor of the cable.	Signal transmission takes place in an optical form over a glass fiber
2.	Noise immunity is low. Therefore more distortion.	Higher noise immunity than the twisted pair cable due to the presence of shielding conductor.	Highest noise immunity as the light rays are unaffected by the electrical noise.
3.	Affected due to external magnetic field.	Less affected due to external magnetic field.	Not affected by the external magnetic field.
4.	Short circuit between the two conductors is possible.	Short circuit between the two conductors is possible.	Short circuit is not possible.
5.	Cheapest	Moderately expensive	Expensive
6.	Can support low data rates.	Moderately high data rates	Very high data rates.
7.	Power loss due to	Power loss	Power loss

Sr. No.	Twisted pair cable	Co-axial cable	Optical fiber
	conduction and radiation.	due to conduction	due to absorption, scattering, dispersion and bending.
8.	Low bandwidth	Moderately high bandwidth	Very high bandwidth
9.	Node capacity per segment is 2	Node capacity per segment is 30 to 100	Node capacity per segment is 2.
10.	Attenuation is very high	Attenuation is low	Attenuation is very low.
11.	Installation is easy	Installation is fairly easy	Installation is difficult.
12.	Electromagnetic interference (EMI) can take place	EMI is reduced due to shielding	EMI is not present.

1.27 Advantages and Disadvantages of Fiber Optical Fibers :

1.27.1 Advantages of Optical Fibers :

Some of the advantages of fiber optic communication over the conventional means of communication are as follows :

- Small size and light weight :**
The size (diameter) of the optical fibers is very small (it is comparable to the diameter of human hair). Therefore a large number of optical fibers can fit into a cable of small diameter.
- Easy availability and low cost :**
The material used for the manufacturing of optical fibers is "silica glass". This material is easily available. So the optical fibers cost lower than the cables with metallic conductors.
- No electrical or electromagnetic interference :**
Since the transmission takes place in the form of light rays the signal is not affected due to any electrical or electromagnetic interference.
- Large bandwidth :**
As the light rays have a very high frequency in the GHz range, the bandwidth of the optical fiber is extremely large. This allows transmission of more number of channels. Therefore the information

carrying capacity of an optical fiber is much higher than that of a co-axial cable.

5. Other advantages :

In addition to the advantages discussed earlier, the optical fiber communication has the following other advantages :

- No cross-talk inside the optical fiber cable.
- Signals at higher data rates can be sent.
- Intermediate amplifier are not required as the transmission losses in the fiber are low.
- Ground loops are absent.
- Installation is easy as the fiber optic cables are flexible.
- These cables are not affected by the drastic environmental conditions. Because of all these advantages the optical fiber cable is replacing the conventional metallic conductor cable rapidly in many areas.

1.27.2 Disadvantages of Optical Fibers :

Some of the disadvantages of optical communication system are :

1. Sophisticated plants are required for manufacturing optical fibers.
2. The initial cost incurred is high.
3. Joining the optical fibers is a difficult job.

1.27.3 Applications :

1. Optical fiber transmission systems are widely used in the backbone of networks.
2. Optical fibers are now used in the telephone systems.

3. In the Local Area Networks (LANs).

1.28 Unguided (Wireless) Media :

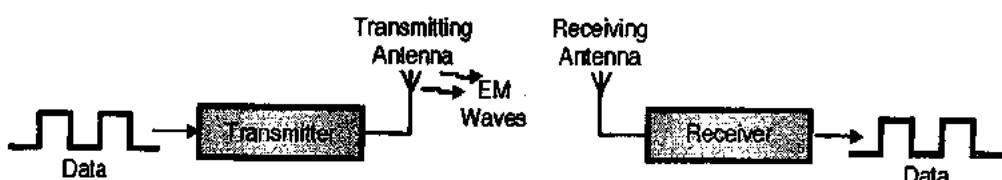
- As already defined, an unguided media (also called as wireless media) does not use a conductor or wire as a communication channel.
- Instead it uses the air or vacuum as medium to carry the information from transmitter to receiver.
- The transmitter first converts the data signal into electromagnetic waves and transmits them using a suitable antenna.
- The receiver receives them using a receiving antenna and converts the EM waves into data signal again, as shown in Fig. 1.28.1.

1.28.1 Unguided Media : Wireless :

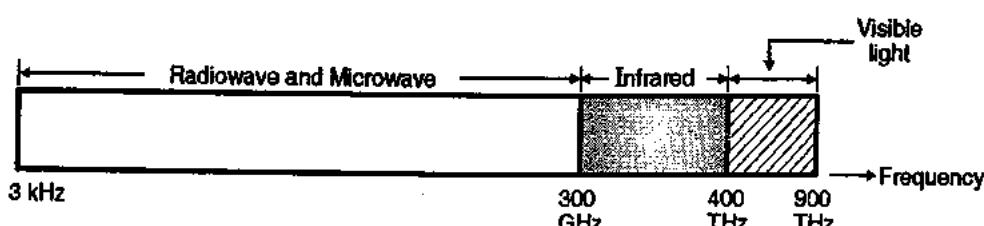
- The electromagnetic spectrum used for wireless communication is shown in Fig. 1.28.2. The signal from sender to receiver travels in the form of electromagnetic radiation through air.

Propagation methods :

- The unguided signals can travel from the transmitter to receiver in many different ways : The three most important methods are :
 1. Ground wave propagation
 2. Sky propagation.
 3. Space propagation or line of sight propagation.



(G-117) Fig. 1.28.1 : Concept of unguided media



(G-597) Fig. 1.28.2 : Electromagnetic spectrum for the wireless communication



1.28.2 Bands :

The electromagnetic spectrum is divided into several subbands. Table 1.28.1 gives various frequency bands, corresponding type of propagation and application.

Table 1.28.1 : Segments of the electromagnetic spectrum

Sr. No.	Name	Frequency	Wavelength
1.	Extremely Low Frequency (ELF)	30-300 Hz	10^7 to 10^6 m
2.	Voice Frequencies (VF)	300-3000 Hz	10^6 to 10^5 m
3.	Very Low Frequencies (VLF)	3-30 kHz	10^5 to 10^4 m
4.	Low Frequencies (LF)	30-300 kHz	10^4 to 10^3 m
5.	Medium Frequencies (MF)	300 kHz - 3 MHz	10^3 to 10^2 m
6.	High Frequencies (HF)	3-30 MHz	10^2 to 10 m
7.	Very High Frequencies (VHF)	30-300 MHz	10 to 1 m
8.	Ultra High Frequencies (UHF)	300 MHz-3GHz	1 to 10^{-1} m
9.	Super High Frequencies (SHF)	3-30 GHz	10^{-1} to 10^{-2} m
10.	Extremely High Frequencies (EHF)	30-300 GHz	10^{-2} to 10^{-3} m
11.	Infrared	-	0.7 to 10 μ m
12.	Visible light	-	0.4 μ m to 0.8 μ m

1.28.3 EM Spectrum and Communication Applications :

- In the radio communication system the frequencies ranging from a few kilohertz to many gigahertz all are being used for various purposes.
- Let us see the applications of various frequency bands.
- The frequencies most commonly used in early days were from about 300 kHz to 3 MHz and were called as Medium Frequencies (MF). The frequencies in the range 30 kHz to 300 kHz are known as the Low Frequencies (LF).

- The frequencies in the range 3 kHz to 30 kHz are called as Very Low Frequencies (VLF). On the higher frequency side High Frequencies (HF) will cover the frequency range from 3 MHz to 30 MHz. Then Very High Frequency (VHF) from 30 MHz to 300 MHz and so on.
- Table 1.28.2 gives you the details of entire usable frequency spectrum and its applications.

Table 1.28.2 : The Radio Frequency Spectrum

Sr. No.	Frequency band	Wavelength	Applications
1.	30 Hz - 300 Hz. Extremely Low Frequencies (ELF).	10^4 km to 10^3 km	Power transmission
2.	300 Hz - 3 kHz. Voice Frequencies (VF)	10^3 km to 100 km	Audio applications
3.	3 kHz - 30 kHz. Very Low Frequencies (VLF)	100 km to 10 km	Submarine communications. Navy, Military communications
4.	30 kHz - 300 kHz. Low Frequencies (LF)	10 km to 1 km. Long waves.	Aeronautical and marine, navigation, these frequencies act as sub carriers.
5.	300 kHz - 30 MHz Medium Frequencies (MF)	1 km to 100 m. Medium waves.	AM radio broadcast, Marine and aeronautical communications.
6.	3 MHz - 30 MHz High Frequencies (HF)	100 m to 10 m Short waves.	Shortwave transmission, Amateur and CB communication.
7.	30 MHz - 300 MHz Very High Frequencies (VHF)	10 m to 1 m	TV broadcasting, FM broadcasting.
8.	300 MHz - 3 GHz Ultra High Frequencies (UHF)	1 m to 10 cm. Microwaves.	UHF TV channels, Cellular phones, Military applications
9.	3 GHz - 30 GHz (SHF)	10^{-1} m to 10^{-2} m	Satellite communication and Radar
10.	30 - 300 GHz (EHF)	10^{-2} m to 10^{-3} m	Satellites and specialized radars.

1.28.4 Infrared Signals :

- The EM signals having frequencies above 300 GHz are not referred as radio waves.
- The signal occupying the range between 0.1 mm and 700 nanometers (nm) are called infrared signals.
- These are used in various special types of communications. Some of them are as follows :
 - In astronomy to detect stars and other heavenly bodies.
 - In the guided weapon systems
 - TV remote control.
 - Wireless keyboards and mouse.

- Light waves can be modulated using the signal to be transmitted and transmitted through the glass fibers in the optical fiber communication system.
- Light signals can also be transmitted through free space. Laser is a type of light, which can be easily modulated with voice, video and data information.

1.29 Network Connecting Devices :

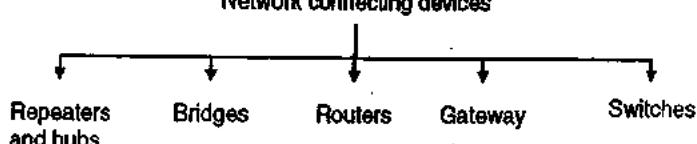
SPPU : May 11, May 12

University Questions

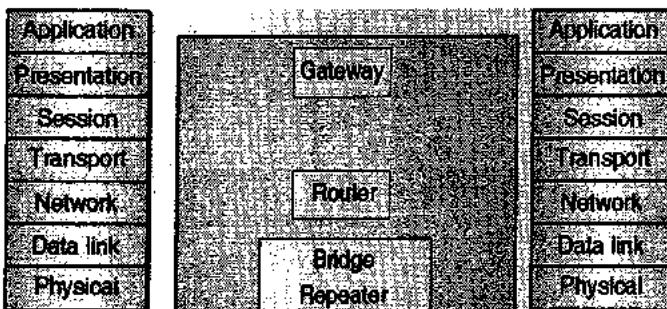
- Q. 1 List and write the use of different network connecting devices. (May 11, 8 Marks)
- Q. 2 Write short note on network hardware components. (May 12, 8 Marks)

- Different types of network connecting devices are as shown in Fig. 1.29.1.

Network connecting devices



(G-348) Fig. 1.29.1



(G-806(a)) Fig. 1.29.2 : Connecting devices and OSI model

- The relation between OSI reference model and various connecting devices is shown in Fig. 1.29.2.

Network connecting devices :

- Two or more devices are connected to each other for the purpose of sharing data or resources from a network.
- A LAN may be spread over a larger distance than its media can handle effectively. The number of stations also can be more than a number which can be handled and managed properly. Such networks should be subdivided into smaller networks and these smaller subnetworks should be connected to each other through connecting devices.
- A device called a repeater is inserted into the network to increase the coverable distance or a device called a bridge can be inserted for traffic management.
- When two or more separate networks are connected for exchanging data or resources it creates an internetwork. Routers and gateways are used for internetworking.
- Each of these device type interacts with protocols at different layers of the OSI model.
- Repeaters act only upon the electrical components of a signal and are therefore active only at the physical layer.
- Bridges utilize addressing protocols and can affect the flow control of a single LAN. Bridges are most active at the data link layer.
- Routers provide links between two separate but same type LANs and are active at the network layer.
- Finally gateways provide translation services between incompatible LANs or applications and are active in all of the layers. Connecting devices and the OSI model is shown in Fig. 1.29.2.

Categories of connecting devices :

Fig. 1.29.2 shows the relationship between the connecting devices and various layers of the internet model.

Table 1.29.1 : Role of networking devices

Sl. No.	Name of the device	Role
1.	Passive hub	Operate below the physical layer.
2.	Repeater	Regenerates the original signal. Operates in the physical layer.
3.	Bridge	Bridges utilize the address protocol. They can carry out the traffic management. They are most active in the data link layer.
4.	Routers	Routers provide connections between two separate but compatible networks. It works in the network layer.
5.	Gateways	Gateways provide translation services between incompatible networks and works in all the layers.

1.30 Hubs :

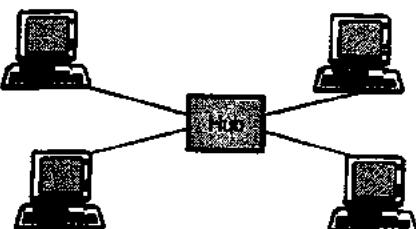
SPPU : Dec. 10, May 11, Dec. 11, Dec. 12

University Questions

- Q. 1** Write the functions of repeater, hub, NIC, media converter, transceiver, switch, router and bridge. (Dec. 10, 8 Marks)
- Q. 2** List and write the use of different network connecting devices. (May 11, 8 Marks)
- Q. 3** Describe the network components (Connectors, Hubs, Switches, Repeaters, and Bridges). (Dec. 11, 6 Marks)
- Q. 4** Write the functions of repeater, Hub, NIC, switch, router and bridge. (Dec. 12, 8 Marks)

- The general meaning of the word hub is any connecting device. But its specific meaning is multiport repeater.
- It is normally used for connecting stations in a physical star topology.
- All networks require a central location to connect various segments of media coming from various nodes.

- Such a central location is called as a hub. A hub organises the cables and relays signals to the other media segments as shown in Fig. 1.30.1.



(G-350) Fig. 1.30.1 : Hub

- There are three main types of hubs :
 - Passive hubs
 - Active hubs
 - Intelligent hubs

1.30.1 Passive Hubs :

- A passive hub simply combines the signals of a network segments. There is no signal processing or regeneration. It merely acts as a connector.
- A passive hub reduces the cabling distance by half because it does not boost the signals and in fact absorbs some of the signal.
- With a passive hub, each computer receives the signals sent from all the other computers connected to the hub.
- This type of hub is a part of communication media. Hence its location is below the physical layer.

1.31 Repeaters :

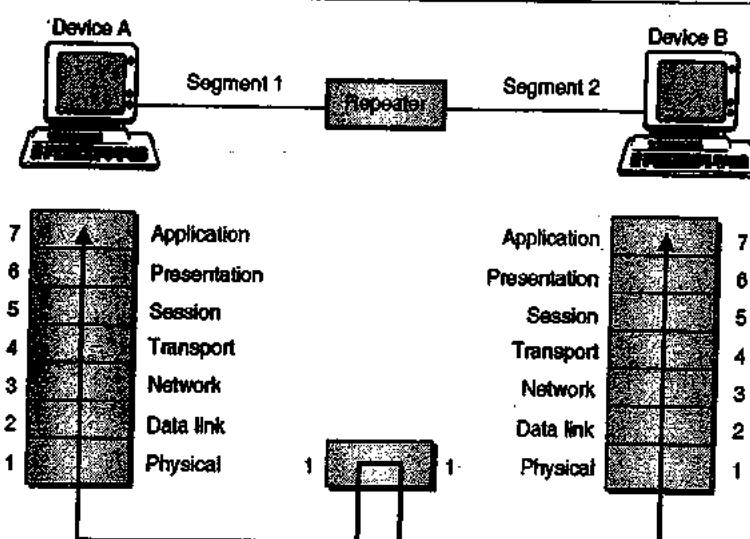
SPPU : Dec. 10, May 11, Dec. 11, Dec. 12, May 13

University Questions

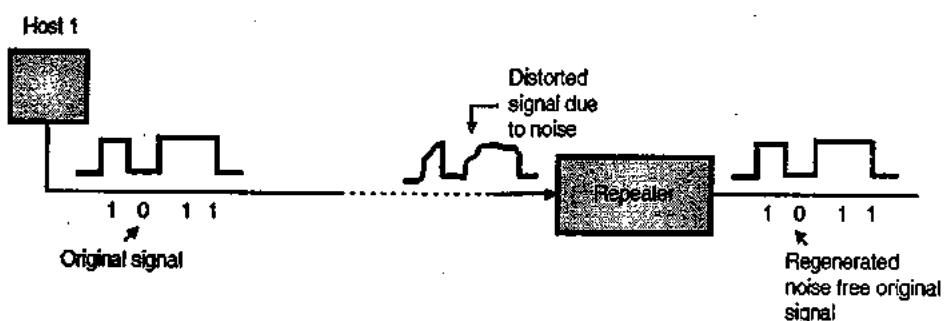
- Q. 1** Write the functions of repeater, hub, NIC, media converter, transceiver, switch, router and bridge. (Dec. 10, 8 Marks)
- Q. 2** List and write the use of different network connecting devices. (May 11, 8 Marks)

- Q. 3** Describe the network components. (Connectors, Hubs, Switches, Repeaters and Bridges). (Dec. 11, 6 Marks)
- Q. 4** Write the functions of repeater, Hub, NIC, switch, router and bridge. (Dec. 12, 8 Marks)
- Q. 5** Explain the following network components :
 1. Connectors 2. Repeaters
 3. Switches 4. Bridges. (May 13, 8 Marks)

- A repeater is a connecting device which can operate only in the physical layer.
- All transmission media weaken the electromagnetic waves that travel through them.
- Attenuation of signals limits the distance any medium can carry data. Devices that amplifies signals to ensure data transmission are called repeaters.
- A repeater receives a signal and before it gets attenuated or corrupted, regenerates the original signal.
- Thus we can use a repeater to extend the physical length of LAN as shown in Fig. 1.31.1(a).
- Repeater is not an amplifier because amplifiers simply amplify the entire incoming signal along with noise.
- Signal – regenerating repeaters create an exact duplicate of incoming data by identifying it amidst the noise, reconstructing it and retransmitting only the desired information.
- The original signal is duplicated, boosted to its original strength and sent as shown in Figs. 1.31.1(a) and (b).
- A repeater does not connect two LANs. It connects only two devices connected in the same LAN.



(G-351) Fig. 1.31.1(a) : Repeater in OSI model



(G-352) Fig. 1.31.1(b) : Function of a repeater

- It cannot connect two LANs of a different protocols.
- A repeater forwards every frame, it cannot filter out some frames and let the others pass through.
- A repeater should be placed at a precise point on the link. Such that the signal reaches it before the noise has induced an error in any of the transmitted bits.
- Fig. 1.31.1(b) illustrates the function of a repeater.
- Repeaters operate at the physical layer of the OSI model and they deal with the actual physical signals.

Advantages of repeater :

1. Repeaters can regenerate the desired information.
2. They can reduce the effect of noise.
3. They can extend the network.
4. It reduces the number of errors introduced due to noise.

Disadvantages of repeater :

1. A repeater cannot connect two LANs. It can only connect two devices connected in the same LAN.
2. It has no filtering capability.
3. Repeaters can operate only in the physical layer.
4. Repeaters must be placed at the precise point on the link so as to be effective.

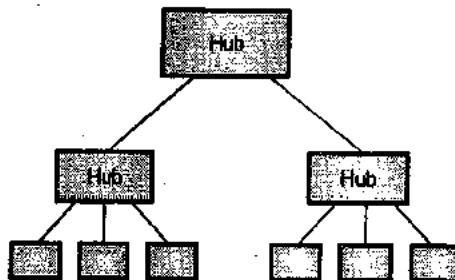
1.31.1 Active Hubs :

- They are like passive hubs but have electronic components for regeneration and amplification of signals. By using active hubs the distance between devices can be increased. An active hub is equivalent to a multipoint repeater.
- The main drawback of active hubs is that they amplify noise as well along with the signals. They are more expensive than passive hubs as well.

1.31.2 Intelligent Hubs :

- In addition to signal regeneration, intelligent hubs perform some other intelligent functions such as network management and intelligent path selection.

- A switching hub chooses only the port of the device where the signal needs to go, rather than sending the signal along all paths.
- Hubs can also be used to create multiple levels of hierarchy as shown in Fig. 1.31.2.



(L-646) Fig. 1.31.2 : Hubs to create multiple levels of hierarchy

1.32 Bridges :

SPPU : Dec. 10, May 11, Dec. 11, Dec. 12, May 13.

University Questions

- Q. 1** Write the functions of repeater, hub, NIC, media converter, transceiver, switch, router and bridge. (Dec. 10, 8 Marks)
- Q. 2** List and write the use of different network connecting devices. (May 11, 8 Marks)
- Q. 3** Describe the network components (Connectors, Hubs, Switches, Repeaters, and Bridges). (Dec. 11, 6 Marks)
- Q. 4** Write the functions of repeater, Hub, NIC, switch, router and bridge. (Dec. 12, 8 Marks)
- Q. 5** Explain the following network components
1. Connectors 2. Repeaters
3. Switches 4. Bridges. (May 13, 8 Marks)

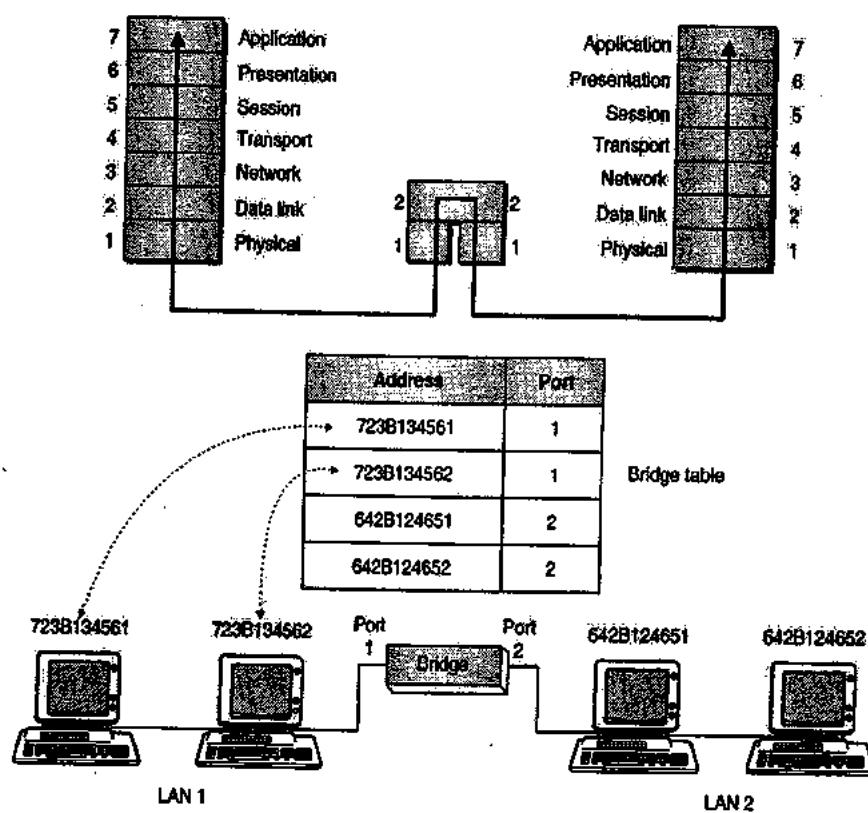
- A bridge can operate in the physical layer as well as in the data link layer of the OSI model.
- It can regenerate the signal that it receives and it can check the physical (MAC) addresses of source and destination mentioned in the header of a frame.

Filtering :

- The major difference between the bridge and repeater is that the bridge has a filtering capability. That means a bridge will check the destination address of a frame and make a decision about whether the frame should be forwarded or dropped.
- If the frame is to be forwarded, then the bridge should specify the port over which it should be forwarded.
- In order to achieve this a bridge has a table relating the addresses and ports as shown in Fig. 1.32.1.
- If a frame for 723B134561 arrives at port 2 then the bridge goes through its table and understands that the frame is to be sent out on port 1 so it will do so.
- In Fig. 1.32.1 a two port bridge is shown but in reality a bridge has more than two ports.
- It is important to note that the bridges do not change the physical address contained in the frame.

Types of bridges :

- The bridges are of two types :
 - Transparent bridges and 2. Routing bridges.
- Transparent bridge is a bridge in which the stations are not at all aware of the existence of the bridge.
- Transparent bridges keep a table of addresses in memory to determine where to send data.
- The duties of a transparent bridge are as follows :
 - Filtering frames
 - Forwarding and
 - Blocking.
- In source routing a sending station defines the bridges that should be visited by the frames.
- The addresses of these bridges are included in the frame. So a frame contains not only the source and destination address but also the bridge addresses.
- Source routing bridges are used to avoid a problem called looping. These bridges were designed for the token ring LANs. But these LANs are not very common now a days.



(L-647) Fig. 1.32.1 : Bridge and bridge table

1.32.1 Transparent Bridge :

- A transparent bridge builds its table of station addresses on its own as it performs its bridge function. When this bridge is first installed, its table is empty.
- As it comes across each packet it looks at both the destination and source addresses.
- It checks the destination to decide where to send the packet. If it does not yet recognise the destination address it relays the packet to all of the stations on both segments.
- It uses the source address to build its table. As it reads the source address it notes which side the packet came from and associates that address with the segment to which it belongs.
- As an example, consider the configuration of Fig. 1.32.2. As shown in the Fig. 1.32.2 bridge B_1 is connected to LANs 1 and 2 and bridge B_2 is connected to LANs 2, 3 and 4.
- A frame arriving at bridge B_1 on LAN 1 destined for A can be discarded immediately because it is already on the right LAN, but a frame arriving on LAN 1 for C or F must be forwarded.
- When a frame arrives, a bridge must decide whether to discard or forward it, and if the latter is true, then decide on which LAN to put the frame.

Bridge learning :

- When a frame arrives at one of the ports of a bridge, it has to make a decision about forwarding the frame to another port. This decision is made based on the destination address of the frame.

- In order to make such decisions every bridge needs a table called **forwarding table** or **forwarding database**.
- This table indicates which side of the port the destination station is attached to, directly or indirectly. The format of a forwarding table is shown in Table 1.32.1.

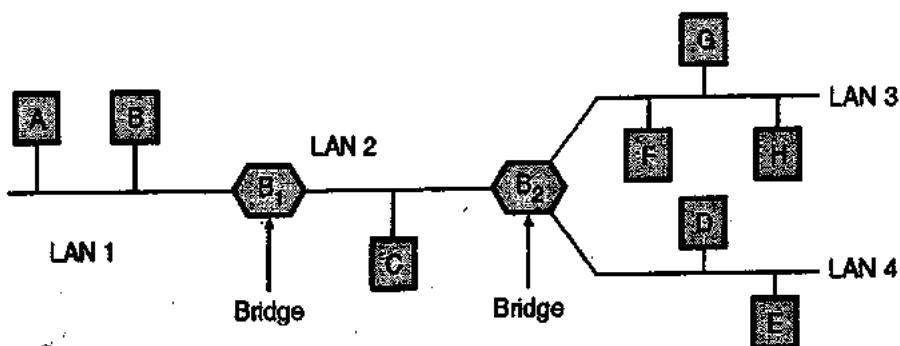
Table 1.32.1 : Format of a forwarding table

MAC address	Port

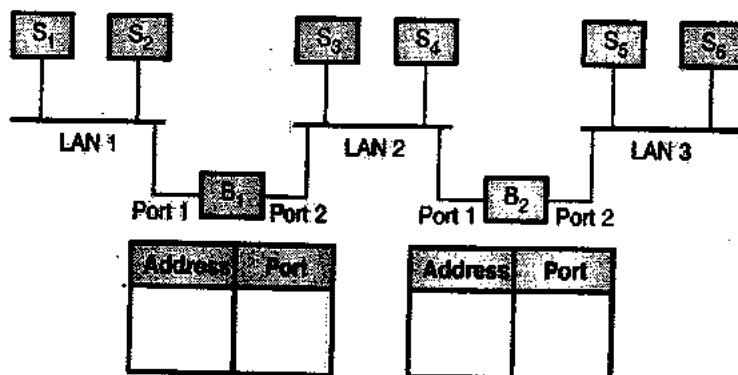
- Note that in practice there are a few thousand entries in a forwarding table.
- Let us see how to fill up these forwarding tables. It is filled up by a process called as "bridge learning".
- The basic bridge learning process is as follows :

Bridge learning procedure :

1. When a bridge receives a frame, it first compares the source address of the frame with each entry in the forwarding table. If no match is found, then the bridge will add this source address alongwith the port number on which the frame was received, to the forwarding table.
2. The bridge compares the destination address of the received frame with each entry in the forwarding table. If a match is found, then the bridge forwards the frame to the port indicated in the entry. But if this port is same as the one on which the frame was received, then the frame is discarded. Finally if a match is not found, then the bridge will send that frame on all its ports except the one on which the frame was received.



(L-648) Fig. 1.32.2 : Configuration of bridge and LAN



(L-64) Fig. 1.32.2(a) : Example network

Example on bridge learning :

Consider the network shown in Fig. 1.32.2(a). Assume that forwarding tables of both the bridges are initially empty.

1. S₂ sends a frame to S₁ :

- If S₂ sends a frame to S₁, then B₁ compares the source address of the received frame with the existing entries. So here S₂ is the sender and S₁ is destination.
- But there are no entries in B₁ table. So it adds the address of S₂ in its forwarding table as shown in Fig. 1.32.2(b).
- Then B₁ compares the destination address of the received frame with the existing entries. But the table is empty. So the bridge B₁ thinks of flooding the frames. But then it understands that the destination S₁ is connected on the same port (Port 1) on which the frame has been received.
- So B₁ will note down the address of S₁ in its table and **discard the frame**. This is because bridge B₁ is not required to be used when a communication between S₁ and S₂ is to be made.
- The traffic is now completely isolated in LAN 1, and the updated bridge tables are shown in Fig. 1.32.2(b).

Address	Port
S ₂	1
S ₁	1

Address	Port

(Fig. 1.32.2(b)) : Forwarding tables after S₂ → S₁**2. S₅ transmits to S₄ :**

- The two stations correspond to two different LANs. S₅ is the sender and S₄ is the destination.

- First B₂ records the address of S₅ and port number (Port 2) because the address of S₅ is not found in its forwarding table.
- Then B₂ checks the destination address. Since there are no entries, it will add S₄ and port 1 in its table as shown in Fig. 1.32.2(c).
- Bridge B₂ will forward the frame to port 2 of B₁ as well as to LAN 2 where S₄ will receive it.
- When this frame arrives at port 2 of B₁ it also adds the source address i.e. S₅ and port 2 in its table as shown in Fig. 1.32.2(c).
- However the destination address (S₄) is on the same port (2) of B₁ on which it has received the frame. So it will note down S₄ and port 2 in its table but **discard the frame**.

B ₁		B ₂	
Address	Port	Address	Port
S ₂ → S ₁	{ S ₂ 1 S ₁ 1 S ₅ 2 S ₄ 2 }	S ₅ → S ₄	{ S ₅ 2 S ₄ 1 }

(G-1970) Fig. 1.32.2(c) : Forwarding tables after S₅ → S₄

- The table entries for the remaining transmissions are given in Figs. 1.32.2(d) and (e).

3. S₃ transmits to S₅ :

B ₁		B ₂	
Address	Port	Address	Port
S ₂ → S ₁	{ S ₂ 1 S ₁ 1 S ₅ 2 S ₄ 2 S ₃ 2 }	S ₅ → S ₄	{ S ₅ 2 S ₄ 1 }
S ₃ → S ₅	{ }	S ₃ → S ₅	{ S ₃ 2 }

(G-1971) Fig. 1.32.2(d) : Tables after S₃ → S₅**4. S₁ transmits to S₂ :**
No change in the tables.



5. S_6 transmits to S_5 :

B ₁		B ₂	
Address	Port	Address	Port
$S_2 \rightarrow S_1$	1	$S_5 \rightarrow S_4$	2
S_1	1	S_4	1
$S_5 \rightarrow S_4$	2	$S_3 \rightarrow S_5$	2
S_4	2	$S_6 \rightarrow S_5$	2
$S_3 \rightarrow S_5$	2	S_3	2

(G-1972) Fig. 1.32.2(e) : Table after $S_6 \rightarrow S_5$

1.32.2 Source Routing Bridges :

- The source routing bridges were developed by the IEEE 802.5 committee and they are used basically to interconnect token ring networks.
- The main idea of source routing is that each station should determine the route to the destination when it wants to send a frame and therefore include the route information in the header of the frame.
- The frame format for source routing is shown in Fig. 1.32.3.
- Note that the routing information field is inserted only if the two communicating stations are on different LANs.
- Fig. 1.32.4 shows the LAN interconnection with source routing bridges. If station-1 wants to send a

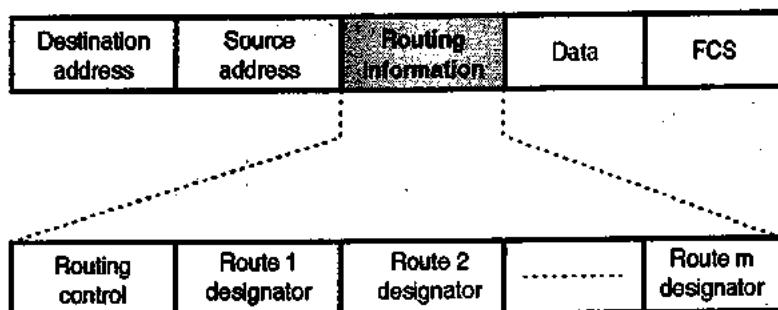
frame to station-2 then a possible route can be LAN-1 \rightarrow B₁ \rightarrow LAN 2 \rightarrow B₄ \rightarrow LAN 4.

- Many more routes are available for the same source destination pair.
- In general when a station wants to transmit a frame to another station on a different LAN, the station consults its routing table.
- If the route to the destination is found, then the station simply inserts the routing information into the frame.

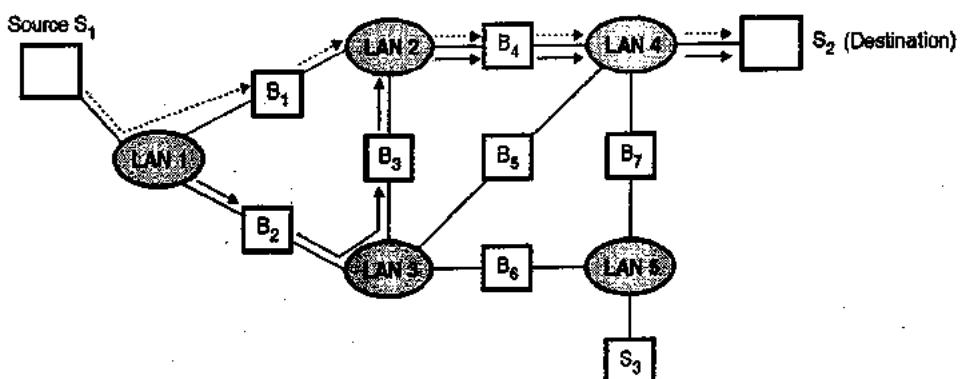
How to discover a route ?

To discover a route the basic idea is as follows :

- The station who wants to discover a route first broadcasts a special frame called single route broadcast frame.
- This frame will visit every LAN exactly once and eventually reaches the destination.
- Then the destination station responds with another special frame called the all routes special frame which generates all possible routes back to the source station.
- After collecting all routes the source chooses the best possible route and saves it.



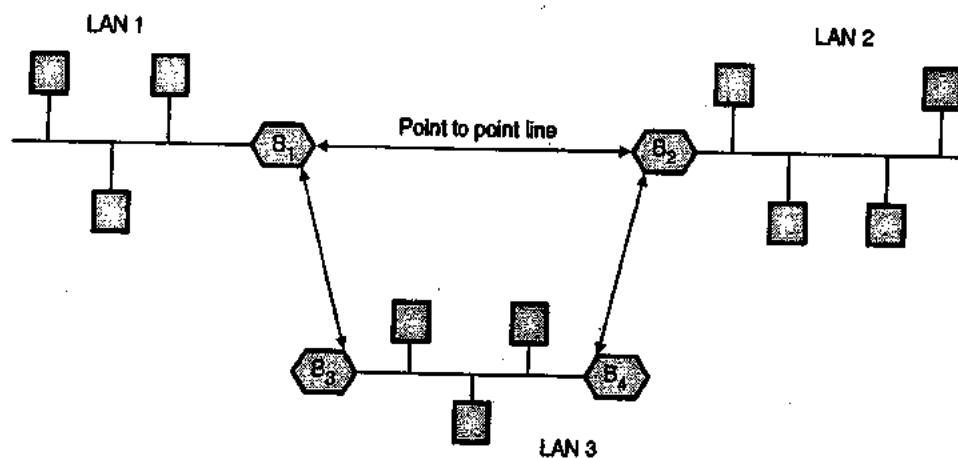
(L-654) Fig. 1.32.3 : Frame format for source routing



(L-655) Fig. 1.32.4 : LANs interconnected with source routing bridges

1.32.3 Comparison of Transparent and Source Routing Bridge :

	Parameters	Transparent Bridge	Source Routing Bridge
1.	Ability to reconfigure	High. Bridges keep information on location of stations.	High. Each station must learn the route to its destination before sending.
2.	Stations responsibilities	None. They just send the frames and let the bridges do the work.	They determine and maintain addresses.
3.	Bridges requirements	Routing tables and the ability to both update them and execute a spanning tree algorithm.	Ability to broadcast or forward, depending on routing designators and ability to execute a spanning tree algorithm.
4.	Routes used	Always along the spanning tree, but not necessarily the cheapest.	Stations can choose the cheapest routes to one another.
5.	Dependence on topology	None. Bridges learn where stations are relative to their ports dynamically and stations have no need to know.	Some Bridges respond to routing information and spanning tree algorithms, but stations must determine a route to a destination.
6.	Orientation	Connectionless	Connection-oriented
7.	Configuration	Automatic	Manual
8.	Failures	Handled by the bridge	Handled by the host
9.	Complexity	In the bridge	In the hosts.



(1-656) Fig. 1.32.5 : Configuration of remote bridges

1.32.4 Remote Bridges :

- If bridges are used to connect LANs, having large distance between them they are called remote bridges. Many point to point links can be used to connect these bridges as shown in the Fig. 1.32.5.
- Various protocols can be used on these point to point lines. One of them is to use a point to point data link protocol (PPP); putting complete MAC frames in the payload field.

- Another option is to strip off the MAC header and trailer at the source bridge and put what is left in the payload of the point to point protocol. A new MAC header and trailer can then be generated at the destination bridge.

1.32.5 Bridges Connecting Different LANs :

Ideally a bridge should be able to connect LANs that use different protocols at the data link layer. For example, wired LAN and wireless LAN. But in practice the following issues are needed to be considered :

- Frame format



2. Maximum data size
3. Bit order
4. Data rate
5. Security issues
6. Multimedia support

1.33 Wireless Access Point (AP) :

- In computer networks, a wireless Access Point (AP) is a device which is used to connect the wireless devices to a wired network using Wi-Fi or related standards.
- The AP usually get connected to a router via a wired network as a standalone device but sometimes it can be an integral component of the router itself.
- With the inclusion of the wireless Access Point (AP) the network users can now add devices that can access the network without any cables.
- An AP generally gets connected directly to a wired Ethernet connection and makes wireless radio frequency links available to the other devices so as to access the wired connection.
- Most APs are designed to facilitate the connection of multiple wireless devices to one wired connection. Most APs use IEEE 802.11 standard.

1.33.1 Applications of AP :

- In typically corporate applications several APs are attached to a wired network and they provide a wireless access to the office LAN.
- The wireless APs are managed by a WLAN controller. This controller automatically adjusts the RF power channels, authentication and security. Such a controller can be a part of mobility group to allow mobile users to access the wired facility.
- A common public application of APs is **hotspot**. In this application, wireless clients can get connected to Internet irrespective of the network to which they belong to for the moment.
- This concept has become common in big cities where places like coffee houses, libraries etc. provide the facility to their clients to stay connected continuously to the Internet. A collection of connected hot spots is known as **Lily Pad Network**.
- The APs are also being used in home wireless networks. Here generally only one AP is used to connect all the computers in a home.

1.33.2 Difference Between A.P. and Ad hoc Network :

- We should not confuse wireless A.P. with wireless ad hoc networks. Note that an ad hoc network uses a connection between two or more devices without

using a wireless access point because the devices communicate directly when in range.

- An ad hoc network does not need an A.P. We can easily and quickly set up and use the ad hoc networks in the situations of quick data exchange.
- Ad hoc networks are like Bluetooth connections due to their peer-to-peer layout and are not preferred for a permanent installation.

1.33.3 Limitations of A.P. :

The wireless A.P. has following limitations :

1. An IEEE A.P. can typically (theoretically) communicate in a radius of 103 m and can serve upto 30 clients located in this region. But the practical range can be much less. Additional repeaters and reflectors need to be used to extend the range.
2. In crowded downtown areas with tall buildings and multiple WAPs, signal overlap takes place which causes interference, signal dropage and data errors.
3. Wireless networks always lag behind wired networks in terms of increasing bandwidth and throughput. In case of APs this problem worsens further because the same frame needs to be transmitted twice. Once from the sender to AP and them from AP to the receiver. This approximately reduces the effective bandwidth to 50 %.

1.33.4 Security :

- If wireless APs connected to the network anybody within the range of the AP can get connected to the network.
- The most common solution to this problem is to use wireless traffic encryption. Modern APs are available with built in encryption. The second generation schemes WPA and WPA2 used with a strong password are considered to provide a good safety.

1.33.5 Specialized APs :

Some industrial grade APs can also act as bridges, routers or clients.

1.34 Routers : SPPU : Dec. 10, May 11, Dec. 12

University Questions

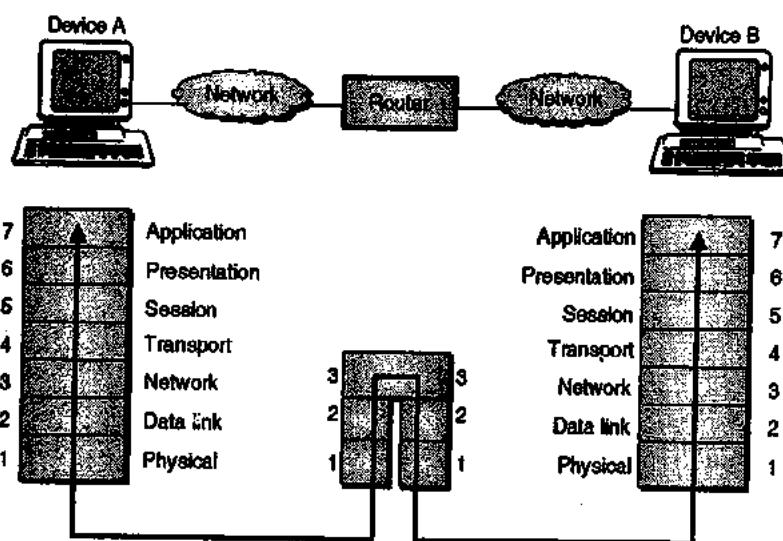
- Q. 1** Write the functions of repeater, hub, NIC, media converter, transceiver, switch, router and bridge. (Dec. 10, 8 Marks)
- Q. 2** List and write the use of different network connecting devices. (May 11, 8 Marks)
- Q. 3** Write the functions of repeater, Hub, NIC, switch, router and bridge. (Dec. 12, 8 Marks)

- Routers are devices that connect two or more networks as shown in Figs. 1.34.1(a) and (b). They consist of a combination of hardware and software.
- The hardware can be in the form of a network server, a separate computer or a special device, as well as the physical interfaces to the various networks in the internetwork.
- Various types of networks can be interconnected through routers as shown in Fig. 1.34.1(b).
- The software in a router are the operating system and the routing protocol. Management software can also be used.
- Routers use logical and physical addressing to connect two or more logically separate networks.
- The large network is organized into small network segments called as subnets and these subnets are interconnected via routers.
- Each of the subnet is given a logical address. This allows the networks to be separate but still access each other and exchange data.

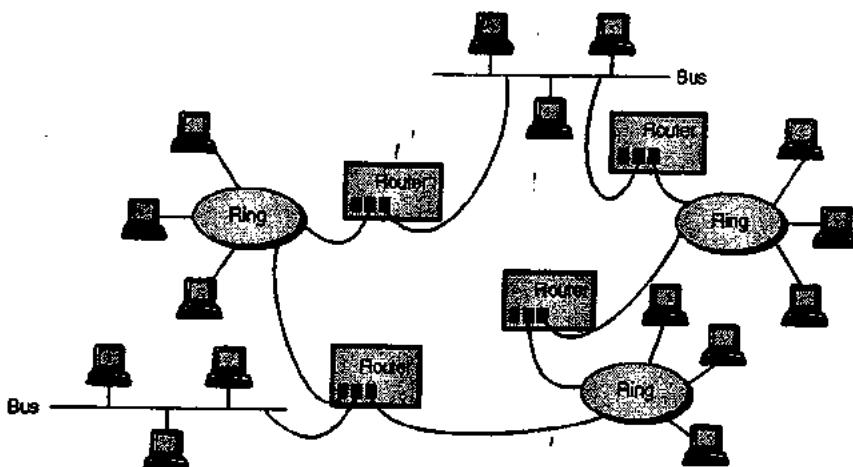
- Data is grouped into packets, or blocks of data. Each packet has a physical device address as well as logical network address.
- The network address allows routers to calculate the optimal path to a workstation or computer.
- Route discovery is the process of finding the possible routes through the internetwork and then building routing tables to store that information. The two methods of route discovery are :
 - Distance vector routing
 - Link state routing.

Note:

- Routers work at the network layer of the OSI model.
- With static route selection, packets always follow a pre-determined path.



(G-364) Fig. 1.34.1 (a) : A router in the OSI model



(G-365) Fig. 1.34.1(b) : Routers in an internet



1.35 Gateways :

SPPU : May 11

University Questions

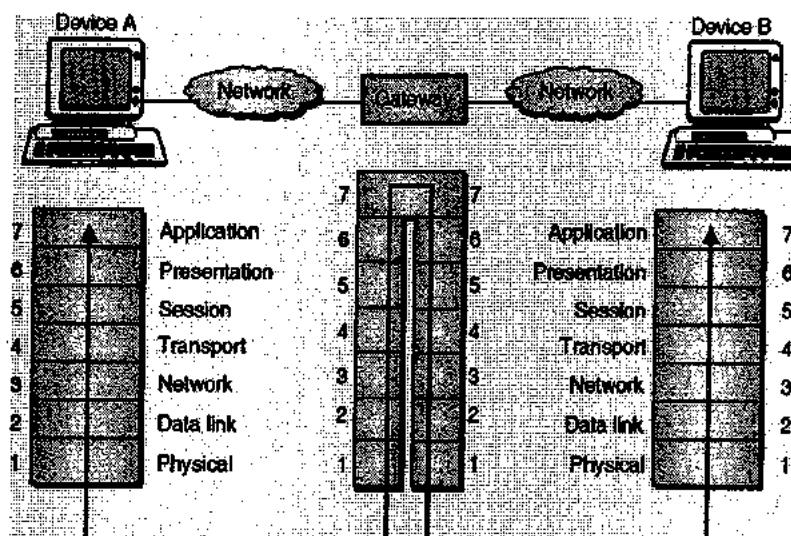
- Q.1** List and write the uses of different network connecting devices. (May 11, 8 Marks)

- When the networks that must be connected are using completely different protocols from each other, a powerful and intelligent device called a gateway is used.
- A gateway is a device that can interpret and translate the different protocols that are used on two distinct networks as shown in Figs. 1.35.1(a) and (b).
- Gateways comprise of software, dedicated hardware or a combination of both. Gateway operate through

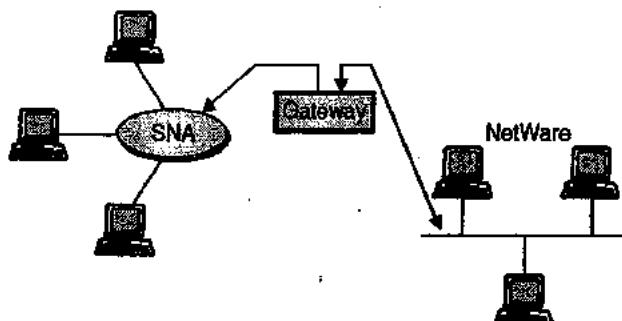
all the seven layers of the OSI model and all five layers of the internet model.

- A gateway can actually convert data so that it works with an application on a computer on the other side of the gateway. For e.g. a gateway can receive e-mail message in one format and convert them into another format.
- Gateways can connect systems with different communication protocols, languages and architecture. For e.g. IBM networks using Systems Network Architecture (SNA) can be connected to LANs using a gateway.

Note: Gateways are slow because they need to perform intensive conversions.



(a) A gateway in the OSI model

(b) A gateway
(G-366) Fig. 1.35.1

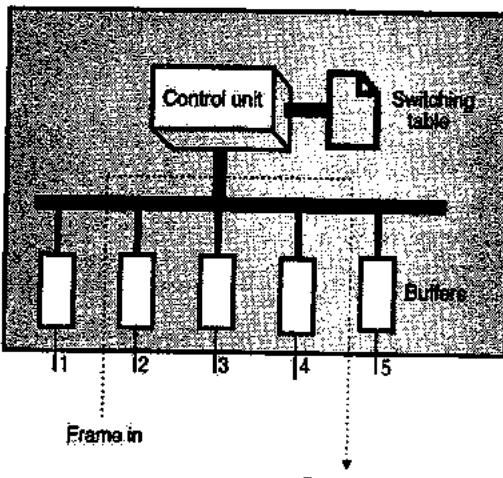
1.36 Switches :

SPPU : Dec. 10, May 11, Dec. 11, Dec. 12, May 13

University Questions

- Q.1** Write the functions of repeater, hub, NIC, media converter, transceiver, switch, router and bridge.
(Dec. 10, 8 Marks)
- Q.2** List and write the use of different network connecting devices.
(May 11, 8 Marks)
- Q.3** What is switch ? Explain difference between manageable and non-manageable switch.
(May 11, 8 Marks)
- Q.4** Describe the network components (Connectors, Hubs, Switches, Repeaters, and Bridges).
(Dec. 11, 6 Marks)
- Q.5** Write the functions of repeater, Hub, NIC, switch, router and bridge.
(Dec. 12, 8 Marks)
- Q.6** Explain the following network components:
 1. Connectors 2. Repeaters
 3. Switches 4. Bridges **(May 13, 8 Marks)**

- A switch is a device which provides bridging functionality with greater efficiency. A switch acts as a multiport bridge to connect devices or segments in a LAN.
 - The switch has a buffer for each link to which it is connected. When it receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link.
 - If the outgoing link is free, the switch sends the frame to that particular link.
- Switches are of two types :
1. Store - and - forward switch
 2. Cut - through switch.
- A store - and - forward switch stores the frame in the input buffer until the whole packet has arrived.
 - A cut-through switch, forwards the packet to the output buffer as soon as the destination address is received.
 - Concept of a switch is shown in Fig. 1.36.1. As shown in the Fig. 1.36.1 a frame arrives at port 2 and is stored in the buffer.
 - The CPU and the control unit, using the information in the frame consult the switching table to find the output port. The frame is then sent to port 5 for transmission.



(G-36) Fig. 1.36.1 : Switch

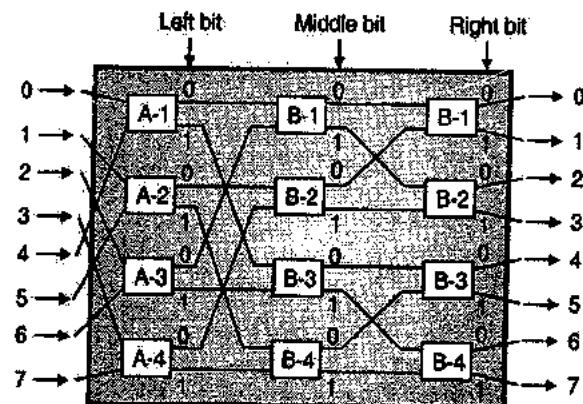
Note: Routing switches use the network layer destination address to find the output link to which the packet should be forwarded.

1.36.1 Two Layer Switch :

- The switches can be of two types namely the two layer switches and the three layer switches.
- A two layer switch operates at the physical as well as data link layer.
- The two layer switch is basically a bridge. It has many ports and it is designed to allow better performance.
- A bridge with few ports is used for connecting a few LANs together. But a bridge with many can allocate a unique port to each station. Thus each station will have its own separate identity.
- Therefore there is no competing traffic and so there are no collisions.

1.36.2 Three Layer Switch :

- A three layer switch is used at the network layer and it is a kind of router.
- A three layer switch is shown in Fig. 1.36.2.



(G-36) Fig. 1.36.2 : A three layer switch



- 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 = $\log_2(n) = \log_2 8 = 3$.

1.36.3 Comparison of Hub and Switch :

Sr. No.	Hub	Switch
1.	It is a broadcast device.	It is a point to point device.
2.	It operates at physical layer.	It operates at datalink layer.
3.	It is not an intelligent device.	It is an intelligent device.
4.	It simply broadcasts the incoming packet.	It uses switching table to find the correct destination.
5.	It cannot be used as a repeater.	It can be used as a repeater.
6.	Not a sophisticated device.	It is a sophisticated device.
7.	Not very costly.	Costly.

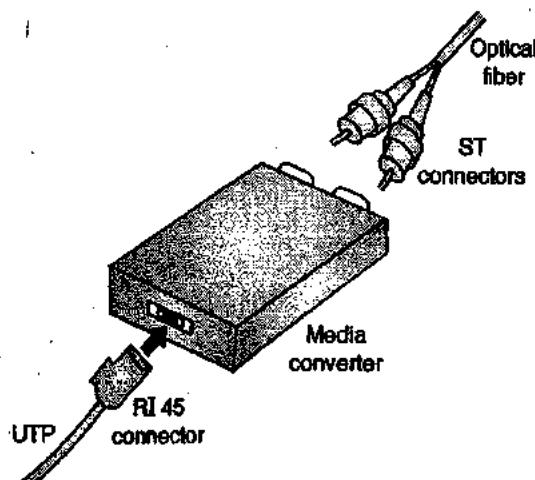
1.36.4 Media Converters :

SPPU : Dec. 10

University Questions

- Q. 1 Write the functions of repeater, hub, NIC, media converter, transceiver, switch, router and bridge.
(Dec. 10, 8 Marks)

- It is a device which is used to connect two different networking media. For example connection between a shielded cable and twisted pair can be achieved through the media converter.
- Fig. 1.36.3 shows the media converter.
- Various functions performed by a media converter are as follows :
 - Connect two different types of wiring systems without an additional repeater.
 - Connect two 10 Base T or 100 Base TX networks in different buildings using fiber-optic cable.
 - To allow the use of different types of cables such as UTP cabling, thin net fiber optic cable, thick net etc. in a single network.



(G-36) Fig. 1.36.3 : Media converter

1.36.5 Comparison of Router and Bridge :

Sr. No.	Parameter	Router	Bridge
1.	Layer in OSI model.	Network layer	Physical or data link.
2.	Operation.	Connect two or more network.	Regeneration, check MAC address.
3.	Types.	Distance vector, Link state	Transparent, Routing.
4.	Principle of working.	Uses hardware and software.	Uses tables relating the addresses and ports.
5.	Used for	Connecting networks	Connecting computers.

1.36.6 Comparison of Bridge, Switch and Hub :

Parameter	Hub	Switch	Bridge
1. Type of device	Broadcast	Point to point	Both
2. Layer of operation	Physical	Data link	Physical and data link
3. Intelligence	Not intelligent	Intelligent	Highly intelligent
4. Duties	Simply broadcast the incoming packet	Uses switching table to find correct destination	Filtering, forwarding and blocking of frames
5. Sophistication	Low	High	Very high
6. Cost	Low cost	Expensive	Very expensive

1.36.7 Comparison of Bridges, Routers and Switches :

Table 1.36.1

Sr. No.	Parameter	Router	Bridge	Switch
1.	Layer in OSI model	Network layer	Physical or data link	Data link and network layer
2.	Type of device	Point to point	Point to point or broadcast	Point to point
3.	Operation	It connects two or more networks	It regenerates, checks MAC address	It provides bridging operation with greater accuracy
4.	Types	Distance vector, link state	Transparent, Routing	Two layer, three layer.
5.	Intelligence	Highly intelligent	Highly intelligent	Highly intelligent
6.	Used for	Connecting networks	Filtering, forwarding and blocking frames.	Uses switching table to find correct destination.

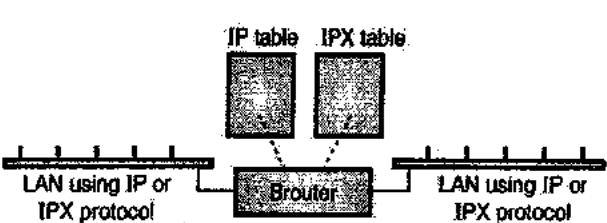
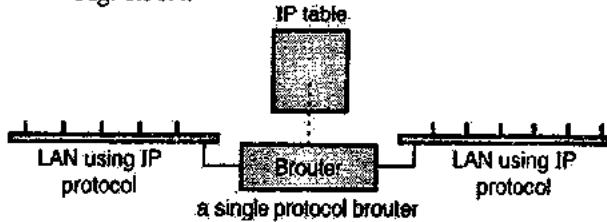
1.36.8 Brouter :

- A bridge router or brouter is a network device that can work as a bridge and as a router.
- A brouter will route the packets for known protocols and simply forward all other packets like a bridge.
- Brouters at the network layer for routable protocols and at the data link layer for non routable protocols.
- As the network are becoming more and more complex, a mix of routable and non-routable protocols are being used which has led to the use of brouters.
- Brouters handle both routable and non routable features by acting as router for the routable protocols and bridge for the nonroutable protocols.
- Bridged protocols might propagate throughout the network but the techniques such as filtering and learning might be used to reduce potential congestion.
- Brouters are used as connecting devices in the networking system. It acts as bridge in a network and as a router in an internetwork.
- While the term brouter is being used to describe bridge / router device, an actual brouter is very rare.

- Instead most brouters are simply routers that have been configured to function as a bridge as well. This functionality can be often implemented using the router's software interface.

Note : Since routers are more complex than bridges, it is more likely for router than a bridge to function as a brouter. Therefore brouters are also called as bridging routers.

- The block diagram of a brouter is as shown in Fig. 1.36.4.



(G-1940) Fig. 1.36.4 : Block diagram of a brouter



- Fig. 1.36.4(a) shows a single protocol router which routes packets using IP protocol. The other packets are passed on the basis of their physical locations.
- Fig. 1.36.4(b) shows a multiprotocol router which routes packets using IP or IPX protocols. Any other packets are passed on the basis of their physical address.

1.37 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. 1.37.1.

1.37.1 Split Phase Manchester Format :

SPPU : Dec. 05, May 13

University Questions

- Q. 1** Write short notes on Manchester code. (Dec. 05, 6 Marks)
- Q. 2** Explain line coding polar schemes. (May 13, 8 Marks)

- The split phase Manchester format is as shown in Fig. 1.37.2.

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.

1.37.2 Differential Manchester Code :

SPPU : May 13

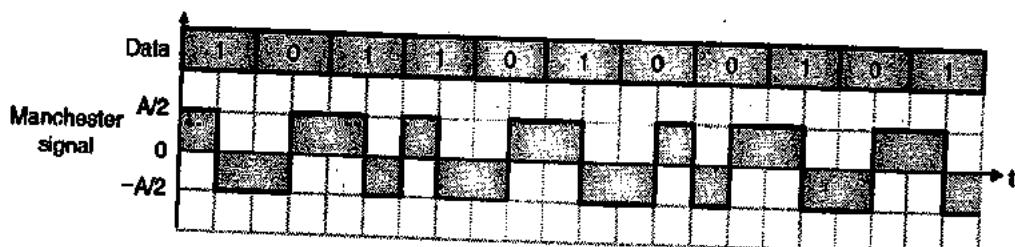
University Questions

- Q. 1** Explain line coding polar schemes. (May 13, 8 Marks)

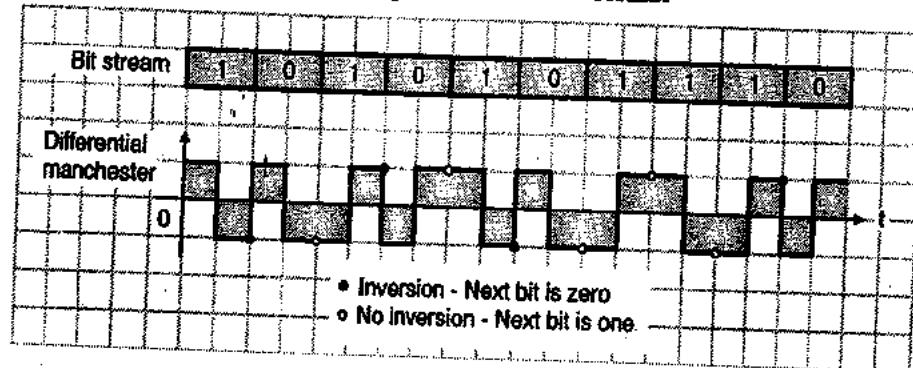
In this code there is always a transition in the middle of a bit interval. The binary zero has an additional transition at the beginning of the bit interval. This is as shown in Fig. 1.37.3.



(L-255) Fig. 1.37.1



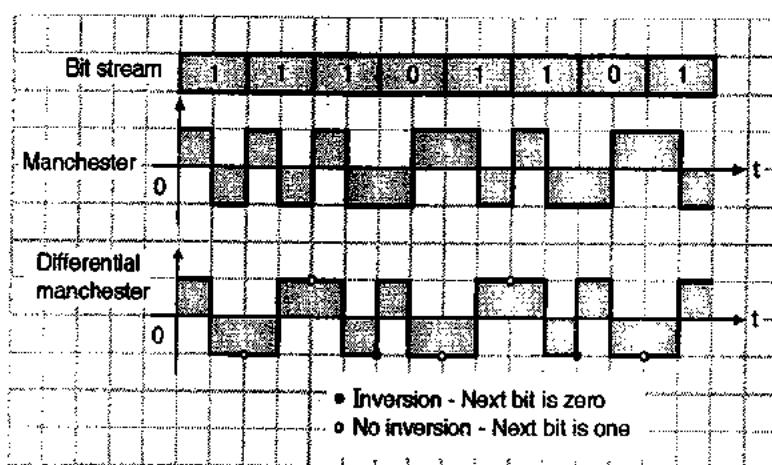
(L-266) Fig. 1.37.2 : Split phase manchester format



(L-286(a)) Fig. 1.37.3 : Differential manchester coding

Ex. 1.37.1 : Show the Manchester and differential Manchester encoding pattern for the bit stream 11101101.

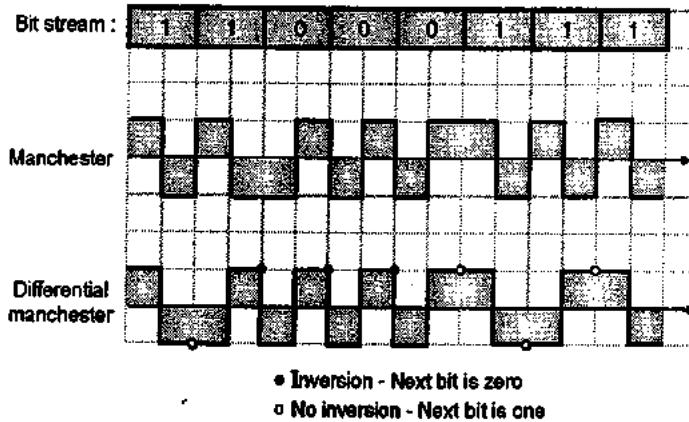
Soln. :



(L-287) Fig. P. 1.37.1

Ex. 1.37.2 : Show Manchester and differential Manchester encoding pattern for the bit stream 11000111.

Soln. :



(L-288) Fig. P. 1.37.2

1.38 Introduction to WLAN and WPAN :

- We all know wired Local Area Networks (LANs) very well. In order to get rid of the wiring associated with the interconnections of PCs in LANs, researchers have tried to use radio waves or infrared light as a replacement to the wires.
- Thus the wireless LANs i.e. WLANs got evolved.
- WPAN is a Wireless Personal Area Network. It is one step down from WLANs. The WPANs cover smaller areas and need to use less power for transmission.
- WPANs are used for networking of portable and very small computers, cell phones, printers, speakers, microphones, etc.

1.38.1 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 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.



1.38.2 Wi-Fi :

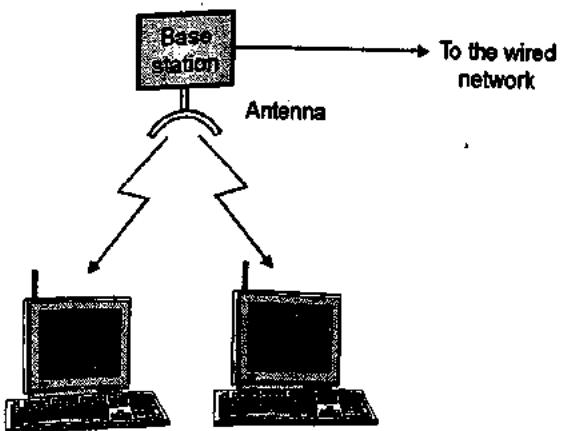
- Wi-Fi is a popular technology which allows an electronic device to exchange data or to connect to the Internet using radio waves.
- We can define Wi-Fi as any wireless local area network (WLAN) product that are based on the IEEE 802.11 standards.
- The devices which can use Wi-Fi are personal computers, video game consoles, smart phones, some digital cameras, Tablet computers etc.
- Wireless communication is one of the fastest growing technologies.
- The wireless LANs are used in following applications :
 1. Office buildings
 2. Colleges
 3. Public areas
- In this chapter we are going to discuss about two important wireless technologies for LANs :
 1. IEEE 802.11 wireless LAN.
 2. Bluetooth

1.39 Wireless LAN - 802.11 (Architecture) :

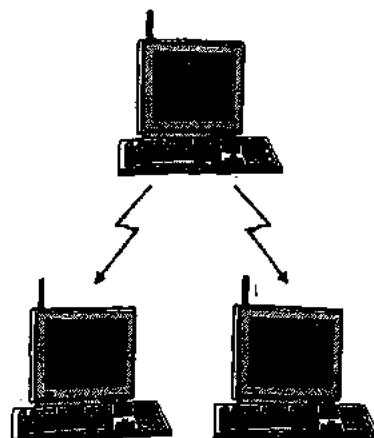
- In wireless LAN, each computer and note book computer is equipped with a short range transmitter and receiver to allow communication between them.
- The IEEE committee standardized the wireless LAN and the standard was 802.11.
- This standard had to work in two different modes :
 1. In the presence of a base station.
 2. In the absence of a base station.

These two modes are shown in Fig. 1.39.1.

- In the network with base station, all the communication is passed through the base station. The Base Station (BS) is also called as the Access Point (AP) in 802.11 terminology.
- In the network without base station, the computers will communicate among each other as shown in Fig. 1.39.1(b). This mode is also called as Ad hoc networking.



(a) With base station



(b) Without base station (Ad hoc networking)
(G-37) Fig. 1.39.1 : Wireless networks

Frequency :

- The frequency of the radio waves being used as a medium is decided by taking into consideration the following factors :
 1. Frequency band which is available worldwide.
 2. Range to be covered
 3. Battery life and power consumed by the device.
 4. Computer mobility.
 5. Users privacy should be maintained.
 6. System should have enough bandwidth.
 7. System should be economically viable.

Compatibility with Ethernet :

- The 802.11 standard was designed such that it is compatible with the Ethernet (Wired LAN).
- It should be possible to send an IP packet over the wireless LAN the same way a wired computer sends an IP packet over Ethernet.

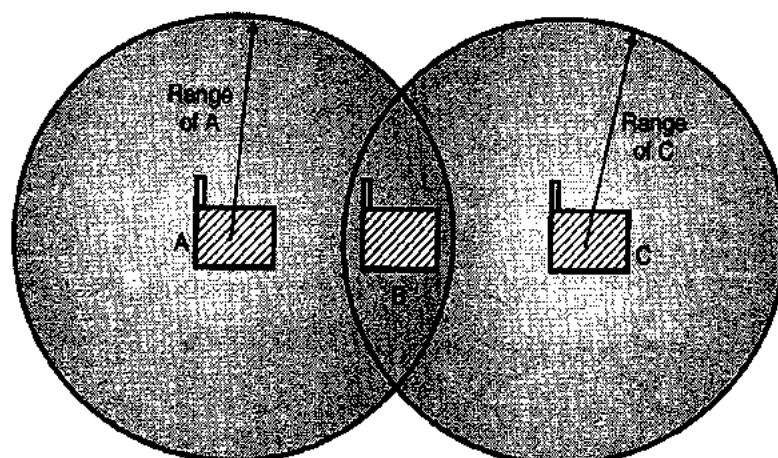
Differences between Ethernet and wireless LAN :

- The Ethernet (Wired LAN) and wireless LAN are compatible above datalink layer but they are different in the physical and data link layers. Some of the differences are as follows :
 - First is, that a computer in Ethernet first listens to the ether and transmits only if the Ether (medium) is idle. But this idea does not work in the wireless LAN at all. Refer Fig. 1.39.2.
 - The second is that a radio signal can be reflected off the solid objects. So the same signal can be received many times along different paths. The interference resulting due to this is called as **multipath fading**.
 - The third is that many softwares are not aware of the mobility. So the software used in Ethernets will not be useful in WLANs.
 - If a notebook computer or a laptop is moved away from its base station which mounted on the ceiling and goes into the range of some other

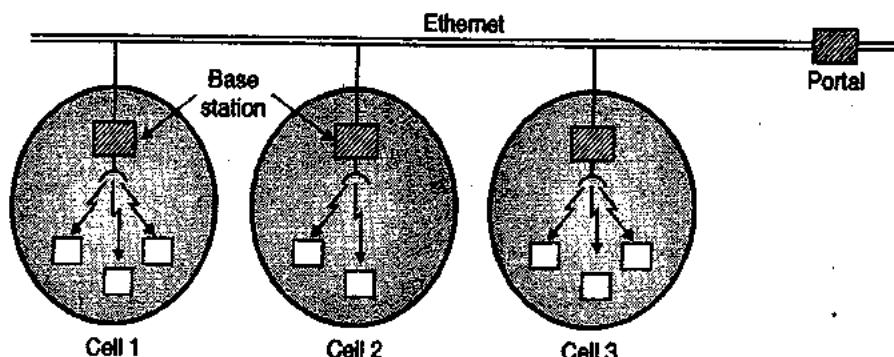
base station then the principle of handoff similar to cellular network needs to be used. This problem does not occur in Ethernet.

A multicell 802.11 network :

- To solve the hand off problem discussed earlier a multicell 802.11 network is designed. It consists of multiple cells and each cell has its base station connected to Ethernet as shown in Fig. 1.39.3.
- From outside the system looks like a single Ethernet. The connection between this system and the outside world is called as **portal**.
- The standard 802.11 a uses a wider frequency band and runs at a speed upto 54 Mbps. The 802.11 b standard uses the same frequency band but speed is upto 11 Mbps.
- WLANs have been widely accepted and airports, trains, hotels, shopping malls, universities are installing it.



(G-372) Fig. 1.39.2 : Range of a single radio does not cover the entire system



(G-373) Fig. 1.39.3 : A multicell 802.11 network

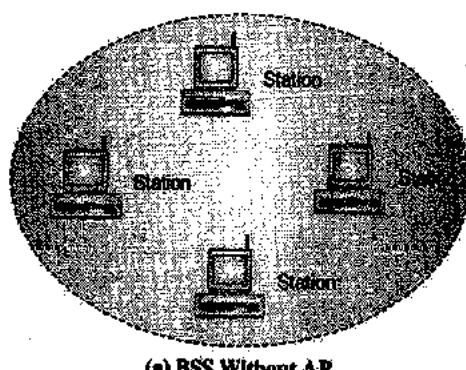


1.40 Components in a Typical IEEE 802.11 Network :

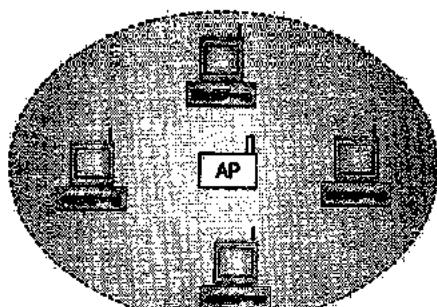
- IEEE 802.11 is the most popular WLAN standard. It defines the specifications for the physical and MAC layers.
- IEEE 802.11 defines two types of services :
 - Basic Service Set (BSS)
 - Extended Service Set (ESS)

1.40.1 Basic Service Set (BSS) :

- As per IEEE 802.11 the BSS has been defined as the basic building block of wireless LAN.
- A BSS consists of stationary or moving wireless stations and a central base station which is optional called as the Access Point (AP).



(a) BSS Without AP



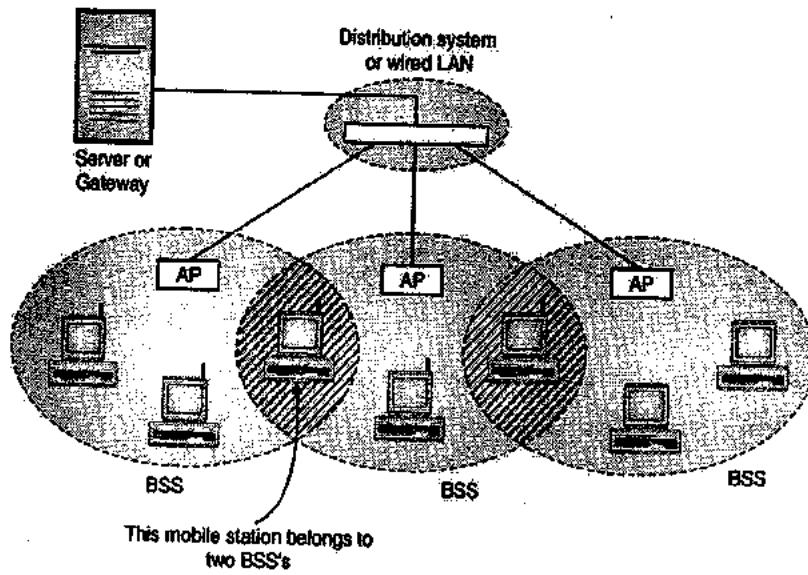
(b) BSS With an AP

(G-380)Fig. 1.40.1 : Types of BSS

- Thus a BSS can be either without AP or with AP as shown in Figs. 1.40.1(a) and (b).
- The BSS without AP cannot send data to another BSS. So no data exchange can take place outside that BSS hence it is known as a standalone network or ad hoc architecture. However all the stations inside a BSS can exchange data among themselves.

Extended Service Set (ESS) :

- An Extended Service Set (ESS) consists of multiple BSSs with APs. The BSSs in this system are connected to each other via a distribution system or a wired LAN as shown in Fig. 1.40.2.
- The APs are connected to each other via the distribution system as shown. The distribution system can be any type of LAN such as Ethernet.
- The ESS contains two types of stations :
 - Mobile stations which can move and change location
 - Stationary or non-moving stations.
- Out of these, the non-moving stations are the APs which are a part of the wired LAN. Whereas the mobile stations are those contained in the BSS. Fig. 1.40.2 shows the structure of an ESS.
- The BSSs are connected to each other to form a network called **infrastructure network**. In such networks the stations close to each other can communicate without taking help of AP.
- But if two stations located in two different BSS wish to communicate with each other, than they have to do so through APs.
- This type of communication is very similar to that in the cellular communication. The BSS acts as a cell and AP as base station.
- As shown in Fig. 1.40.2 it is possible that a mobile station can belong to more than one BSSs simultaneously.



(G-38)Fig. 1.40.2 : ESS

1.40.2 Types of Stations in ESS :

- Three types of stations are defined by IEEE 802.11 depending on their mobility in the wireless LAN as :
 1. No transition
 2. BSS transition
 3. ESS transition

1. No transition mobility :

It is defined as a station which is not-moving at all (stationary) or moving inside a BSS only.

2. BSS transition mobility :

A station having BSS transition mobility is the one which can move from one BSS to the other BSS but does not move outside one ESS.

3. ESS transition mobility :

A station having ESS transition mobility is the one which can move from one ESS to any other ESS. But IEEE 802.11 does not guarantee a continuous communication when the station is moving.

1.41 Introduction to Spread Spectrum :

- PCM, DM etc. are practically used digital communication systems. The focus of our attention while discussing those systems was on two important factors, viz.

1. How to utilize the channel bandwidth efficiently ?

- ##### 2. How to minimize the amount of transmitted power ?
- However the efficient utilization of bandwidth and minimizing the transmitted power are not the "only" problems faced by a communication system. Some other problems encountered by it are as follows :

Problems encountered by a communication system :

1. In the areas such as "military communication", the information has to be "secured". That means an unauthorized user is not expected to access the

information. Also he should not be allowed to interfere the communication by any means.

2. Sometimes a hostile transmitter (say used by terrorists) can "jam" the desired or legitimate transmission. To avoid this the channel should be "immune" to any external interference.
3. Even in the non-military communications an unintentional interference is caused by a user who is transmitting its information through a channel which is already being used.

Remedy :

These problems can be successfully solved by using a technique called "Spread Spectrum Modulation".

1.41.1 How is the SS Signal Different from the Normal Signal ?

The spread spectrum (SS) signal is different from a normal signal, in the following aspects :

1. This signal occupies a larger bandwidth than that of a normal signal. (Therefore the name spread spectrum).
2. The spread spectrum signal invariably uses some kind of coding. The spectrum spreading at the transmitter and despreading (opposite to spreading) at the receiver is obtained with the help of this code word. The code word associated with an SS signal is independent of the information carried by the signal.
3. The most important point is that the SS signal is "pseudorandom" in nature. This makes it appear like "random noise". Therefore the normal receiver cannot demodulate the SS signal. Only a specially designed receiver can demodulate it to recover the information. Due to this characteristics the SS signal appears as noise to any unintended receiver.



1.42 Applications of Spread Spectrum Modulation :

The spread spectrum signals are used in the following applications :

1. To avoid the intentional interference (called as jamming).
2. To reject the unintentional interference from some other user : This is possible to achieve by assigning a different code for the signals from various users. This type of communication which allows multiple users to share a common channel for transmission of information is called as Code Division Multiple Access (CDMA).
3. To avoid the self interference due to multipath propagation : A signal can take multiple paths while travelling over a communication channel from transmitter to receiver. The signal components following different path lengths will result in a dispersed signal at the receiver. This is known as the self-interference. This type of interference also can be suppressed by using the SS modulation.
4. In low probability of intercept (LPI) signals : A message can be hidden in the background noise by spreading its bandwidth using the code word and then transmitting the coded signal at a low power level. Due to these modifications, the probability that such a signal be intercepted (detected) is reduced to a great extent. Hence such a spread and coded signal is

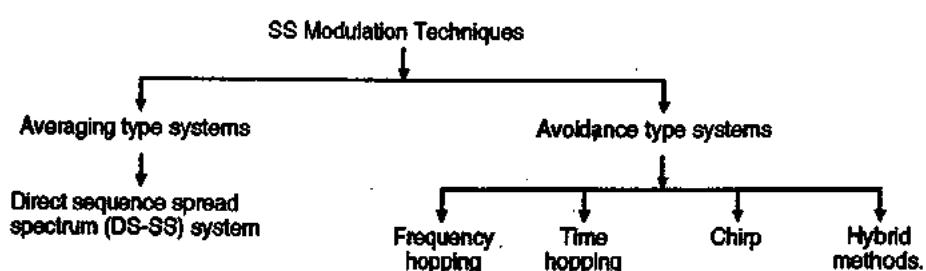
called as the low probability-of-intercept (LPI) signal.

5. In obtaining the message privacy : The message privacy can be obtained by superimposing a pseudorandom pattern on the transmitted message.

1.43 Classification of the Spread Spectrum Modulation Techniques :

The SS modulation techniques are broadly categorized into two categories namely the averaging type systems and the avoidance type systems as shown in Fig. 1.43.1.

- The averaging systems reduce the interference by averaging it over a long period. The direct sequence spread spectrum (DS-SS) system is an averaging system.
- The avoidance systems reduce the interference by making the signal avoid the interference over a large fraction of time. The avoidance systems are further classified depending on the type of modulation used. Some of the avoidance type systems using different modulation techniques are :
 1. Frequency hopping system
 2. Time hopping system
 3. Chirp
 4. Hybrid modulation system.



(E-470) Fig. 1.43.1 : Classification of spread spectrum technique

1.44 Model of Spread Spectrum Digital Communication System :

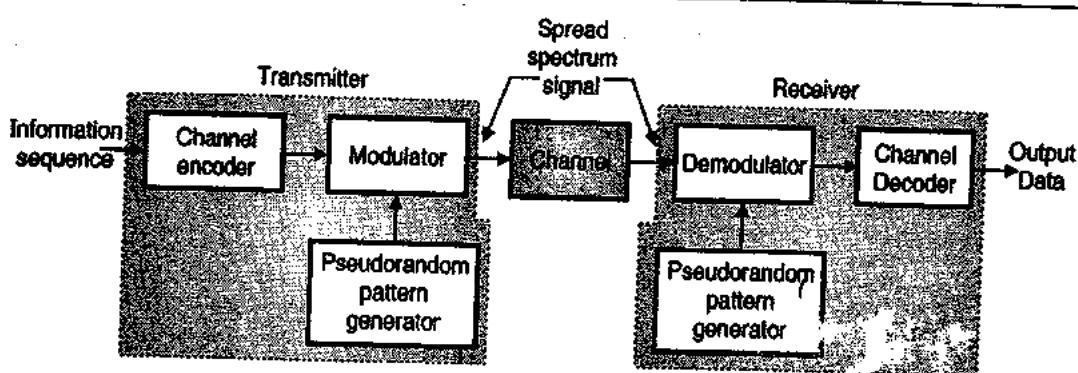
The block diagram shown in Fig. 1.44.1 illustrates the basic elements of a spread spectrum digital communication system.

Operation :

- The information sequence at the input of the system is a binary information sequence. The same signal is recovered at the output of the system as output data signal.
- We have already discussed the role of a channel encoder, channel decoder, modulator and demodulator.
- In addition to these basic building blocks of a digital communication system, two additional blocks called "pseudo-random pattern generator" are used as shown in Fig. 1.44.1. One of them is connected to the modulator on the transmitter side whereas the other is connected to the demodulator on the receiving side. Both these generators are identical to each other.
- These generators generate a pseudorandom or pseudonoise (PN) binary sequence. It is impressed on the transmitted signal at the modulator. Thus the modulated signal along with the pseudorandom sequence travels over the communication channel. This sequence spreads the signal randomly over a wide frequency band. Thus the output of the modulator is a spread spectrum signal.
- The pseudorandom sequence is removed from the received signal, by the other "pseudorandom

generator" operating at the receiver. Thus the pseudorandom pattern generators operate in synchronization with each other.

- The synchronization between these pattern generators is achieved before the beginning of the signal transmission. This is done by transmitting a fixed pseudorandom bit pattern which a receiver can recognize even in presence of interference. Once this synchronization is established, it is possible to begin the transmission.
- Thus in the spread spectrum receiver, the receiver can demodulate the transmitted signal if and only if a known pseudo-noise sequence has been transmitted along with the information signal.
- Two types of interferences are present in the SS. digital communication system namely the narrow band or broadband interference.
- The modulation techniques used are :
 - Phase Shift Keying (PSK) and
 - Frequency Shift Keying (FSK)
- If PSK is used, then the PN sequence generated at the modulator is used along with the PSK modulation to shift the phase of the PSK signal pseudorandomly. The resulting signal at the modulator output is called as a "Direct-Sequence" (DS) spread spectrum signal.
- If binary or M-ary FSK is being used, then the frequency of the FSK signal is shifted pseudorandomly. The resulting signal at the output of the modulator is called as "Frequency Hopped" (FH) spread spectrum signal.



(E-47) Fig. 1.44.1 : Model of spread spectrum digital communication system

1.45 Direct Sequence Spread Spectrum (DS-SS) :

- The most important advantage of spread spectrum modulation is that it provides protection against externally generated interfering signals. Such signals are called as a jamming signals.
- The information bearing signal is made to occupy a bandwidth which is much larger than the minimum bandwidth required for its transmission.
- This will make the signal to appear like a noise and blends into the background.
- Thus the spread spectrum is a method of camouflaging the message signal.
- One of the methods to used for widening the bandwidth of the data sequence is to use the modulation.
- Refer Fig. 1.45.1 which shows the transmitter, channel and receiver of an idealized model of baseband spread spectrum system. This is also known as direct sequence spread spectrum (DS-SS) modulation.

1.45.1 Operation of the Encoder (Transmitter) :

- The input data sequence is denoted by $d(t)$. This data sequence is first converted into an NRZ sequence $b(t)$ by the NRZ encoder.
- The NRZ signal $b(t)$ and the pseudonoise signal $c(t)$ are applied to the two inputs of a product modulator.
- At the output of the product modulator, we obtain the spread spectrum signal. The spectrum of this signal is

quite spread out as compared to the spectrum of $b(t)$ which is a narrow band signal.

- Thus a data sequence $b(t)$ is used to modulate a wideband pseudo-noise (PN) sequence $c(t)$ by applying these two sequences to the product modulator or multiplier. Both sequences $b(t)$ and $c(t)$ are in polar form.
- According to the fourier transform theory the multiplication of signals in the time domain results in convolution of their frequency domain i.e.

$$c(t) \times b(t) \xleftrightarrow{F} C(f) * B(f) \quad \dots(1.45.1)$$

- Hence if the data sequence $b(t)$ is narrowband and the PN sequence $c(t)$ is a wideband sequence, then the product sequence $m(t) = c(t) \times b(t)$ will have a spectrum $M(f)$ which will be nearly the same as that of the PN sequence $c(t)$.

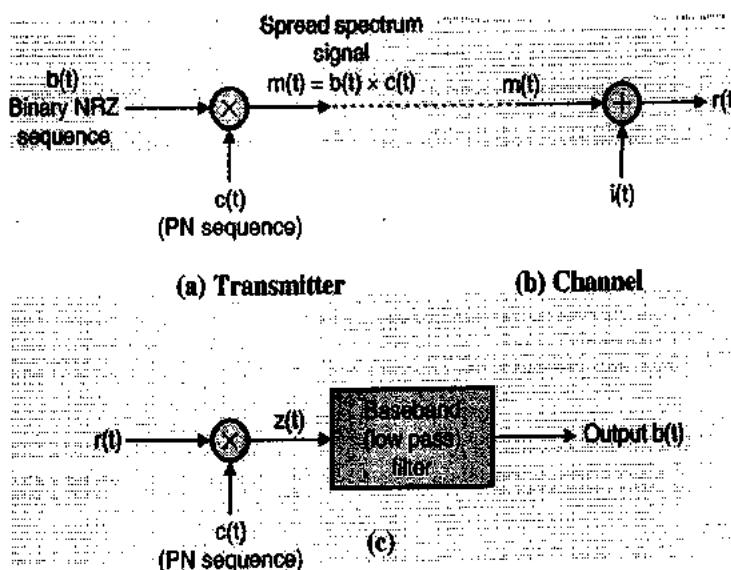
Thus the narrowband signal $b(t)$ will be spread over the wideband and the PN sequence performs the role of a spreading code.

- Note that the transmitted signal $m(t)$ is a baseband signal.
- The spread spectrum signal $m(t)$ is transmitted over the channel where an additive interference $i(t)$ is added to it.
- The signal is received by the receiver. The received signal is therefore expressed as,

$$r(t) = m(t) + i(t) \quad \dots(1.45.2)$$

$$= c(t) b(t) + i(t) \quad \dots(1.45.3)$$

- The waveforms at different points in the transmitter are as shown in Fig. 1.45.2.



(E-478) Fig. 1.45.1 : Idealized model of DS-SS system

1.45.2 Receiver :

- To recover the original sequence $b(t)$, the received signal $r(t)$ is applied to a demodulator as shown in Fig. 1.45.1(c).
- The demodulator consists of a multiplier followed by a low-pass filter.
- The multiplier is supplied with a locally generated PN sequence which is an exact "replica" of the PN sequence used at the transmitter.
- The receiver needs to operate in perfect "synchronization" with the transmitter.
- The demodulated signal is given by,

$$z(t) = c(t) \times r(t) \quad \dots(1.45.4)$$

- Substituting the expression for $r(t)$ i.e.

$$r(t) = c(t)b(t) + i(t)$$

We get,

$$z(t) = c(t)[c(t)b(t) + i(t)]$$

$$\therefore z(t) = c^2(t)b(t) + c(t)i(t) \quad \dots(1.45.5)$$

- In Equation (1.45.5) note that the desired signal $b(t)$ has been multiplied by $c^2(t)$. We know that,

$$c(t) = \pm 1$$

$\therefore c^2(t) = +1$ for all the values of t .

Hence Equation (1.45.5) gets converted to,

$$z(t) = b(t) + c(t)i(t) \quad \dots(1.45.6)$$

- Thus the multiplier output in a receiver contains the desired signal $b(t)$ and the product of the PN sequence $c(t)$ and interference signal $i(t)$.
- Due to the multiplication, the product signal $c(t) \cdot i(t)$ becomes a wideband signal whereas $b(t)$ is a narrow band signal.

- Hence by applying the multiplier output to a baseband (low pass) filter we can pass only signal $b(t)$ and attenuate the interference signal $c(t)i(t)$ heavily.
- Thus the effect of interference signal is reduced to a great extent.

1.45.3 Features of DSSS :

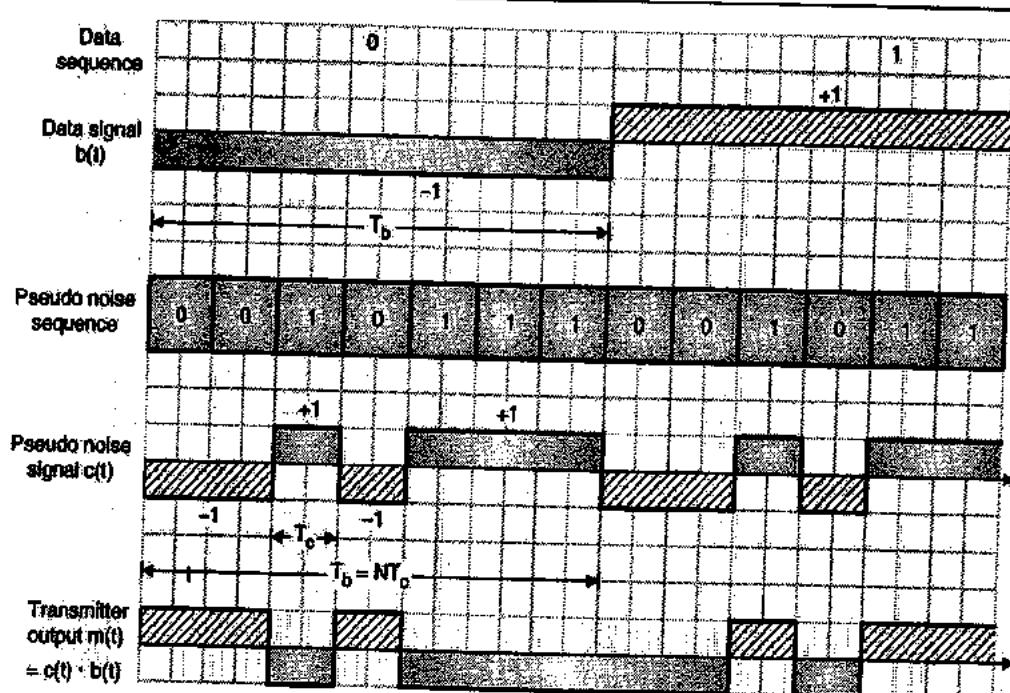
Some of the important features of DSSS are as follows :

- It provides good security against potential jamming or interpretation.
- The DSSS is extremely effective against narrowband jamming signals.
- The narrowband communication signals can coexist with the DSSS signals.
- The DSSS signal is not very effective against broadband interference.

1.45.4 Applications of DS-SS System :

Some of the important applications of the DS-SS system are as follows :

- To combat the intentional interference (jamming).
- To reject the unintentional interference.
- To minimize the self interference due to multipath propagation.
- In the low probability of intercept (LPI) signal.
- In obtaining the message privacy.
- Code division multiple access with DS-SS.



(E-479) Fig. 1.45.2 : Waveforms of DS-SS transmitter

1.46 Frequency Hop Spread Spectrum (FH-SS) Signals :

- In the DS-SS system discussed in the previous section, the NRZ data sequence $b(t)$ modulates the PN sequence.
- The product signal [$m(t) = b(t) \times c(t)$] is spread instantaneously in the frequency domain due to this process.
- The capacity of DS-SS system to reject the intentional interference (jamming) is dependent on the "processing gain PG".
- The processing gain $PG = (T_b/T_c)$. Hence PG increases if the chip period T_c is decreased which in turn permits a greater transmission bandwidth and more chips per bit.
- Problem :** But the capabilities of the physical devices used for the generation of PN spread spectrum signal put a practical limitation on the maximum value of "processing gain" and hence on the capability to combat jamming.
- Under some operating conditions the maximum attainable processing gain PG_{max} is not sufficiently high for combating the jamming.
- Under such conditions an alternative system called Frequency Hop (FH) spread spectrum is used.

Principle of operation of (FH - SS) system :

- In this system the data is used to modulate a carrier. The data modulated carrier is then randomly hopped from one frequency to the other.
- Due to this, the spectrum of transmitted signal is spread sequentially rather than instantaneously.

Types of modulation :

A common modulation technique used is the M-ary frequency shift keying (MFSK). The combination of frequency hopping (FH) and MFSK is known as FH/MFSK.

Note : It is important to understand that the frequency hopping does not cover the entire spread spectrum instantaneously. Rather it covers the entire spectrum sequentially. Therefore we have to consider the rate at which the frequency hops occur. Based on the rate of hopping, the FH/MFSK system has been classified into two categories.

1.46.1 Types of Frequency Hopping :

- Depending on the rate of frequency hopping, the FH/MFSK systems are classified into two categories :
 - Slow frequency hopping.
 - Fast frequency hopping.

Slow frequency hopping :

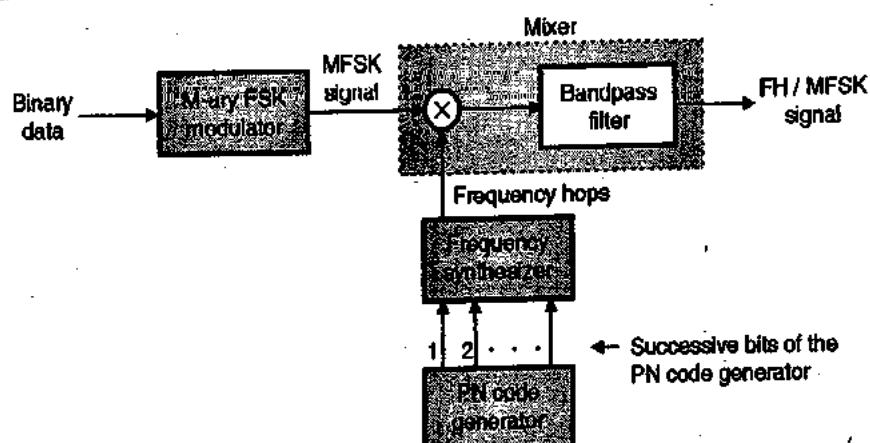
- In slow frequency hopping the symbol rate R_s of the MFSK signal is an integer multiple of the hop rate R_h .
- That means several symbols are transmitted corresponding to each frequency hop.
 \therefore Each frequency hop \Rightarrow Several symbols.
 i.e. frequency hopping takes place slowly.

Fast frequency hopping :

- In the fast frequency hopping the hop rate R_h is an integer multiple of the MFSK symbol rate R_s .
- That means during the transmission of one symbol, the carrier frequency will hop several times.
 \therefore Each symbol transmission \Rightarrow Several frequency hops.
- Thus the frequency hopping takes place at a fast rate.

1.47 Slow Frequency Hopping :

- Fig. 1.47.1 shows the block diagram of a slow-frequency hopping FH/MFSK transmitter.



(L-69) Fig. 1.47.1 : Frequency hop spread M-ary FSK transmitter

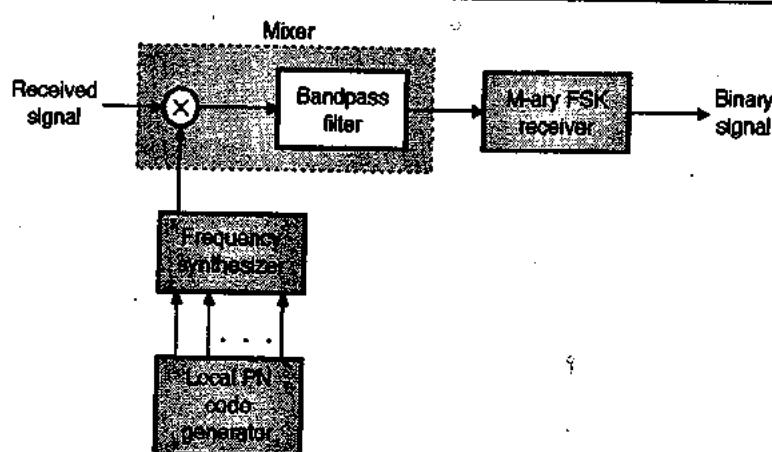
1.47.1 Operation of the FH/MFSK Transmitter :

- The binary data sequence $b(t)$ is applied to the M-ary FSK modulator the output of which goes to the input of the mixer.
- The other input to the mixer block is obtained from a digital frequency synthesizer. The mixer consists of a multiplier followed by a bandpass filter.
- At the multiplier output we get the two input frequencies, their sum and their difference frequency components.
- The bandpass filter is designed to select only the sum frequency component rejecting all other components. This sum components of frequency is then transmitted.
- Successive K-bits of the input binary data sequence will form one symbol. M such symbols can be transmitted using the M-ary FSK system with $M = 2^k$.
- The M-ary FSK modulator will assign a distinct frequency for each of these M symbols.
- Thus the frequency of mixer input obtained from MFSK modulator is changing continuously.
- The other input to the mixer is obtained from the digital frequency synthesizer. The synthesizer output at a given instant of time is the "frequency hop".
- Each frequency hop is mixed with the MFSK signal to produce the transmitted signal.
- The frequency hops at the output of the synthesizer are controlled by the successive bits at the output of the PN code generator.

- The output bits of the PN generator change randomly. Therefore the synthesizer output frequency will also change randomly.
- Hence the frequency hops produced will vary in a random manner.
- If the number of successive bits at the output of PN generator is "n", then the total number of frequency hops will be 2^n .
- The total bandwidth of the transmitted FH/MFSK signal is equal to the sum of all the frequency hops.
- Therefore the bandwidth of the transmitted FH/MFSK signal is very large of the order of few GHz.

1.47.2 FH/MFSK Receiver :

- Due to the large bandwidth occupied by the FH/MFSK signal, the coherent detection of this signal is possible within each hop.
- This is because for coherent detection, the phase synchronization of the locally generated carrier with the transmitted carrier is essential.
- But the frequency synthesizers used in FH/MFSK receiver are unable to maintain this phase coherence over successive hops.
- Therefore most frequency hop spread spectrum systems use the non-coherent M-ary modulation schemes.
- The block diagram of an FH-MFSK receiver is as shown in Fig. 1.47.2.



(L-61) Fig. 1.47.2 : An FH-MFSK receiver

Operation of FH/MFSK receiver :

- The received signal is applied to a mixer. The other input to the mixer comes from a digital frequency synthesizer.
- This digital synthesizer is driven by a PN code generator which is synchronized with the PN code generator at the transmitter and generates the same code sequence.
- Therefore the frequency hops produced at the synthesizer output will be identical to those at the synthesizer output at the transmitter.
- At the output of the multiplier we get the input signals, their sum and difference (as far as frequency is concerned).
- Out of these frequency components, the difference frequency component is selected by the bandpass filter that follows the multiplier.
- This difference signal is the MFSK signal. Thus the mixer removes the frequency hopping.
- The MFSK signal at the mixer output is then applied to a non-coherent MFSK demodulator. At the output of the MFSK detector we obtain the digital modulating signal $b(t)$.
- The non-coherent M-ary FSK detector can be implemented by using a bank of M , non coherent matched filters.
- Each matched filter is matched to one of the tones of the MFSK signal. The largest output out of the M available outputs of filters is selected to obtain the digital modulating signal.

1.48 Fast Frequency Hopping :

- As explained earlier, the fast FH/MFSK system is different than the slow FH/MFSK system.
- Because in the fast FH/MFSK system, there are multiple hops for each M -ary symbol. Hence each hop is a "chip".
 $\therefore \text{Chip rate } R_c = \text{Rate of hopping } R_h$
- The fast frequency hopping is used for defeating a smart jammer who tries to interfere the transmission.
- Before the jammer could understand the frequency band which is being used by the transmitter, the transmitted signal is hopped to a new carrier frequency.
- The principle of fast frequency hopping is illustrated in Fig. 1.48.1 (on next page).
- The data sequence used for the fast hopping is same as the one used for the slow hopping.

- The number of bits per MFSK symbol = $k = 2$. Therefore the number of MFSK tones = $2^k = 4$.
- The length of PN segment per hop i.e. $n = 3$. Therefore the total number of frequency hops = $2^n = 8$.
- The PN sequence decides the hopping frequency (shown by dotted lines in Fig. 1.48.1(a)). Two successive input binary bits 0 1 form the first symbol.
- During this symbol duration the PN sequence (3 digit) has two distinct values viz. : 001 and 110.
- Therefore one symbol duration corresponds to two frequency hops. As shown in Fig. 1.48.1(b) the frequency of the MFSK modulator for symbol 01 is f_2 and the outputs of the synthesizer corresponding to 001 and 110 outputs of the PN sequence generator are say FH_1 and FH_6 .
- Therefore the transmitted frequencies are $(FH_1 + f_2)$ and $(FH_6 + f_2)$. The operation for the first symbol 01 is summarized below.

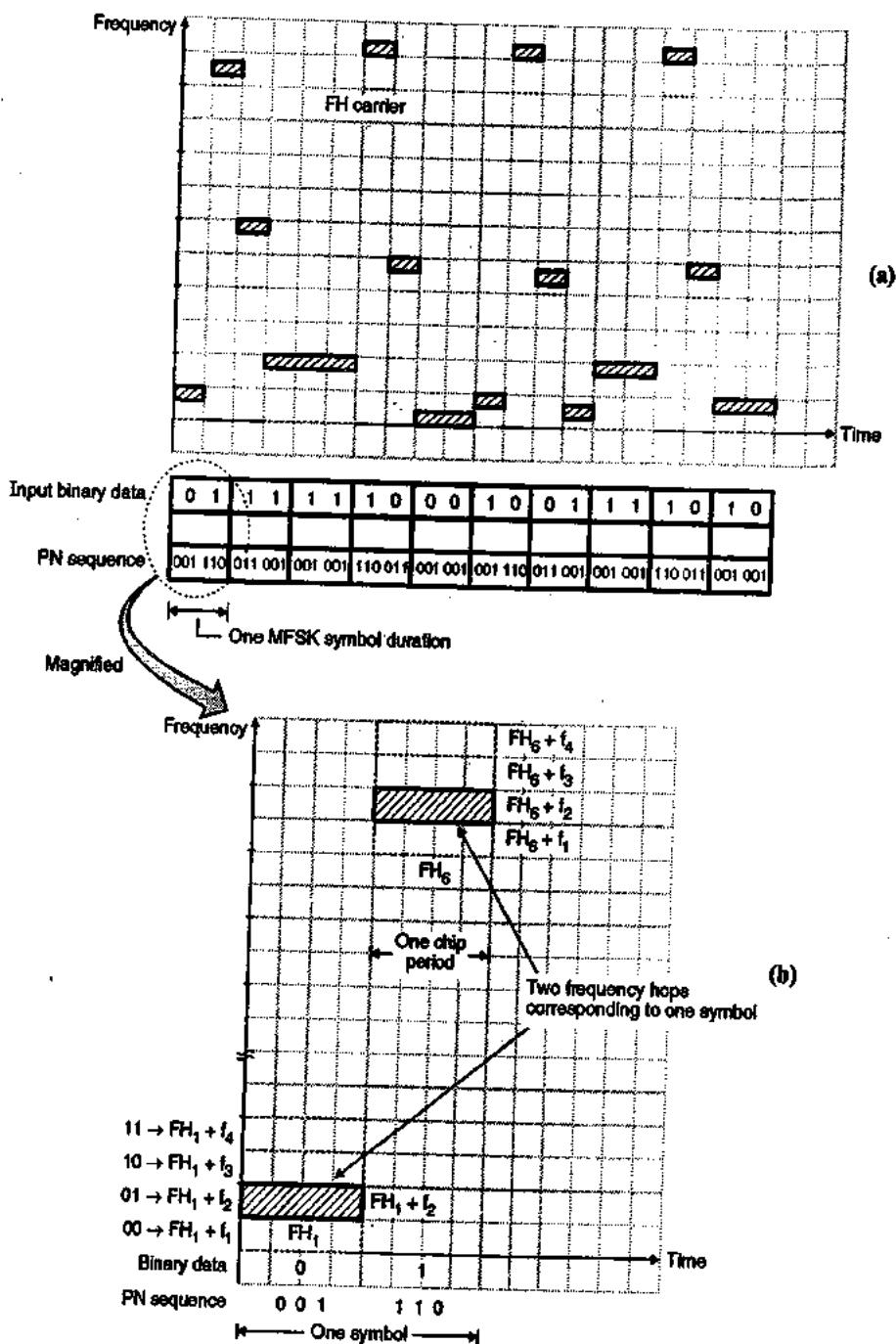
Summary of operation in the first symbol duration :

Symbol : 01	
Frequency of MFSK modulator = f_2	
Output of PN code generator	Frequency of synthesizer (hop)
0 0 1	FH_1
1 1 0	FH_6
Transmitted frequencies : $(f_2 + FH_1)$ and $(f_2 + FH_6)$	

Receiver used for fast hopping :

- For the recovery of the data, at the receiver, noncoherent detection is used.
- But the detection procedure is very much different from that used for a slow FH/MFSK system.
- In practice the following two procedures are considered :
 1. In this procedure, a separate decision is made on the k frequency-hop chips received. Then the estimation of the dehopped MFSK symbol is done based on the simple rule based on majority vote.
 2. In the second procedure, for each FH/MFSK symbol likelihood functions are computed, as functions of the total signal received over k chips and the largest one of them is selected.

The receiver based on the second procedure minimizes the average probability of error. Hence practically it is preferred.



(E-1) Fig. 1.48.1 : Waveforms of fast hopping system

1.49 Advantages and Disadvantages of DS-SS and FH-SS Systems :

1.49.1 Advantages and Disadvantages of the DS-SS System :

Advantages :

1. This system has a very high degree of discrimination against the multipath signals. Therefore the interference caused by the multipath reception is minimized successfully.
2. The performance of DS-SS system in presence of noise is superior to other systems such as FH-SS system.

3. This system combats the intentional interference (jamming) most effectively.

Disadvantages :

1. With the serial search system, the acquisition time is too large. This makes the DS-SS system slow.
2. The sequence generated at the PN code generator output must have a high rate. The length of such a sequence needs to be long enough to make the sequence truly random.
3. The channel bandwidth required, is very large. But this bandwidth is less than that of a FH-SS system.
4. The synchronization is affected by the variable distance between the transmitter and receiver.



1.49.2 Advantages and Disadvantages of FH-SS System :

Advantages :

1. The synchronization is not greatly dependent on the distance.
2. The serial search system with FH-SS needs shorter time for acquisition.
3. The processing gain PG is higher than that of DS-SS system.

Disadvantages :

1. The bandwidth of FH-SS system is too large (in GHz).
2. Complex and expensive digital frequency synthesizers are required to be used.

1.50 Comparisons :

1.50.1 Comparison of Slow and Fast Frequency Hopping :

- Table 1.50.1 shows the comparison of FH-SS methods.

Table 1.50.1

Sl. No.	Slow frequency hopping	Fast frequency hopping
1.	More than one symbols are transmitted per frequency hop.	More than one frequency hops are required to transmit one symbol.
2.	Chip rate is equal to the symbol rate.	Chip rate is equal to the hop rate.
3.	Symbol rate is higher than hop rate.	Hop rate is higher than symbol rate.
4.	Same carrier frequency is used to transmit one or more symbols.	One symbol is transmitted over multiple carriers in different hops.
5.	A jammer can detect this signal if the carrier frequency in one hop is known.	A jammer can't detect this signal because one symbol is transmitted using more than one carrier frequencies.

1.50.2 Comparison of DS-SS and FH-SS Systems :

Sl. No.	Parameter	Direct sequence spread spectrum	Frequency hopping spread spectrum
1.	Definition	PN sequence of large bandwidth is multiplied with narrow band data signal.	Data bits are transmitted in different frequency slots which are changed by PN sequence.

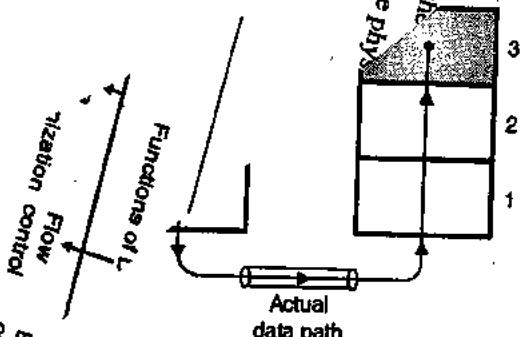
Sl. No.	Parameter	Direct sequence spread spectrum	Frequency hopping spread spectrum
2.	Chip rate	It is fixed $R_c = \frac{1}{T_c}$	$R_t = \max(R_s, R_v)$
3.	Modulation technique	BPSK	M-ary FSK
4.	Acquisition time	Long	Short
5.	Effect of distance	This system is distance relative	Effect of distance is less

Review Questions

- Q. 1 Write a short note on MAN.
- Q. 2 Write a short note on WAN.
- Q. 3 Compare LAN, WAN and MAN.
- Q. 4 Define peer.
- Q. 5 How does the actual data transfer take place between two machines.
- Q. 6 Write a note on : Virtual communication between layers.
- Q. 7 Discuss the important design issues for various layers.
- Q. 8 Write a note on connection oriented and connectionless services.
- Q. 9 What is relationship between services and protocols ?
- Q. 10 Draw the OSI reference model and explain the functions of different layers.
- Q. 11 Compare different types of network topologies.
- Q. 12 State the difference between broadcast and point to point networks.
- Q. 13 Compare peer to peer and client server networks.
- Q. 14 State the reasons for having a layered protocol architecture and state its advantages and disadvantages.
- Q. 15 What are the design issues for the layers ?
- Q. 16 Define : Interfaces and services.
- Q. 17 Name the different network topology types.
- Q. 18 Explain the basic concepts of bus topology with the help of suitable diagram.
- Q. 19 State the important characteristics of bus topology.

- Q. 20 Name the transmission media used for bus LANs.
- Q. 21 State advantages and disadvantages of bus topology.
- Q. 22 Write a note on : Ring topology.
- Q. 23 What are the problems faced by the ring topology ?
- Q. 24 State the advantages and disadvantages of ring topology.
- Q. 25 Write a short note on star topology.
- Q. 26 What is the difference between single level star topology and two level star topology.
- Q. 27 State the advantages and disadvantages of star topology.
- Q. 28 Write a short note on Mesh topology.
- Q. 29 State advantages and disadvantages of mesh topology.
- Q. 30 Write a short note on tree topology.
- Q. 31 Compare Ring and Bus.
- Q. 32 Compare Star and Ring.
- Q. 33 Explain the TCP / IP reference model
- Q. 34 Compare the OSI and TCP / IP reference models.
- Q. 35 Explain the classification of transmission media.
- Q. 36 What is the difference between guided and unguided transmission media ?
- Q. 37 State the types of guided media.
- Q. 38 Explain the difference between UTP and STP.
- Q. 39 What is the effect of twisting the wires in UTP cables ?
- Q. 40 Give applications of co-axial cable.
- Q. 41 Compare the guided transmission media.
- Q. 42 State advantages of optical fiber cable.
- Q. 43 State the applications of microwave communication.
- Q. 44 In the context of the fiber optic communication system explain the meaning of the following :
1. Step index fiber
 2. Graded index fiber
 3. Multimode fibers
- Q. 45 Explain the function of repeaters.
- Q. 46 Compare repeater and hub.
- Q. 47 Write a note on : Bridges.
- Q. 48 With the help of suitable explanatory diagram, explain the routers and gateways.
- Q. 49 Explain different types of switches.
- Q. 50 Compare switches and hub.
- Q. 51 What is line coding ?
- Q. 52 Explain differential manchester code.
- Q. 53 Define manchester encoding.
- Q. 54 Write a short notes on : WLAN.
- Q. 55 Write a short notes on : WPAN.
- Q. 56 How is SS signal different from the normal one ?
- Q. 57 State true or false : The SS signal is pseudorandom in nature.
- Q. 58 State some applications of modulation.
- Q. 59 Name various modulations.
- Q. 60 Which modulation is best?
- Q. 61 Explain the following terms:
- Q. 62

Fig. 2.3.1
1 : Functions of data link layer
2 : Transfer of data
3 : Communication



(b) Actual data path



Logical Link Control

Unit II

Syllabus :

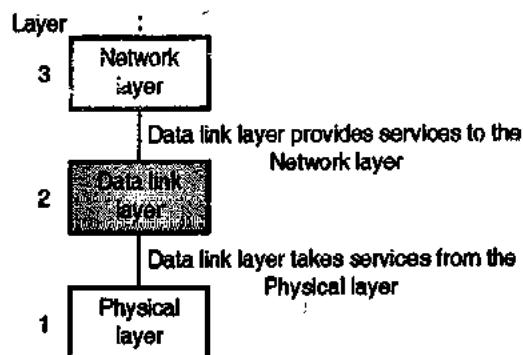
Design Issues: Services to Network Layer, Framing, Error Control and Flow Control. Error Control : Parity Bits, Hamming Codes (11/12-bits) and CRC. Flow Control Protocols: Unrestricted Simplex, Stop and Wait, Sliding Window Protocol, WAN Connectivity : PPP and HDLC.

2.1 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.

2.1.1 Position of Data Link Layer :

- Fig. 2.1.1 shows the position of data link layer in the five layer Internet model. It is the second layer.

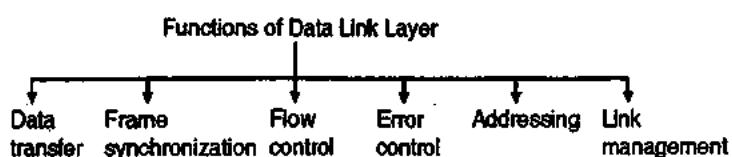


(L-66) Fig. 2.1.1 : Position of data link layer

- It receives services from the physical layer and provides services to the network layer.

2.2 Data Link Layer Design Issues (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-66) Fig. 2.2.1 : 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 :

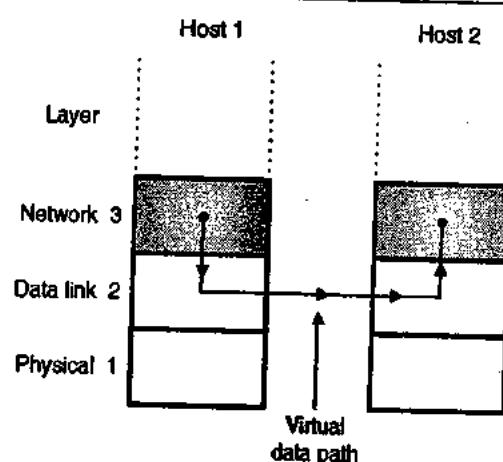
The data and control information is combined in a frame and transmitted from the source to destination machine. The destination machine must be able to separate out the control information from the data being transmitted.

7. Link management :

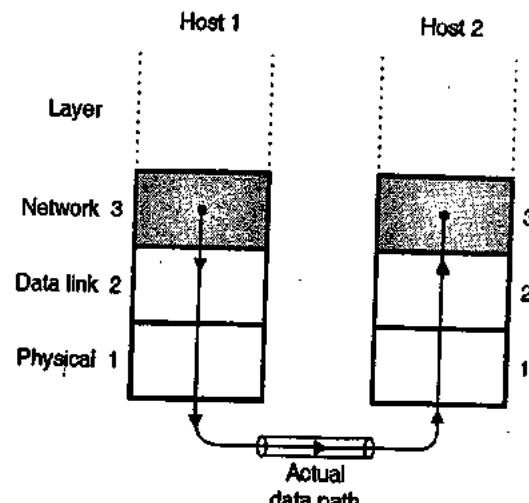
The communication link between the source and destination is required to be initiated, maintained and finally terminated for effective exchange of data. It requires co-ordination and co-operation among all the involved stations. Protocols or procedures are required to be designed for the link management.

2.3 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. 2.3.1(a). It is not the actual path.
- The actual path followed by the data from sending machine to destination is shown in Fig. 2.3.1(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. 2.3.1(a)) using a data link layer protocol.



(a) Virtual communication



(b) Actual data path

2.3.1 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.

2.3.2 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.

2.3.3 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.

2.3.4 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.

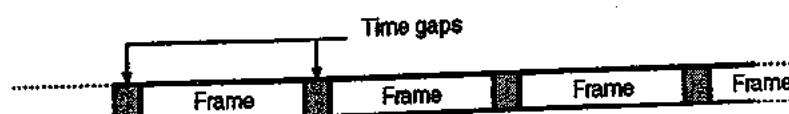
- All the frames are guaranteed to be received in the same order as the order of transmission. Each received frame will be acknowledged individually by the destination machine.
- The data transfer takes place by following three distinct phases given below :
 1. Connection is established.
 2. The data frames are actually transmitted.
 3. The connection is released after completion of data transfer.

2.4 Framing :

- The bits to be transmitted is 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.
- Breaking the bit stream into frames is called as framing. One way of doing it is by inserting time gaps between frames as shown in Fig. 2.4.1.
- 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.

2.4.1 Framing Methods :

- Following methods are used for carrying out framing :
 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.



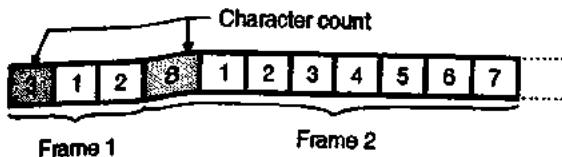
(G-178) Fig. 2.4.1 : Framing

2.4.2 Character Count :

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. 2.4.2.



(L-68) Fig. 2.4.2 : Character count method

- The two frames shown in Fig. 2.4.2 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.

2.4.3 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).

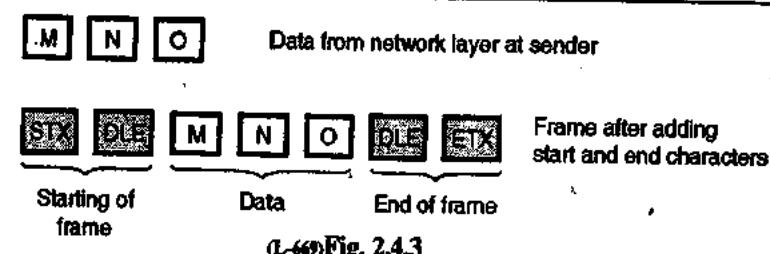
- After each frame the ASCII character sequence DLE ETX is transmitted. Here DLE stands for Data Link Escape and ETX stands for End of TeXt.
- So if the receiver loses the synchronization, it just has to search for the DLE STX or DLE ETX characters to return back on track. This is shown in Fig. 2.4.3.

2.4.4 Character Stuffing :

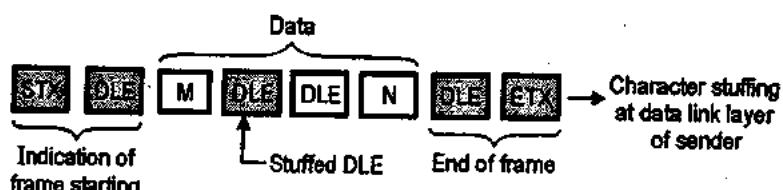
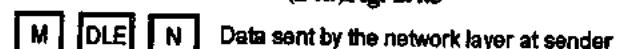
- The problem with this system is that the characters DLE STX or DLE ETX can be a part of data as well.
- If so, they will be misinterpreted by the receiver as start or end of frame.
- This problem is solved by using a technique called character stuffing, which is as follows.
- The data link layer at 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. 2.4.4. Note that at the receiving end the destuffing is essential. Destuffing process is exactly opposite to the character stuffing process.

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.



(L-69) Fig. 2.4.3



(G-18) Fig. 2.4.4 : Character stuffing

Byte stuffing :

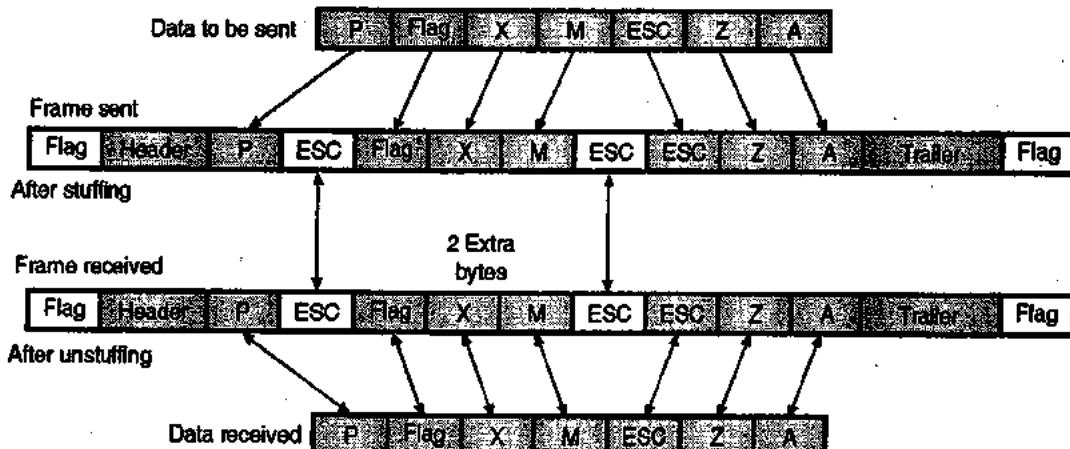
- In byte stuffing a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is called as the escape character (ESC).
 - At the receiver these ESC bytes are removed from the data section and the next character is treated as data.
 - Fig. 2.4.5 demonstrates the concept of byte stuffing.
 - Byte stuffing by the escape character will allow the presence of the flag in the data section of the frame. But it has a problem, if the text contains one or more escape characters followed by a flag.
 - Because then the receiver will remove the escape character but will keep the flag.
 - This problem is solved by marking the escape characters that are a part of the text by another escape (ESC) character as shown in Fig. 2.4.5.

2.4.5 Starting and Ending Flags, with Bit Stuffing :

- In this framing techniques 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. 2.4.6.
 - 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. 2.4.6.
 - Due to bit stuffing, the possible problem if the data contains the flag byte pattern (0111 1110) is eliminated.



(G-18) Fig. 2.4.5 : Byte-stuffing

Original data :

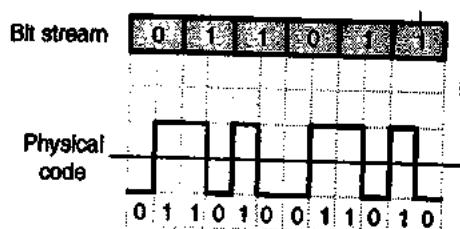
0	1	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Data after destuffing :	<table border="1"><tr><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr></table>	0	1	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1
0	1	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1		

(G-183) Fig. 2.4.6 : Bit stuffing and destuffing

2.4.6 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. 2.4.7. 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. 2.4.7. 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.



(G-184)Fig. 2.4.7

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.

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 :

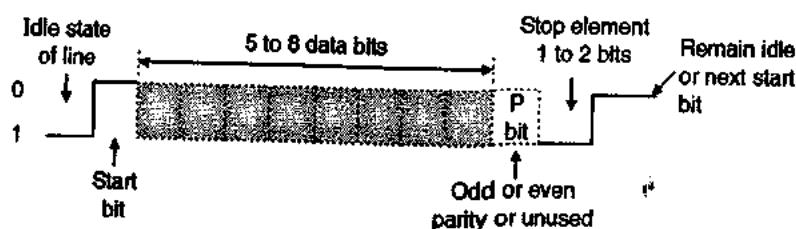
1. Asynchronous
2. Synchronous

Asynchronous frame format :

- The asynchronous frame format is shown in Fig. 2.4.8. 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. 2.4.9.
- 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 synchronisation is to include the clocking information in the data signal itself.



(G-185)Fig. 2.4.8 : Asynchronous frame format



(G-186)Fig. 2.4.9 : Synchronous frame format



- As shown in the Fig. 2.4.9, 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.

2.5 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.

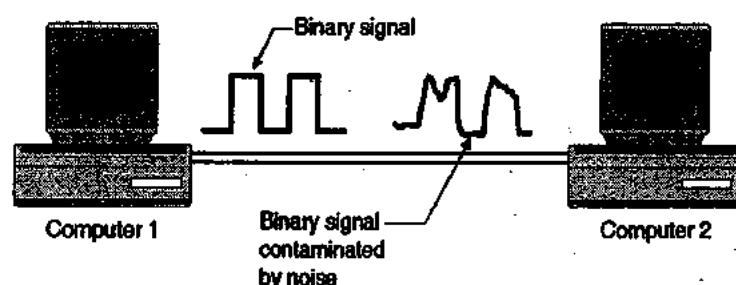
2.5.1 Function of a Timer :

- 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.

2.6 Error Detection and Correction :

- When transmission of digital signals takes place between two systems such as computers as shown in Fig. 2.6.1, the signal get contaminated due to the addition of "Noise" to it.
- 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 error can become a serious threat to the accuracy of the digital system. Therefore it is necessary to detect and correct the errors.



(L-302) Fig. 2.6.1 : Noise contaminates the binary signal

Types of errors :

The errors introduced in the data bits during their transmission can be categorised as :

1. Content errors
 2. Flow integrity errors.
- 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.
 - 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.

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. 2.6.2.

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. 2.6.3 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. 2.6.3.

Disadvantages of coding :

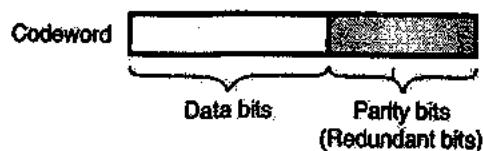
Some of the disadvantages of the coding technique are :

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.

2.6.1 Important Definitions Related to Codes :

Codeword :

The codeword is the n bit encoded block of bits. As already seen it contains message bits and parity or redundant bits, as shown in Fig. 2.6.4.



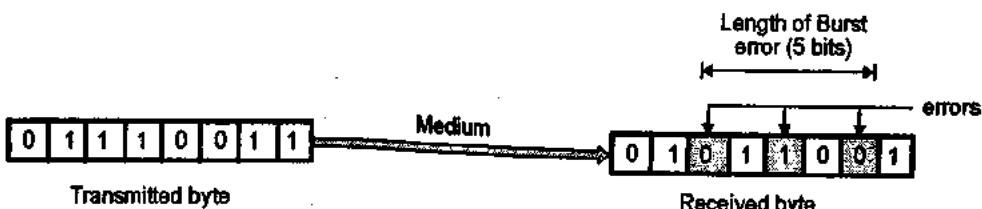
(L-30) Fig. 2.6.4 : Structure of a transmitted codeword
Code rate :

The code rate is defined as the ratio of the number of message bits (k) to the total number of bits (n) in a codeword.

$$\therefore \text{Code rate } (r) = \frac{k}{n} \quad \dots(2.6.1)$$



(G-18) Fig. 2.6.2 : Single bit error



(G-18) Fig. 2.6.3 : Burst errors

Hamming weight of a codeword [$w(x)$] :

The Hamming weight of a codeword x is defined as the number of non zero elements in the codeword. Hamming weight of a code vector (codeword) is the distance between that codeword and an all zero code vector. (A code having all elements equal to zero).

Code efficiency :

The code efficiency is defined as the ratio of message bits to the number of transmitted bits per block.

$$\therefore \text{Code efficiency} = \text{Code rate} = \frac{k}{n} \quad \dots(2.6.2)$$

Hamming distance :

- Consider two code vectors (or codewords) having the same number of elements.
- The "Hamming distance" or simply distance between the two codewords is defined as the number of locations in which their respective elements differ. For example consider the two codewords given below :

(G-19(a))

Code word No.1	:	1	1	1	1	0	1	0	0
		↓	↑	↑	↑	↓			
Code word No.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.

Minimum distance d_{\min} :

- 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 codeword is less than the minimum distance d_{\min} , because then the erroneous word is not a valid codeword.

- But when the number of errors equals or exceeds d_{\min} , the erroneous codeword may correspond to another valid codeword and errors cannot be detected.
- The error detection and correction capabilities of a coding technique depend on the minimum distance as shown in the Table 2.6.1.

Table 2.6.1 : 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. 2.6.1 : Find the Hamming weight of the following code vector :

$$x = 11010100$$

Soln. :

As the number of non-zero elements in the above codeword is 4, the Hamming weight $W(x) = 4$.

2.6.2 Error Detection :

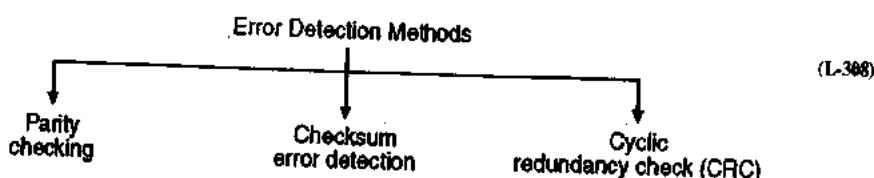
- When a codeword is transmitted, one or more number of transmitted bits will be reversed (0 to 1 or vice versa) due to transmission impairments.
- Thus errors will be introduced.
- It is possible for the receiver to detect these errors if the received codeword (corrupted) is not one of the valid codewords.
- 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. 2.6.5.
- 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.

Transmitted code word	1 0 1 0 1 1 0 0	1 1 1 0 1 0 1 1	0 0 1 0 0 1 0 1
Received code word	1 0 1 0 1 1 0 0 ↓ error	1 1 1 0 1 0 1 1 ↓ error	0 0 1 0 0 0 0 1 ↓ error
Number of errors	1	2	3
Distance	1	2	3

(L-305) Fig. 2.6.5

2.6.3 Error Detection Methods :

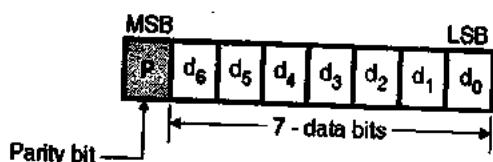
- Some of the most important error detection methods are as follows :



- Before thinking of correcting the errors introduced in the data bits it is necessary to first detect them. Some of the popular error detection methods are as follows :
 1. Parity checking
 2. Checksum error detection
 3. Cyclic Redundancy Check (CRC).
- For error detection and correction it is necessary to add some check bit to a block of data bits. These check bits are also known as redundant bits because they do not carry any useful information.

2.6.4 Parity :

- 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. 2.6.6, 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.

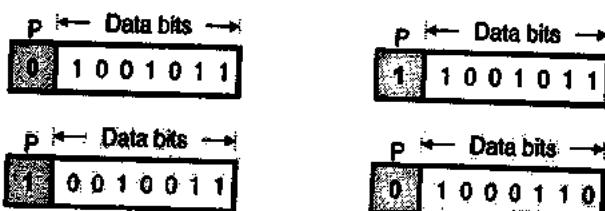


(L-309) Fig. 2.6.6 : Format of a transmitted word with parity bit

- 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...).

Use of parity bit to decide parity :

- The parity bit can be set to 0 or 1 depending on the type of parity required.

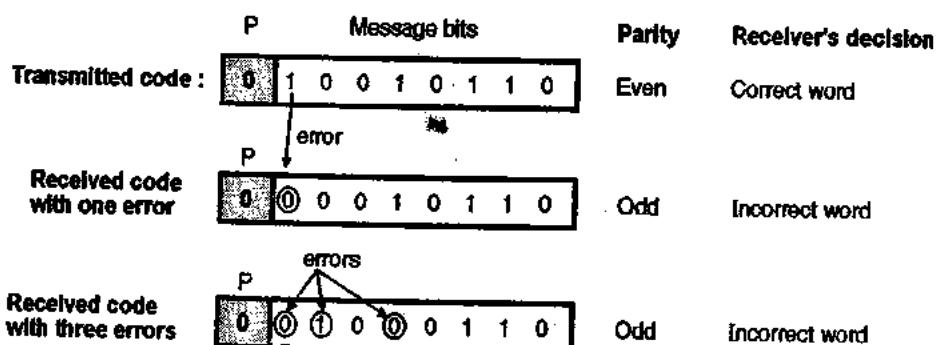


(a) Inclusion of a parity bit to obtain an even parity (b) Inclusion of a parity bit to parity obtain the odd parity

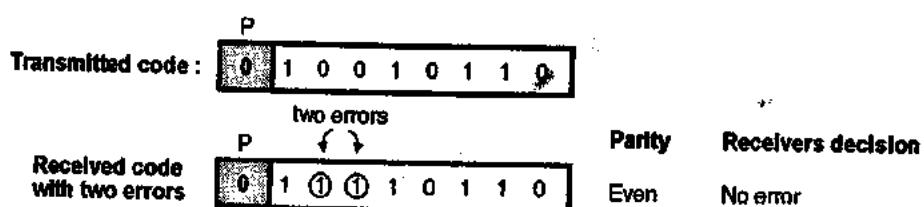
(L-310) Fig. 2.6.7

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. 2.6.8.
- If a single error or an odd number of bits change due to errors introduced during transmission the parity of the codeword will change.
- Parity of the received codeword 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. 2.6.8.
- 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.



(L-311) Fig. 2.6.8 : The receiver detects the presence of error if the number of errors is odd i.e. 1, 3, 5



(L-312) Fig. 2.6.9 : The receiver cannot detect the presence of error if the number of errors is even i.e. 2, 4, 6

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 codeword will not change. It will still remain even as shown in Fig. 2.6.9 and the receiver will fail to detect the presence of errors.

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.

Ex. 2.6.2 : Write the ASCII code of word "HOLE" using even parity.

Soln. : The following table shows the ASCII code of word HOLE using even parity.

Table P. 2.6.2

		7	6	5	4	3	2	1
H		1	0	0	1	0	0	0
O		1	0	0	1	1	1	1
L		1	0	0	1	1	0	0
E		1	0	0	0	1	0	1

Note that the parity bits are selected in order to obtain an even parity for each row (i.e. for each letter).

Burst errors :

- The errors generally occur in bursts. The reason for generation of burst errors can be an external interference such as lightning which lasts for a duration of several bits.
- So the noise or interference produced by the lightning will corrupt a block of several bits. Such errors are called as burst errors.
- The parity checking method is not useful in detecting the burst errors.
- The checksum and cyclic redundancy check (CRC) methods can detect the burst errors.

Checksum for error detection :

- As discussed in the previous section, simple parity cannot detect two or even number of errors within the same codeword.



- One way to overcome this problem is to use a sort of two dimensional parity.
- 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. 2.6.9(A). The final carry is ignored.

$$\begin{array}{r} \text{Word A : } 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \\ + \\ \text{Word B : } 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \\ \hline \text{Sum : } 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \end{array}$$

Fig. 2.6.9(A) : Concept 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 transmitted.
- 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". Hence the carries of the MSB are ignored while finding out the checksum byte.
- The generation of checksum will be clear if you refer to the following example.

Ex. 2.6.2(A) : Find the checksum of the following message.

10110001, 10101011, 001101
01,10100001

Soln. : Ignored (G-1943)

Checksum		10	1	0	1	1	1	0
Data bytes		+	1	0	1	1	0	0
		+	1	0	1	0	1	1
		+	0	0	1	1	0	1
		+	1	0	1	0	0	0
Checksum byte		0 0 1 1 0 0 1 0						

Note that the carries of MSB have been ignored while writing the checksum byte.

How to detect 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 transmitted after the data bytes.

- If the contents of the accumulator is zero after accumulation of the 2's complement of the checksum byte then it indicates that there are no errors.

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.

2.6.5 Two Dimensional Parity Check :

- 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. 2.6.10.
- 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 :
 - 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. 2.6.10.

The Vertical Redundancy Check (VRC) Bits :

- As shown in Fig. 2.6.10 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

(G-1944)

← VRC bit = 1 to make the parity of first column even

- 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. 2.6.10.



Characters	C	O	M	P	U	T	E	R
b_1	1	1	1	0	1	0	1	0
b_2	1	1	0	0	0	0	0	1
b_3	0	1	1	0	1	1	1	0
b_4	0	1	1	0	0	0	0	0
b_5	0	0	0	1	1	1	0	1
b_6	0	0	0	0	0	0	0	0
b_7	1	1	1	1	1	1	1	1
VRC bits (even parity) \rightarrow	1	1	0	0	0	1	1	1

These bits will make the parity of each column even

LRC bits \rightarrow These bits (even parity) will make the parity of each row even

(1-315) Fig. 2.6.10 : Vertical and longitudinal parity check bits

The Longitudinal Redundancy Check (LRC) Bits :

- The LRC bits are parity bits associated with the rows of the data block of Fig. 2.6.10.
- Each LRC bit will make the parity of the corresponding row, an even parity. For example, consider row 1 of Fig. 2.6.10.

Row 1 : **b₁ 1 1 1 0 1 0 1 0** ← 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.

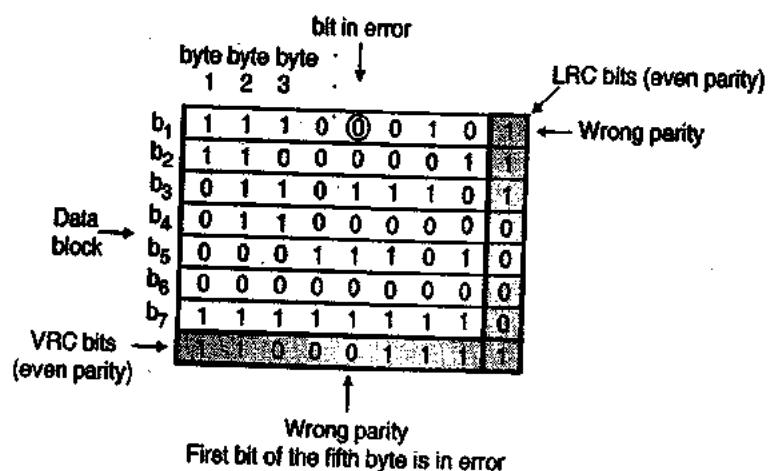
Ex. 2.6.3 : The following bit stream is encoded using VRC, LRC and even parity. Locate and correct the error if it is present.

11000011 1111001110110010
00001010
00101010 001010110100011
01001011
11100001

Soln. :

- Fig. P. 2.6.3 shows the received data block alongwith the LRC and VRC bits.
- 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.



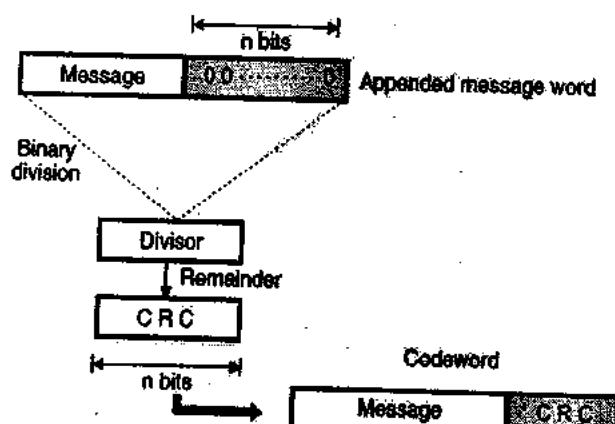
(G-199) Fig. P. 2.6.3

2.6.6 Cyclic Redundancy Check (CRC) :

- 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 dataword (message) polynomial $M(x)$ with the help of long division.
- This technique is more powerful than the parity check and checksum 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.

CRC generator :

- The CRC generator is shown in Fig. 2.6.11.



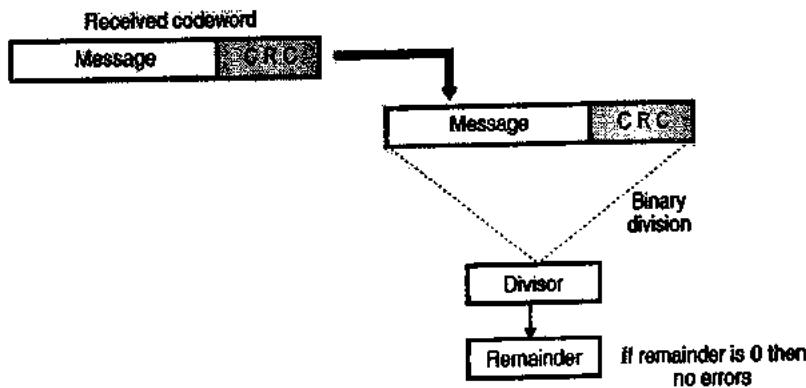
(L-819) Fig. 2.6.11 : CRC generator

- The stepwise procedure in CRC generation is as follows :

- Step 1 : Append a train of n 0s to the message word where n is 1 less than the number of bits in the predecided divisor (i.e. generator word). If the divisor is 5-bit long then we have to append 4-zeros to the message.
- Step 2 : Divide the newly generated data unit in step 1 by the divisor (generator). This is a binary division.
- Step 3 : The remainder obtained after the division in step 2 is the n bit CRC.
- Step 4 : This CRC will replace the n 0s appended to the data unit in step 1, to get the codeword to be transmitted as shown in Fig. 2.6.11.

CRC checker :

- Fig. 2.6.12 shows the CRC checker.



Q-82) Fig. 2.6.12 : CRC checker

- The codeword received at the receiver consists of message and CRC. (Fig. 2.6.12)
 - 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.
 - 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.

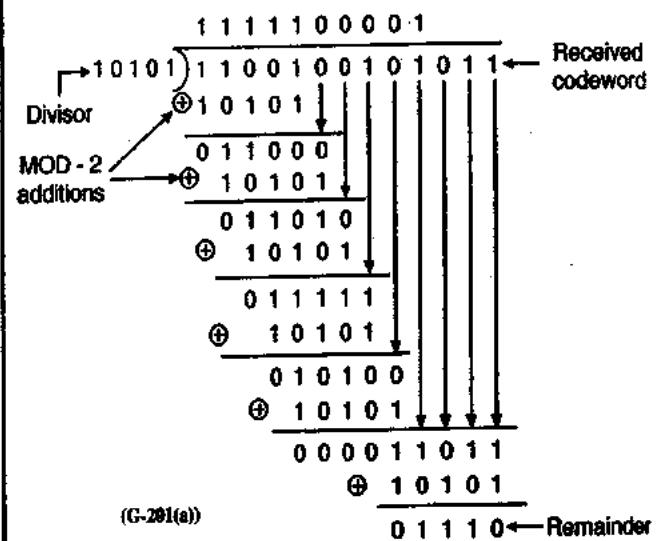
Ex. 2.6.4: The codeword is received as 1100 1001 01011. Check whether there are errors in the received codeword, if the divisor is 10101. (The divisor corresponds to the generator polynomial).

Soln. i

- 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.

Data word : 1100 1001 01011

Divisor : 10101



The non zero remainder shows that there are errors in the received codeword.

Generation of CRC code :

The generation of CRC code is clear after solving the following example.

Ex. 2.6.5 : Generate the CRC code for the data word of 1 100 10101. The divisor is 10101.

Soln. i

Given : Data word : 110010101

Divisor : 10101.

The number of data bits = m = 9

The number of bits in the codeword

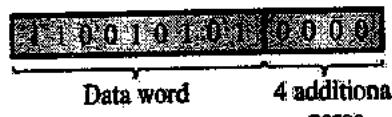
$\approx B \approx 5$

Dividend = Data word

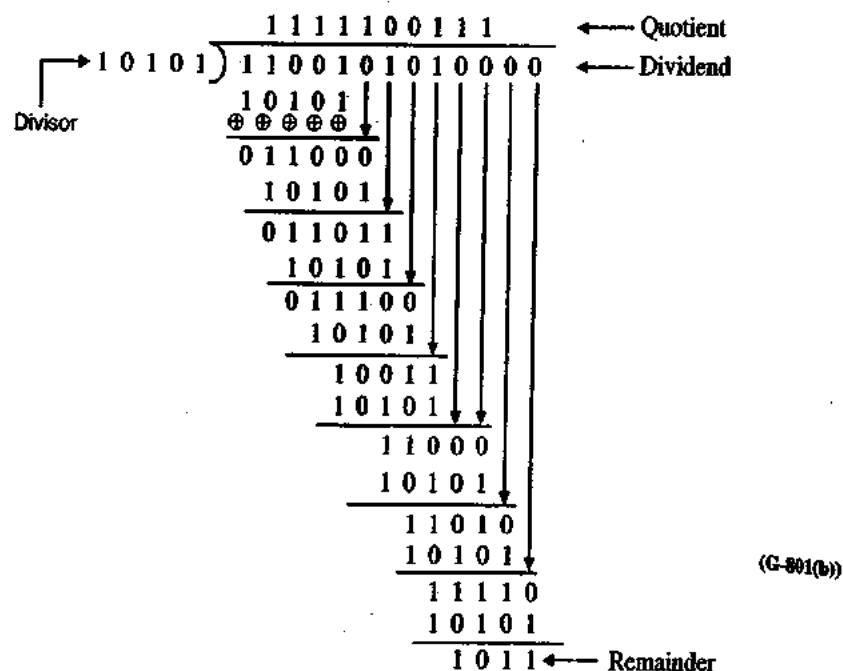
+ (n - 1) zeros.

ANSWER

(G-201(a))



Carry out the division as follows :



Codeword :

In CRC the required codeword is obtained by writing the data word followed by the remainder.

$$\begin{array}{r}
 \text{Dividend} \\
 + \quad \text{1011 Remainder} \\
 \hline
 \text{Codeword} = \boxed{\text{1100101010}} \quad \boxed{\text{1011}}
 \end{array} \quad (\text{G-1761})$$

Data word Remainder

Undetected errors in CRC :

- CRC cannot detect all types of errors.
- The probability of error detection and the types of detectable errors depends on the choice of divisor.

2.6.7 Error Correction :

We are going to discuss two completely different approaches for the error control. They are :

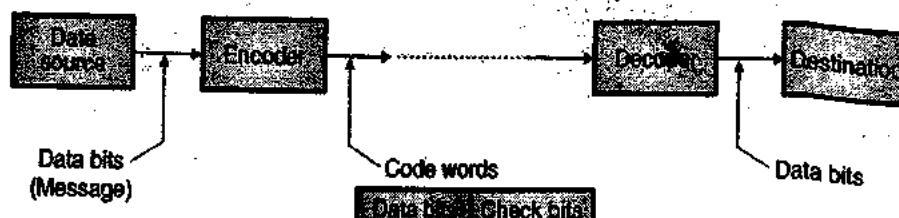
- Forward error correction (FEC)
 - Automatic request for retransmission (ARQ).
- The ARQ technique :** In the ARQ system, the receiver can request for the retransmission of the complete or a part of message if it finds some error in the received message. This needs an additional

channel called feedback channel to send the receiver's request for retransmission.

- The FEC technique :** In the FEC technique there is no such feedback path and request for retransmission. So error correction has to take place at the receiver.

Error correction techniques :

- In the error correction techniques, codes are generated at transmitter by adding a group of parity bits or check bits as shown in Fig. 2.6.13.
- 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. 2.6.13, 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.

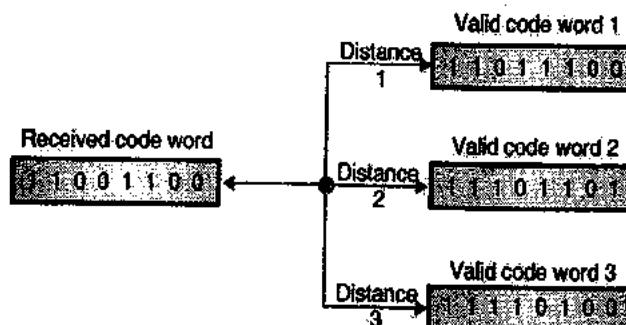


(L-306) Fig. 2.6.13 : Error correction technique



FEC (Forward Error Correction) :

- 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 words 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. 2.6.14.



(L-30) Fig. 2.6.14 : Concept of FEC

- In Fig. 2.6.14, the valid code word 1 has the minimum distance (1), hence it is the most likely correct code word.

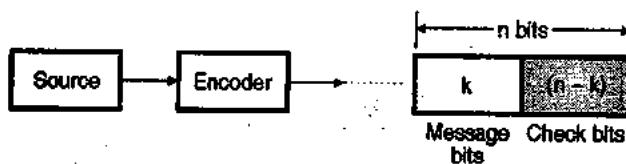
Error correction techniques :

Some of the FEC techniques are as follows :

- Linear block codes.
- Convolutional coding.
- Hamming codes.
- Cyclic codes.

2.6.8 Linear Block Codes :

- The generation of block codes is illustrated in Fig. 2.6.15. 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 block (of k message bits) it adds $(n - k)$ parity bits as shown in Fig. 2.6.15. 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 to the " k " message bits. The n bit code word is thus produced as shown in Fig. 2.6.15.

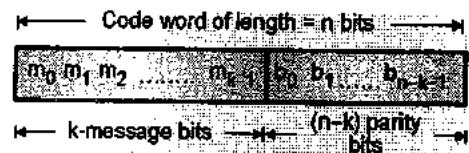
(L-31) Fig. 2.6.15 : Generation of an n bit linear block code

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.

Codeword structure :

The codeword structure of a linear block code is as shown in Fig. 2.6.16.



(G-26) Fig. 2.6.16 : Structure of the codeword for a linear block code

2.6.9 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 :

- Block length : $n = 2^m - 1$
- Number of message bits : $k = 2^m - m - 1 \dots (2.6.3)$
- Number of parity bits : $(n - k) = m$.
Where $m \geq 3$. i.e. minimum number of parity bits is 3.
- The minimum distance $d_{min} = 3$.
- The code rate or code efficiency $= \frac{k}{n}$
 $= \frac{2^m - m - 1}{2^m - 1} = 1 - \frac{m}{2^m - 1} \dots (2.6.4)$

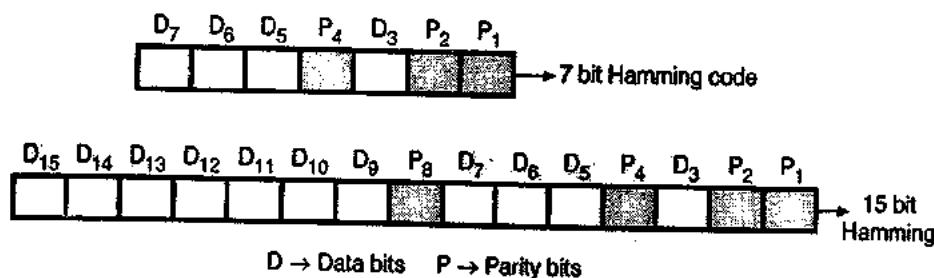
If $m \gg 1$ then code rate $r \approx 1$.

Error detection and correction capabilities of Hamming code :

For the minimum distance $d_{min} = 3$,

- The number of errors that can be detected per word = 2.
since. $d_{min} \geq (s + 1) \therefore 3 \geq s + 1 \therefore s \leq 2$
- 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.



(G-194) Fig. 2.6.17 : Hamming code words

Hamming code structure :

- 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. 2.6.17.
- 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 and P_8 is at 2^3 as shown in Fig. 2.6.17.

7-Bit Hamming Code :

1. 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. 2.6.18.



(G-194) Fig. 2.6.18 : Code word pattern for Hamming code

2. The D bits in Fig. 2.6.18 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 2.6.2(a) gives a listing of minimum number of parity bits needed for various ranges of "m" information bits.

Table 2.6.2(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 :

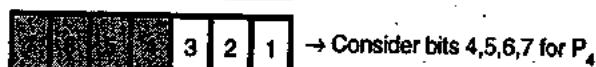
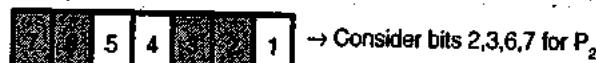
Table 2.6.2(b) indicates which bit positions are associated with each parity bit in order to establish required parity (even or odd) over the selected bits positions.

Table 2.6.2(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,....

Selection of parity bits :**Selection of P₁ :**

P₁ is adjusted to 0 or 1 so as to establish even parity over bits 1,3,5 and 7 i.e. P₁, D₃, D₅ and D₇.



**Selection of P₂:**

P₂ is adjusted to 0 or 1 so as to set even parity over bits 2,3,6 and 7 (P₂, D₃, D₆ and D₇).

Selection of P₄:

P₄ is adjusted to 0 or 1 so as to set even parity over bits 4,5,6 and 7 (P₄, D₅, D₆ and D₇).

The selection of parity bits will be clear after solving the following example.

Ex. 2.6.6 : A bit word 1 0 1 1 is to be transmitted.

Construct the even parity seven-bit Hamming code for this data.

Soln.:**Step 1 : The codeword format :**

The seven bit Hamming code format is shown in Fig. P. 2.6.6 : Given bit word = 1 0 1 1

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
1	0	1		1		

↓↓↓↓↓↓↓
To be decided

(G-1948) Fig. P. 2.6.6

Step 2 : Decide P₁:

P₁ sets the parity of bits P₁, D₃, D₅ and D₇. As D₇, D₅, D₃ = 1 1 1 we have to set P₁ = 1 in order to have the even parity.

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
1	0	1		1		1

↓
Set P₁ = 1 to have
the even parity of P₁, D₃, D₅, D₇

Step 3 : Decide P₂:

P₂ is set to have the even parity of P₂, D₃, D₆ and D₇. But D₃, D₆, D₇ = 1 0 1 hence set P₂ = 0.

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
1	0	1		1	0	1

↓
Set P₂ = 0 to have
even parity of P₂, D₃, D₆ and D₇

Step 4 : Decide P₄:

P₄ is set to have the even parity of P₄, D₅, D₆ and D₇. But D₅, D₆, D₇ = 1 0 1, hence set P₄ = 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 P₄, D₅, D₆, D₇

Ex. 2.6.7 : Encode the data bits 0 1 0 1 into a seven bit even parity Hamming code.

Soln. :

Step 1 : D₇ D₆ D₅ P₄ D₃ P₂ P₁

0	1	0		1		
---	---	---	--	---	--	--

(G-1952)

Step 2 : Select P₁ for P₁, D₃, D₅, D₇:

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
0	1	0		1		1

(G-1953)

P₁ = 1 for P₁, D₃, D₅, D₇ = 1 1 0 0**Step 3 : Select P₂ for P₂, D₃, D₆, D₇:**

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
0	1	0		1	0	1

(G-1954)

P₂ = 0 for P₂, D₃, D₆, D₇ = 0 1 1 0**Step 4 : Select P₄:**

D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	D ₁
0	1	0	1	1	0	1

(G-1955)

Set P₄ = 1 to have P₄, D₅, D₆, D₇ = 1 0 1 0

Hence the complete 7-bit Hamming codeword is as shown below.

0	1	0	1	1	0	1
---	---	---	---	---	---	---

(G-1956)

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 codeword is correct i.e. it does not contain errors.
- But if the parity is not even 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. 2.6.8 : If the 7-bit Hamming codeword received by a receiver is 1 0 1 1 0 1 1. Assuming the even parity state whether the received codeword is correct or wrong. If wrong, locate the bit in error.

Soln. :

(G-1957)

	D ₇	D ₆	D ₅	P ₄	D ₃	P ₂	P ₁
Received codeword :	1	0	1	1	0	1	1

Step 1 : Analyze bits 4, 5, 6 and 7 :

$$P_4 D_5 D_6 D_7 = 1101 \rightarrow \text{Odd parity.}$$

;: error exists here.

\therefore Put $P_4 = 1$ in the 4's position of the error word.

Step 2 : Analyze bits 2, 3, 6 and 7 :

$\therefore P_2 D_3 D_6 D_7 = 1001 \rightarrow$ Even parity so no error.

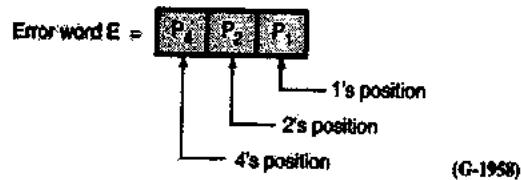
Hence put $P_2 = 0$ in the 2's position of the error.

Step 3 : Check the bits 1, 3, 5, 7 :

$\therefore P_1 D_3 D_5 D_7 = 1011 \rightarrow$ Odd parity so error exists.

Hence put $P_1 = 1$ in the 1's position of the error word.

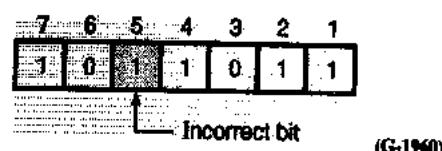
Step 4 : Write the error word :



Substituting the values of P_4 , P_2 and P_1 obtained in steps 1, 2 and 3 we get,

$$E = \boxed{1 \quad 0 \quad 1} \quad (G-1959)$$

Hence bit 5 of the transmitted codeword is in error.



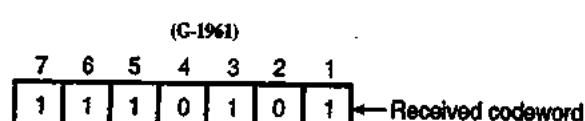
Step 5 : Correct the error :

Invert the incorrect bit to obtain the correct codeword as follows :

Correct codeword = [10010111]

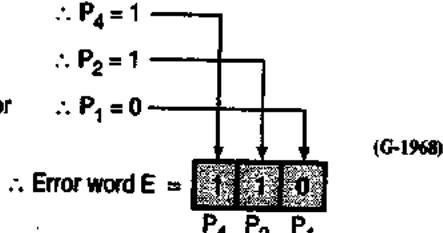
Ex. 2.6.9: A seven bit Hamming code is received as 1 1 1 0 1 0 1. What is the correct code?

Solo 1



1. Check bits 4, 5, 6, 7 → Odd parity, hence error
 2. Check bits 2, 3, 6, 7 → Odd parity, hence error
 3. Check bits 1, 3, 5, 7 → Even parity, hence no error

4. Decimal equivalent of $E = 1\ 1\ 0 = (6)_{10}$



∴ 6th bit in the received codeword is incorrect. So invert it.

∴ Correct codeword : 



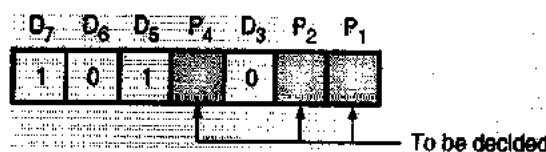
Ex. 2.6.10 : Write the steps to generate the Hamming code. Prepare hamming code for bit pattern 10101010. Suppose while transmitting, error occurs in 7th bit, write the bit pattern at the receiver. Using Hamming code explain how will you detect and correct the error.

Soln. :

- Refer section 2.6.9 for the procedure to generate the Hamming code.
- Let us obtain the 7 bit hamming code for the bit pattern 1010.

Step 1 : The codeword format :

The seven bit Hamming codeword format is shown in Fig. P. 2.6.10(a).



(G-196) Fig. P. 2.6.10(a)

Step 2 : Decide P₁, P₂ and P₄ :

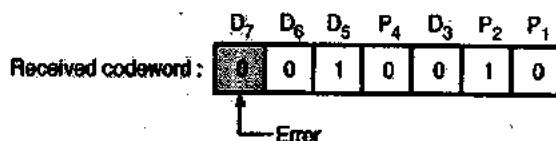
- P₁ sets the parity of P₁, D₃, D₅ and D₇. As D₇, D₅, D₃ = 110, P₁ = 0 so as to have the even symmetry.
- P₂ is set to have the even parity of P₂, D₃, D₆ and D₇. But D₃, D₆, D₇ = 001. Hence P₂ = 1.
- P₄ is set to have the even parity of P₄, D₅, D₆ and D₇. But D₅, D₆, D₇ = 101 so P₄ = 0.
- The codeword is shown in Fig. P. 2.6.10(b).



(G-196) Fig. P. 2.6.10(b)

The error detection and correction :

The 7th bit is in error. So the received codeword is as shown in Fig. P. 2.6.10(c).



(G-195) Fig. P. 2.6.10(c)

Step 3 : Error detection and correction :

- Analyze bits 4, 5, 6, 7
 $P_4 D_5 D_6 D_7 = 0100 \rightarrow$ Odd parity so error exists here.
∴ Put P₄ = 1 in the 4's position of error word.
- Analyze bits 2, 3, 6, 7
 $P_2 D_3 D_6 D_7 = 1000 \rightarrow$ Odd parity so error exists here.
∴ Put P₂ = 1 in the 2's position of error word.
- Check the bits 1, 3, 5, 7
 $P_1 D_3 D_5 D_7 = 0010 \rightarrow$ Odd parity so error exists.
∴ Put P₁ = 1 in the 1's position of error word.
- The error word is shown in Fig. P. 2.6.10(d).

$$\text{Error word } E = \boxed{P_4 \quad P_2 \quad P_1} = \boxed{1 \quad 1 \quad 1}$$

(G-196) Fig. P. 2.6.10(d) : Error word

The decimal equivalent of error word is (7)₁₀. Hence bit 7 in the received codeword is in error.

Ex. 2.6.11 : 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.

Soln. :

- For checksum in CRC refer section 2.6.6.
- The generator polynomial actually acts as the divisor in the process of CRC generation.

∴ Data word : 110101011

Divisor : $x^4 + 0x^3 + 0x^2 + x + 1$

= 10011

The number of data bits = m = 9

The number of bit in the codeword = N

Dividend = Data word + (N - 1) number of zeros.



(G-216)

Carry out the division as follows :

Mod 2 addition →

$$\begin{array}{r}
 110000111 \\
 10011 \\
 \hline
 10011 \\
 \hline
 010011 \\
 \hline
 10011 \\
 \hline
 00000001100 \\
 \hline
 10011 \\
 \hline
 11111 \\
 \hline
 10011 \\
 \hline
 011000 \\
 \hline
 10011 \\
 \hline
 010110 \\
 \hline
 10011 \\
 \hline
 00101
 \end{array}$$

(G-216(a))

Codeword : The codeword is given by :

Codeword = 

(G-216(b))

Internationally used CRC polynomials :

The three polynomials which are used internationally are :

$$\text{CRC } 12 = x^{12} + x^{11} + x^3 + x^2 + x + 1$$

$$\text{CRC } 16 = x^{16} + x^{15} + x^2 + 1$$

$$\text{CRC - CCITT} = x^{16} + x^{12} + x^5 + 1$$

2.6.10 Solved Examples :

Ex. 2.6.12: If the frame is 1101011011 and generator is $x^4 + x + 1$ what would be the transmitted frame.

Soln.:

Given : Data word : 1101011011

$$\text{Generator: } x^4 + x + 1 = x^4 + 0x^3 + 0x^2 + x + 1$$

$$= 10011 = n$$

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 : (G-216(e))

The diagram shows a horizontal sequence of 16 boxes representing bits. The first 12 boxes contain binary digits (0 or 1), while the last 4 boxes are entirely filled with zeros. An arrow labeled "Data word" points to the first 12 boxes, and another arrow labeled "4 additional zeros" points to the last 4 boxes.

Step 2 : Carryout the long division :

The diagram illustrates a binary division process. At the top left is the label "Generator" with a downward arrow pointing to the first bit of the dividend. The dividend is a 16-bit number: 1100001010 followed by 16 zeros. A 5-bit divisor, 10011, is shown with a plus sign and four addition symbols below it, indicating it is being subtracted from the dividend. The quotient is calculated bit by bit: 010011 (5 bits) and 10011 (5 bits). The remainder is 0010100 followed by 10011 (5 bits), with a final remainder of 001110 (5 bits) at the bottom right.

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 :

The diagram shows a 32-bit register divided into two fields: "Dataword" and "Remainder". The "Dataword" field occupies the lower 24 bits, and the "Remainder" field occupies the upper 8 bits.

(G-216(e))

Ex. 2.6.13 : What is the remainder obtained by dividing $x^7 + x^5 + 1$ by the generator polynomial $x^3 + 1$?

Soln. 3

Given:

$$\begin{aligned} \text{Dividend : } & x^7 + x^5 + 1 = x^7 + 0x^6 + x^5 + 0x^4 + 0x^3 \\ & \quad + 0x^2 + 0x + 1 \\ & = 10100001 \end{aligned}$$

$$\text{Divisor: } x^3 + 1 = x^3 + 0x^2 + 0x + 1$$

The long division is as follows:

$$\begin{array}{r}
 & 1 0 1 1 0 \\
 1 0 0 1 \overline{) 1 0 1 0 0 0 0 1} \\
 & \underline{1 0 0 1} \quad \downarrow \quad \downarrow \\
 & 0 0 1 1 0 0 \\
 & \underline{1 0 0 1} \quad \downarrow \\
 & 0 1 0 1 0 \\
 & \underline{1 0 0 1} \\
 & 0 0 1 1 1 \leftarrow \text{Remainder}
 \end{array}$$

The remainder is,

$00111 = x^2 + x + 1$ in the polynomial form.

Ex. 2.6.14 : 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

Generator polynomial :

$$= 1001 = a$$

Step 1 : Obtain the dividend :

Dividend = Data word + 3 zeros.

The dividend is as follows :

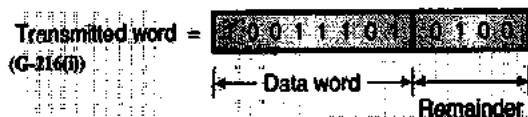


Step 2 : Carry out the division :

$\begin{array}{r} 100011100 \\ \hline 1001 \overline{) 100111101000} \\ \oplus 1001 \\ \hline 00001101 \\ \quad\quad\quad\downarrow \\ 1001 \\ \hline 01000 \\ \quad\quad\quad\downarrow \\ 1001 \\ \hline 000100 \end{array}$	(G-216(b))
--	------------

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 :

The received word = 1 0 1 1 1 0 1 0 0 0 1

At the receiver, this word is divided by the same divider used at the transmitter i.e. 1001.

A non zero remainder indicates that there is an error in the received codeword.

Ex. 2.6.15: A bit string 011110111101111110, 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. 2.6.15.

Original data	: 0 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 1 0
Outgoing data	: 0 1 1 1 1 0 1 1 1 1 0 1 1 1 1 1 0 0 1 1 1 1 0 1 0

Starting flag byte

Stuffed bits

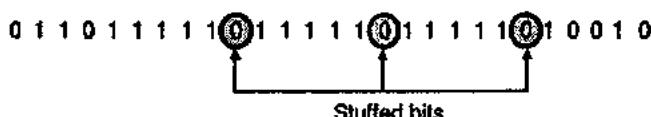
(G-217) Fig. P. 2.6.15

Ex. 2.6.16: Apply bit stuffing

011011111111111110010

Soln. :

The outgoing data after bit stuffing is shown in Fig. P. 2.6.16.



(G-218) Fig. P. 2.6.16

Ex. 2.6.17 : Generate the Hamming code for the data 111011001 with even parity.

Soln. :

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	0	1	0	1

(G-218(a))

Step 3 : Select P₂ :

To select P₂ we have to consider the bits in positions 2, 3, 6, 7, 10 and 11

$$\therefore 1 \ 0 \ 1 \ 0 \ 1 \ P_2 \rightarrow P_2 = 1 \quad \therefore P_2 = 1$$

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.

$$\therefore 1 \ 1 \ 1 \ 0 \ 0 \ P_4 \quad \therefore P_4 = 1$$

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.

$$1 \ 1 \ 1 \ 0 \ 1 \ P_8 \quad \therefore P_8 = 0$$

So the codeword is as follows :

Codeword									P ₈	P ₄	P ₂	P ₁	
1	1	1	0	1	0	1	0	0	1	1	1	1	0

(G-218(c))

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

(G-218(b))

For even parity P₁ should be 1. $\therefore P_1 = 1$

2.6.11 ARQ Technique :

- 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, a request is made for the retransmission of that signal. Therefore a feedback channel is required for sending the request for retransmission.
- The ARQ systems differ from the FEC systems in three important respects. They are as follows :
 1. 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.
 2. A return transmission path and additional hardware in order to implement repeat transmission of codewords will be needed.
 3. 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. 2.6.19.

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 look for errors.

- The decoder will output a "positive acknowledgment" (ACK) if no errors are detected and it will output a negative acknowledgment (NAK) if errors are detected.
- 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 :

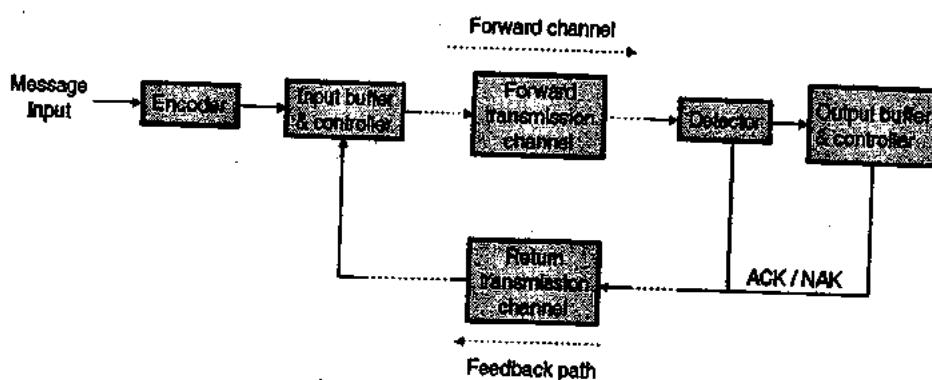
The bit rate of the return transmission which involves the return transmission of ACK/NAK signal is low as compared to the bit rate of the forward transmission. Therefore the error probability of the return transmission is negligibly small.

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.



(a-372) Fig. 2.6.19 : Block diagram of the basic ARQ system

2.7 Flow Control :

- This is another important design issue related to the data link layer.
- 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.
- The flow control will 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.

Note : 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.

2.8 Elementary Data Link Protocols :

- In this section we are going to discuss some elementary data link layer protocols.

2.8.1 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.

2.8.2 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.
- 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.
- The best thing about this protocol is that the incoming frame is always an acknowledgement. It need not be even checked.

2.8.3 A Simplex Protocol for Noisy Channel :

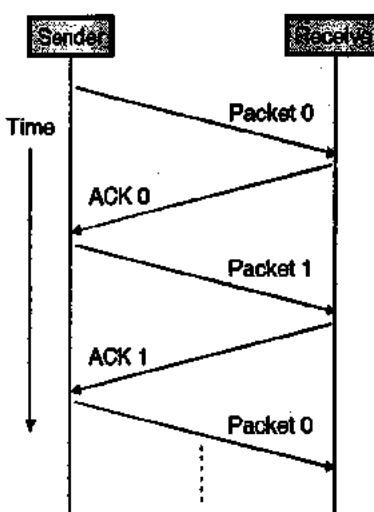
- This is the third protocol in which we go one step ahead and assume that the communication channel is noisy and can introduce errors in the data travelling over it.
- The channel noise can either damage the frames or they may get lost completely.
- In this protocol, the sender waits for a positive 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.
- The operation can be divided into two modes :
 - Normal operation and
 - Time out.

1. Normal operation :

- After transmitting one frame, the sender waits for an *acknowledgement (ACK)* from the receiver before transmitting the next one.
- 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.

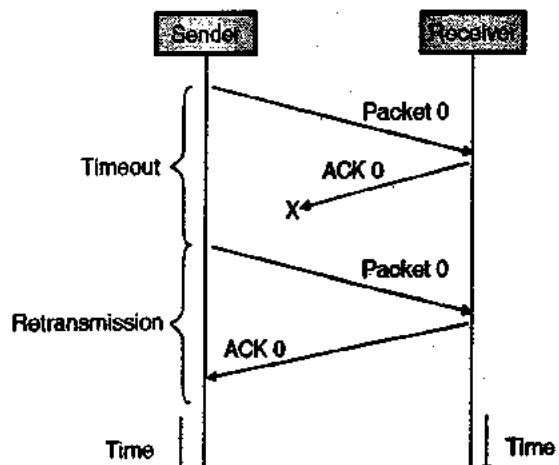


(G-22) Fig. 2.8.1 : Positive acknowledgement with retransmission

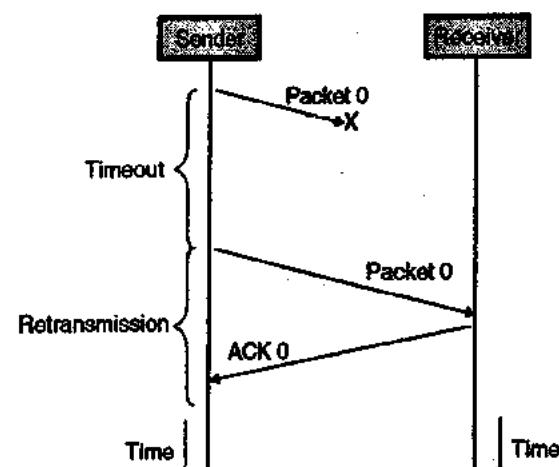
2. Time out :

- If the sender does not receive ACK for previous 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. 2.8.2.
- To support this feature, the sender keeps timer for each frame.
- We have already discussed that a timer is introduced in the data link layer.



(a) Sender does not receive acknowledgement



(G-22) Fig. 2.8.2 : Timeout and retransmission

2.8.4 Piggybacking :

- 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 bothways, with both channels having the same capacity.

- 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, the receiver waits, does not send the control frame (acknowledgement) back immediately.
- The receiver waits until its network layer passes in the next data packet.
- The acknowledgement is then attached to this outgoing data frame. Thus the acknowledgement travels alongwith next data frame.
- This technique in which the outgoing acknowledgement is delayed temporarily is called as piggybacking.

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 :

- The disadvantage of piggybacking is the additional complexity.
- If the data link layer waits too long before transmitting acknowledgement, then retransmission of frame would take place.

2.9 Sliding Window Protocols :

- 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.

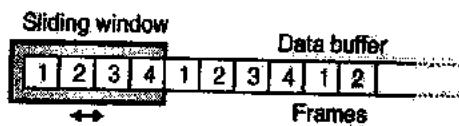
Sequence number :

- 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 upto 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. 2.9.1(a).



(G-222)Fig. 2.9.1(a) : Sliding window

- In Fig. 2.9.1(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. 2.9.1(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 .

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. 2.9.1(b) and sends 5th and 6th frames (i.e. frames 1 and 2 of the next lot).

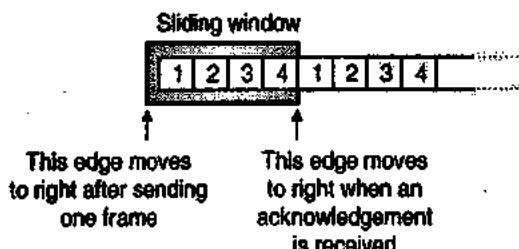


(G-223)Fig. 2.9.1(b) : Illustration of sliding window mechanism

- 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.

Movement of sender's window :

- Fig. 2.9.1(c) shows the sender's window.



(G-224)Fig. 2.9.1(c) : Sender sliding window

- If the sender's window size is 4 and frames 1 and 2 are sent but acknowledgement has not been received so far, then as shown in Fig. 2.9.1(d), the sender's windows will only contain two frames i.e. 3 and 4.



(G-225)Fig. 2.9.1(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 sender's window now expands and includes the next two frames as shown in Fig. 2.9.1(e).

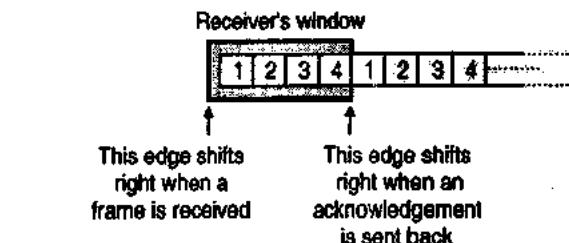


(G-226)Fig. 2.9.1(e) : Sender's window after receiving acknowledgement bearing number-3

- In this way the left edge of sender's window will shift right when the data frames are sent and the right edge of the sender's window will shift right when the acknowledgement is received.

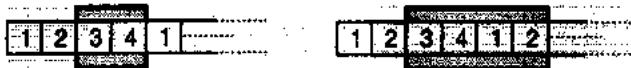
Movement of receiver's windows :

- Fig. 2.9.1(f) shows the receiver's window. Its left edge shifts right on receiving each data frame, whereas its right edge shifts right when an acknowledgement is sent.



(G-227)Fig. 2.9.1(f) : Receiver's sliding window

- If we take the same example that we discussed for the sender's window then the position of receiver's windows are as shown in Fig. 2.9.1(g) and (h).



(g) Two frames (1 and 2) received but no acknowledgement sent

(h) After sending the acknowledgement

(G-228)Fig. 2.9.1 : Movement of receiver window

Ex. 2.9.1 : 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 sends any frame
- After A sends frame 0, 1, 2 and receives ACK (acknowledgement) from B for 0 and 1.

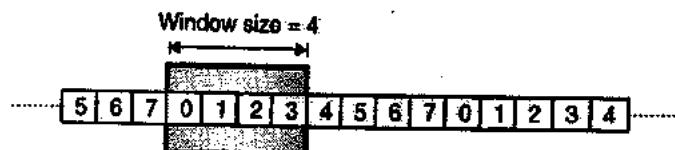
Soln. :

- 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,

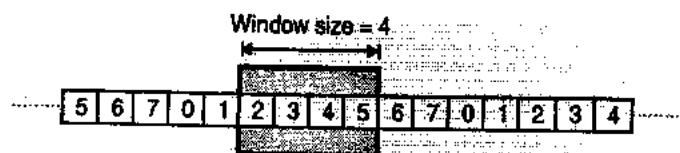
- The size of the window is 4.

Fig. P. 2.9.1(a) shows the sender window (at A) before sending any frame.

Fig. P. 2.9.1(b) shows that the window slides 2 positions because acknowledgement for frames 0 and 1 have been received.



(G-229) Fig. P. 2.9.1(a) : Before A sends any frame



(G-230) Fig. P. 2.9.1(b) : After sliding two frames

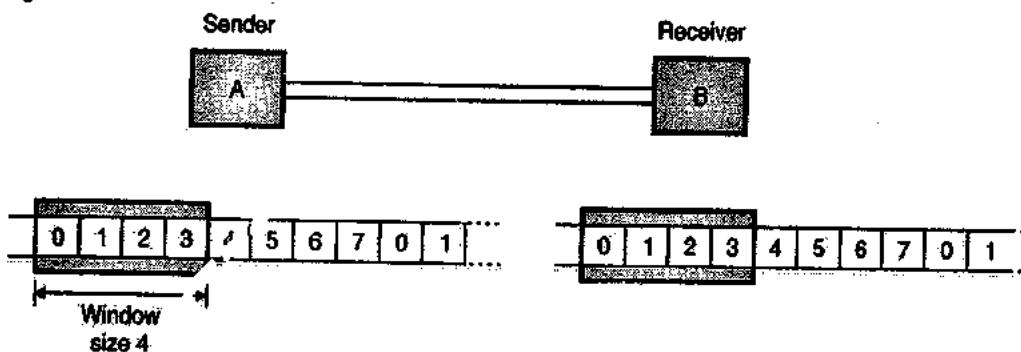
Ex. 2.9.2: Two neighbouring nodes A and B use Go-Back N ARQ with a 3 bit sequence number. Assuming that A is transmitting and B is receiving. Show the window position and frame flow for the following sequence of events.

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 receiver REJ 3 from B.

Soln. :

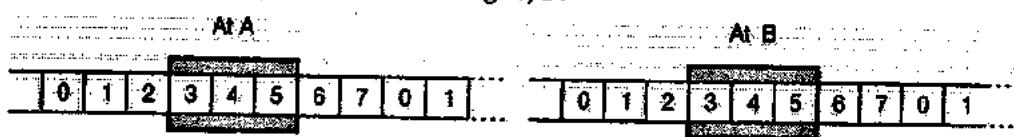
- The number of sequence bits = $m = 3$.
- \therefore The sequence numbers will be 0, 1, 2, 3 ... , 6, 7. Then these numbers will get repeated. So the sequence will be 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, ...
- The size of the window is 4.
- The positions and frame flow at A and B for different situations are as shown in Fig. P. 2.9.2.

Case 1 : Initial position :



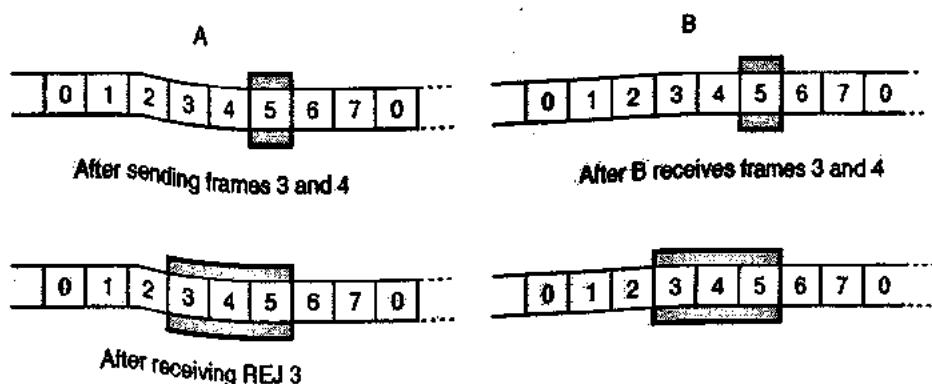
(G-231) Fig. P. 2.9.2(a)

Case 2 : After A sends frames 0, 1, 2 and B acknowledge 0, 1 :



(G-232) Fig. P. 2.9.2(b)

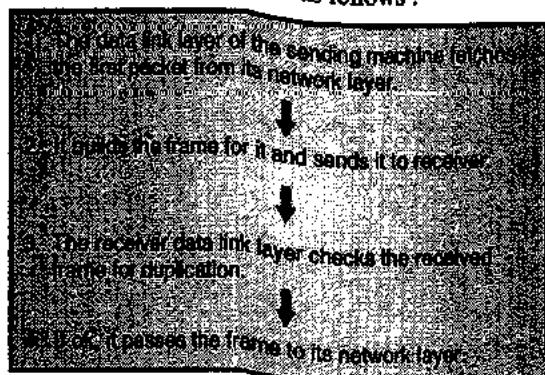
Case 3 : A sends frames 3 and 4 and then receives REJ 3 from B :



(G-233) Fig. P. 2.9.2(c)

2.9.1 A One Bit Sliding Window Protocol (Stop and Wait ARQ) :

- 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 :



(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.

- The transmitter stores the copy of last frame transmitted until an acknowledgement for that frame is received from the destination.
- 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 ACK 1 frame. After receiving ACK1 the sender sends next data frame having a number 1.
- 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.
- 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.

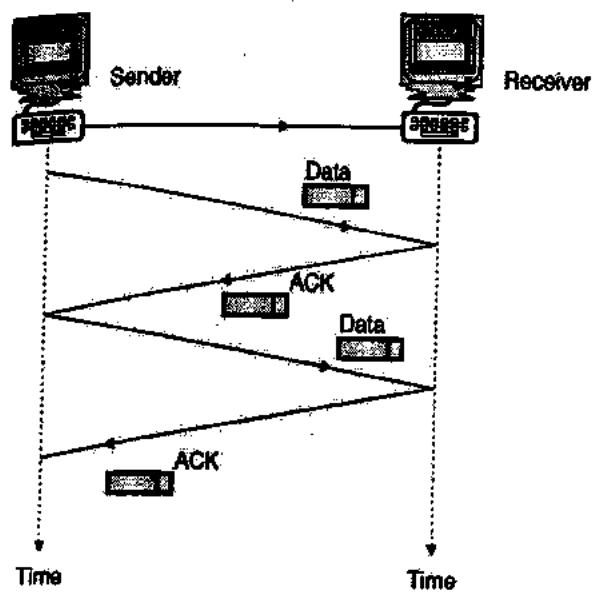
When is the retransmission necessary ?

- The retransmission of frame is essential under the following events :
 - If the received frame is damaged.
 - If the transmitted frame is lost.
 - 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. 2.9.2 illustrates the protocol operation when everything is normal.

No frame is lost so retransmission is not necessary.



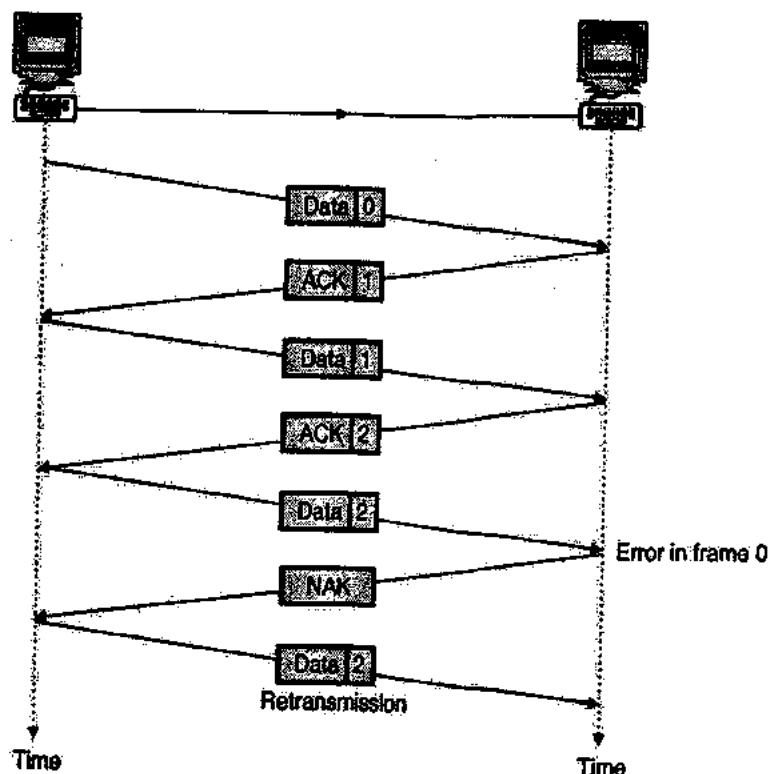
(G-235) Fig. 2.9.2 : Stop and wait under normal condition

Stop and wait ARQ for damaged frame :

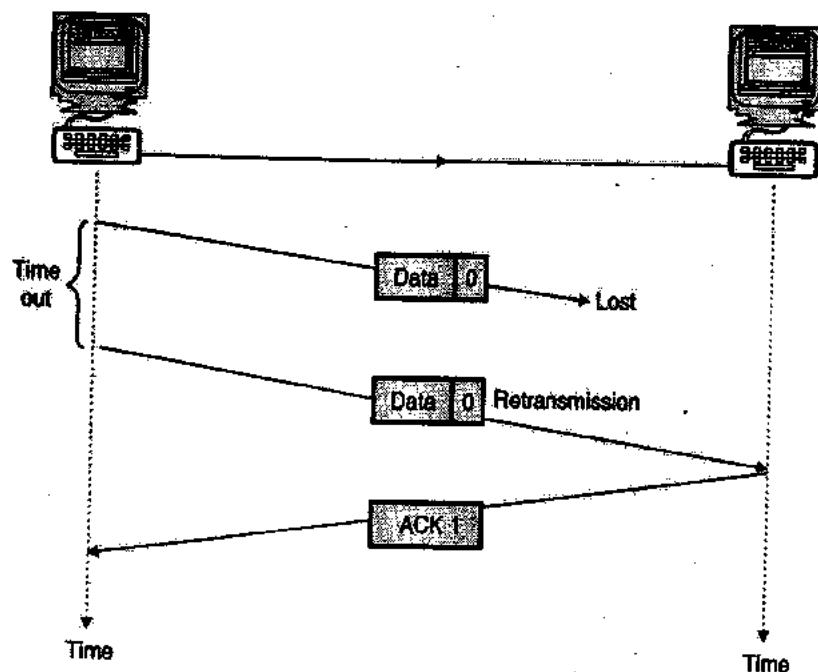
- As seen in Fig. 2.9.3(a) the transmitter transmits data frame numbered 0. The receiver returns an ACK 1 indicating that the data frame numbered 0 is received without any error.
- The next data frame i.e. data 1 is sent. The corresponding acknowledgement ACK2 is received.
- The process goes on in this 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.

Stop and wait ARQ for lost data frame :

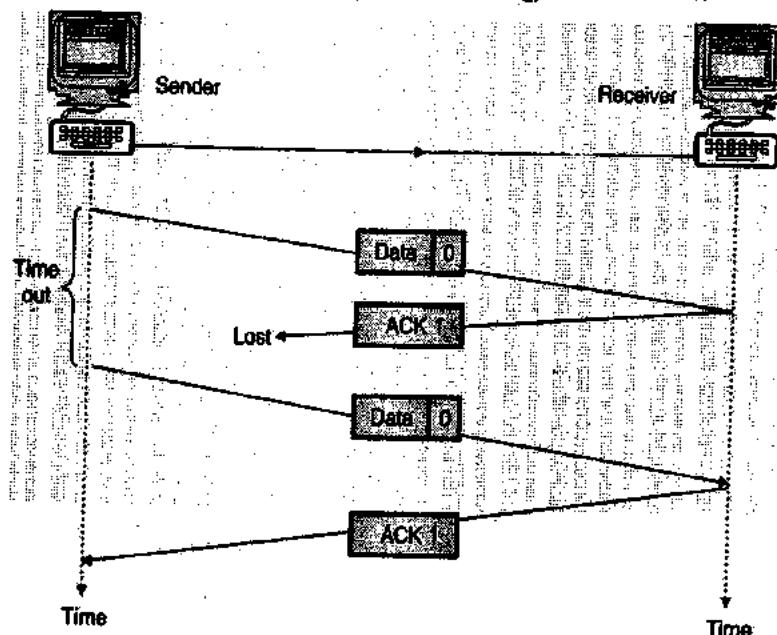
- Fig. 2.9.3(b) shows that if a data frame is lost and if the transmitter does not receive any type of acknowledgement from the receiver with a specified time it retransmits the same frame again.



(G-236) Fig. 2.9.3(a) : Stop and wait ARQ damaged frame



(G-237)Fig. 2.9.3(b) : Stop and wait ARQ, lost data frame



(G-238)Fig. 2.9.3(c) : Stop and wait ARQ, lost ACK frame

Stop and wait ARQ for lost acknowledgement :

- Fig. 2.9.3(c) shows that if the acknowledgement sent by the receiver is lost, the transmitter retransmits the same data frame after its timer goes off.
- 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.

Stop-and-Wait ARQ was used in IBM's Binary Synchronous Communications (Bisync) Protocol. It is also used in X-modem, a popular file transfer protocol for modem.

Disadvantages of stop and wait protocol :

1. Problem with Stop-and-Wait protocol is that it is very inefficient. At any one moment, only one frame is in transition.
2. 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.

2.9.2 A Protocol using GO Back n :

- 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.

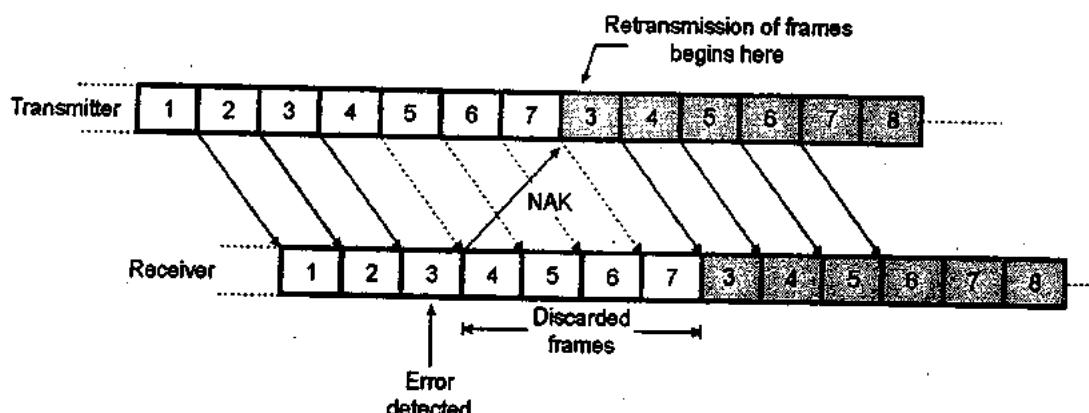
- In this method if one frame is damaged or lost, all frames are sent since the last frame acknowledged are retransmitted.

Principle of GO-back-n ARQ :

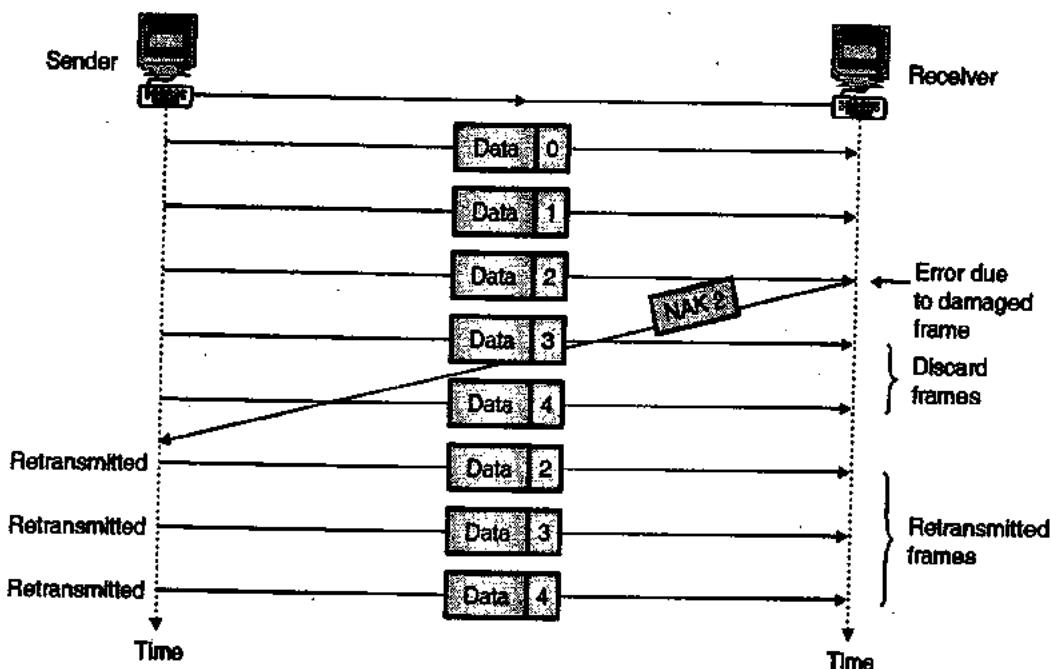
- Refer Fig. 2.9.4 to understand the principle of GO-Back-n ARQ.
- The major difference between this and the previous system is that the sender does not wait for ACK signal for the transmission of next frame.
- It transmits the frames continuously as long as it does not receive the "NAK" signal. NAK 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. 2.9.4, 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 :

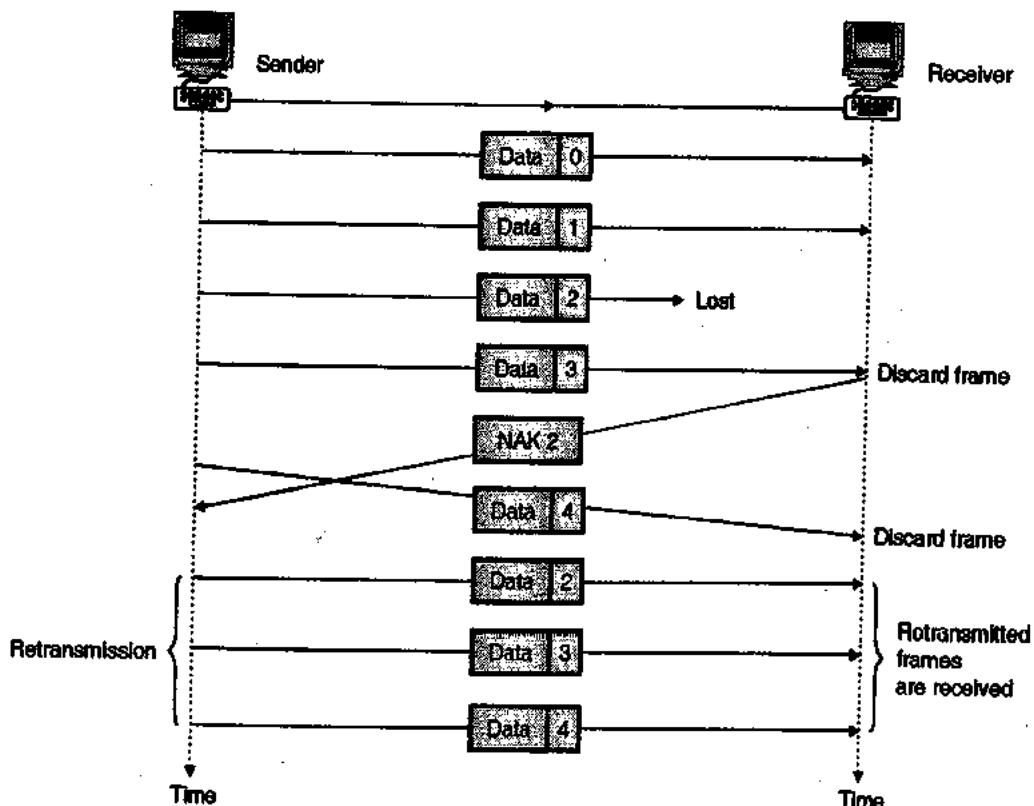
- The errors can get introduced, if the transmitted frames are damaged or lost or if the acknowledgement is lost.
- Let us consider the operation of this protocol under these conditions.



(G-239)Fig. 2.9.4 : Go back n ARQ system



(G-24)Fig. 2.9.5(a) : Go-back-n, damaged data frame



(G-24)Fig. 2.9.5(b) : Go-back-n, lost data frame

Operation when the frame is lost :

- This condition is illustrated in Fig. 2.9.5(a).
- 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. 2.9.5(b) the case of lost frame is also treated in the same manner as that of the damaged 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. 2.9.5(c) shows the condition for lost acknowledgement. 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.

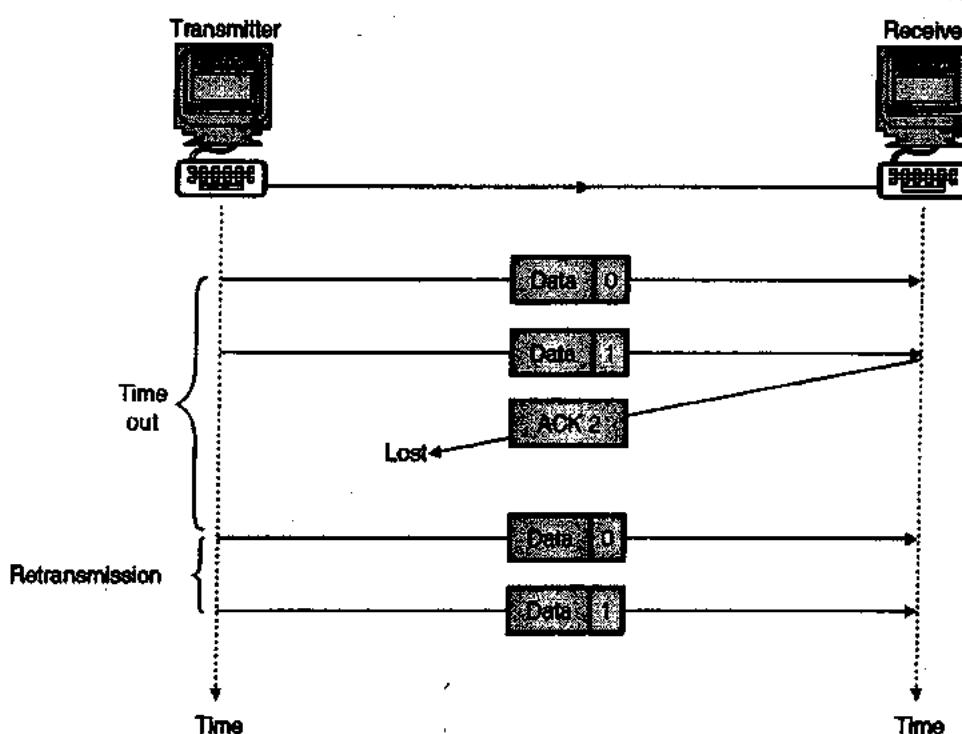
- The disadvantage of Go-back-n ARQ protocol is that in noisy channels it has poor efficiency because of the need to retransmit the frame in error and all the subsequent frames.

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.

2.9.3 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.



(G-242)Fig. 2.9.5(c) : Go-back-n, lost ACK frame



2.9.4 Selective Repeat ARQ :

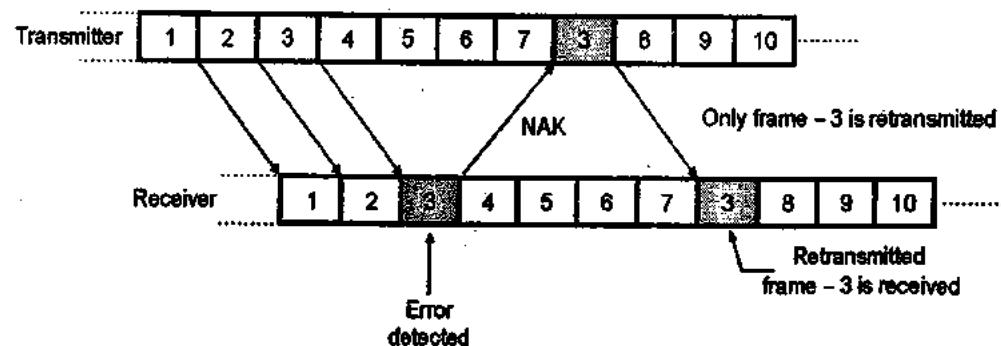
In this method only the specified damaged or lost frame is retransmitted. A selective repeat systems differs from the go-back-n method in the following ways :

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. 2.9.6.
- 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. 2.9.6.
- By the time this "NAK" signal reaches the transmitter, it had transmitted the frames upto 7 as shown in Fig. 2.9.6.
- 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. 2.9.6.

- 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.



(G-24)Fig. 2.9.6 : Selective repeat ARQ system

2.9.5 Protocol Performance :

- 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 :

$$\eta = \frac{t_f}{t_f + 2t_p} \quad \dots(2.9.1)$$

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. 2.9.3 : 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. :

$$\begin{aligned} t_f &= \frac{\text{Frame size}}{\text{Bit rate}} \\ &= \frac{4800}{9600} = 0.5 \text{ sec} \end{aligned}$$

$$t_p = \frac{2000}{200000} = 0.01 \text{ sec}$$

$$\text{We know, } A = t_p/t_f$$

$$\therefore A = 0.01 / 0.5 = 0.02$$

$$\begin{aligned} \text{Since, } \eta &= 1/(1+2A) \\ &= 1/(1+2 \times 0.02) = 0.96 \end{aligned}$$

$$\therefore \% \eta = 96 \% \quad \dots\text{Ans.}$$

Ex. 2.9.4 : 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 $\eta \geq 50 \% \quad \text{i.e. } 0.5 \leq \eta \leq 1$

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 $t_f = \text{Transmission time for 1 frame}$

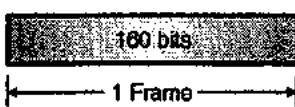
Step 2 : Calculate the frame size :

$$R = \text{Data rate} = 4 \text{ kbps} = 4000 \text{ bps}$$

$$\therefore N = R \times t_f$$

where $N = \text{Frame size}$

$$\therefore N = 40 \times 10^{-3} \times 4 \times 10^3 = 160 \text{ bits} \quad \dots\text{Ans.}$$



(G-244)Fig. P. 2.9.4 : 1 frame size



- Ex. 2.9.5 :** A channel has a bit rate of 4.8 kbit/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 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 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 : Bit rate (B) = 4.8 k bits sec.,
Propagation delay (T) = 20 msec.
Efficiency = 50%, frame size (L) = ?

$$\text{Efficiency} = \frac{L}{(L + BT)}$$

$$0.5 = \frac{L}{(L + 4.8 \times 10^3 \times 20 \times 10^{-3})}$$

$$= \frac{L}{(L + 96)}$$

$$0.5(L + 96) = L$$

$$0.5L + 48 = L$$

$$\therefore L = \frac{48}{0.5}$$

$$= 96 \text{ bits.}$$

...Ans.

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 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.

2.10 Other Data Link Protocols :

A data link protocol is a set of rules or specifications used to implement the data link layer. Data link protocols are divided into two subgroups:

- Asynchronous protocols - treat each character in a bit stream independently.
- Synchronous protocols - take the whole bit stream and divides it into characters of equal size.

2.11 High Level Data Link Control (HDLC) Protocol :

- 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:

- Primary station
- Secondary station
- 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:
 - Normal Response Mode (NRM)
 - Asynchronous Response Mode (ARM)
 - 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.

2.11.1 Frame Structure in HDLC :

- 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. 2.11.1(a) and Fig. 2.11.1(b). 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.

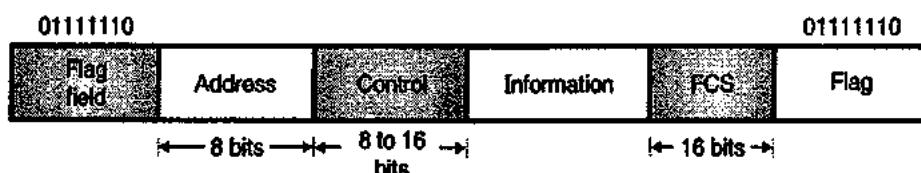
Flag field : The flag is a unique 8-bit word pattern (01111110). It is used to identify the start and end of each frame as shown in Fig. 2.11.1(a). It is also used to fill the idle time between consecutive frames.

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.



(a) Information transfer frame



(b) Supervisory and unnumbered frames

(G-250) Fig. 2.11.1



2.11.2 Frame Types in HDLC :

- There are three types of frames defined in HDLC as follows :
 - The I-frame or information frame.
 - The S-frame or supervisory frame.
 - The U-frame or the unnumbered frame.

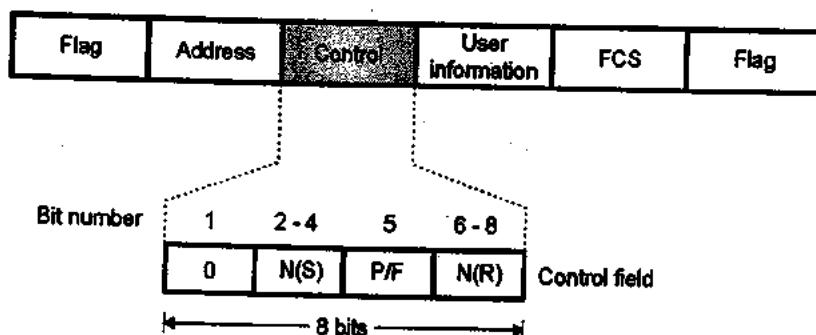
The I-frame :

- Fig. 2.11.2 shows the format of the information frame or I-frame.
- 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.

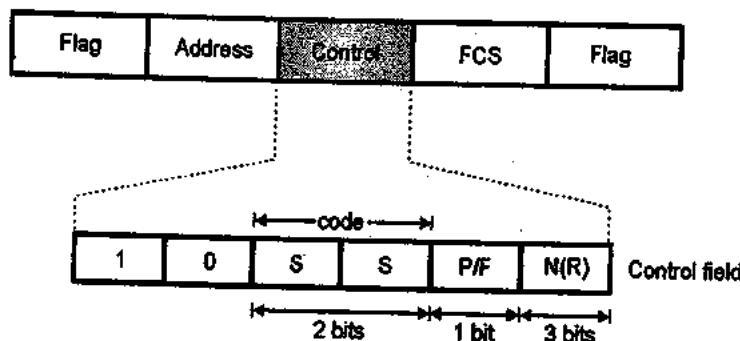
Explanation :

- Concentrate on the control field of the I-frame.
- As shown in the Fig. 2.11.2 if the first bit in the control field is 0 it is identified as an information frame (I-frame).

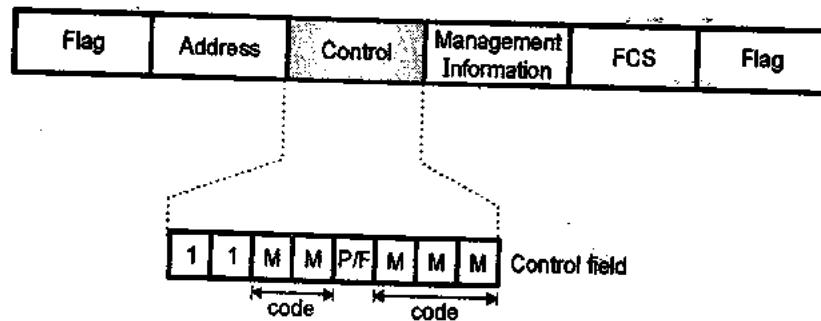
- The next three bits (2 to 4) are called N(S) and their job is to define the sequence number of the frame.
- Since there are only 3 bits, we can define only eight combinations ($2^3 = 8$). Therefore a sequence number is between 0 and 7 only.
- The value of N(S) field corresponds to the value of control 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 = 0, 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.



(G-25)Fig. 2.11.2 : I-frame format



(G-25)Fig. 2.11.3 : S-frame format



(G-253)Fig. 2.11.4 : Format of U-frame

The S-Frames :

- Fig. 2.11.3 shows the format of S-frames or supervisory frames.
- 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. 2.11.3.
- 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.
 - SS = 00 → corresponds to receive ready (RR) frames which are used to acknowledge frames when no I frames are available to piggyback the acknowledgement.
 - SS = 01 → corresponds to Reject (REJ) frames which are used by the receiver to send a NAK when error has occurred.
 - SS = 10 → corresponds to a Receive Not Ready (RNR) frame and it is used for flow control.
 - 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. 2.11.4.
- 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. 2.11.4.
- 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. 2.11.4) are divided into two sections. Two bits before P/F 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.

2.11.3 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 0111110 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.

2.11.4 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.



2.12 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.

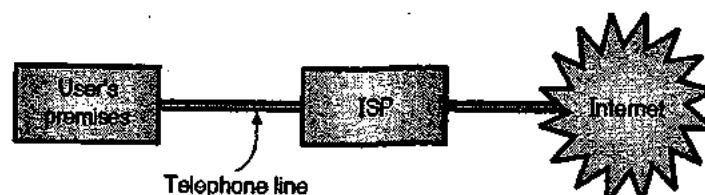
2.13 Ways of Accessing the Internet :

- Now we can access the Internet in a number of different ways. Earlier the only way to access the Internet was to obtain a telephone connection and then open an account with an ISP (Internet Service Provider). This type of Internet access is known as the basic access method and it is as shown in Fig. 2.13.1. So in this system the ISP will allow the user to access the Internet.
- In modern era, the basic framework of Internet access has not changed considerably. But the ways of getting connected to the ISP from user's premises have changed to a great extent.
- The different possible ways are as follows :
 1. Dial up access
 2. ADCL
 3. ISDN
 4. Cable modems
 5. Leased lines

- One important thing to be noted is that all such methods still use the services of an ISP. They only provide different ways for the user to get connected to the ISP and Internet.

Dial up access for an individual user :

- A user can access the Internet backbone and the computers connected in a number of different ways. The simplest way is to use Internet protocol called TELNET. This protocol is an integral part of the TCP/IP suite. Here the ISP is not required but the user should have the knowledge of using the TELNET program.
- But home users generally do not know how to use TELNET. So they prefer a direct connection to the Internet, that means they want to connect to Internet through an ISP. This is a simpler way of getting connected.
- For this type of connection, the serial communication is used. The communication between client (home user) and ISP takes place using two data link layer protocols :
 1. Point to Point Protocol (PPP) and
 2. Serial Line Internet Protocol (SLIP)
- Using these two protocols the home user can dial into an ISP over the pre-existing telephone line.
- If one uses PPP and SLIP then connection is called as dial up connection because the client first dials up into server computer of ISP and makes the Internet access.
- Due to the use of PPP and SLIP protocols the communication between the client and the Internet takes place in such a way as if there is a direct connection between the home user and Internet.



(G-1435) Fig. 2.13.1 : Basic Internet access method

2.14 SLIP-Serial Line IP :

- The home users of Internet generally prefer a direct connection to Internet.
- For such type of connection, the serial communication is used. The communication between client and ISP takes place using two data link layer protocols :
 - Serial Line Internet Protocol (SLIP)
 - Point to Point Protocol (PPP)

SLIP :

- This protocol was devised in 1984, to connect a workstation to the internet over a dial-up line using a modem. It is a connection oriented protocol.
- This protocol is very simple. The workstation sends raw IP packets over the line with a flag byte at the end for framing purpose.
- If the flag format appears in the data, then a two byte sequence (0XDB, 0XDC) is sent in its place.
- If 0XDB occurs in the flag byte, then it is also stuffed.
- In some SLIP implementations, a flag byte is attached at the front and back of each IP packet sent.

Problems with SLIP protocol :

- SLIP is a simple and widely used protocol. But it has some serious problems. They are as follows :
 - It does not have any error detection or correction facility.
 - SLIP supports only IP. So it cannot be used over the networks which do not use IP.
 - It is necessary that both the communicating sides must know the other's IP address in advance. It is not possible to dynamically assign the address during the set up.
 - SLIP does not provide any authentication. So neither party knows whom it is talking to.

- It is not an approved Internet standard. So many versions exist which makes networking difficult.

2.15 Point-to-Point Protocol (PPP) :

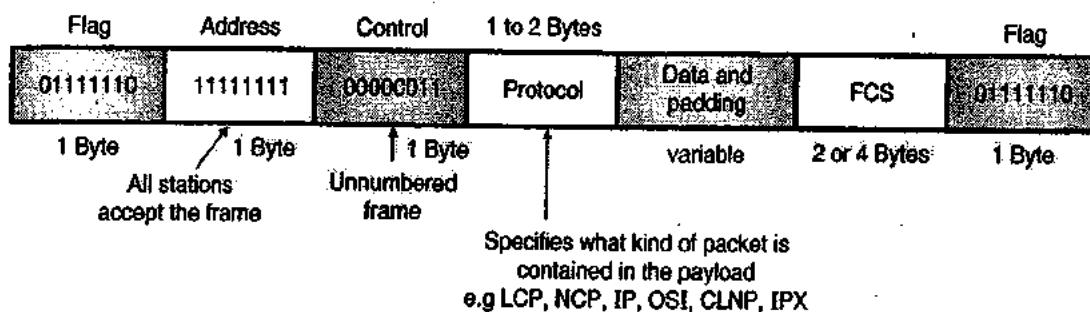
- One of the most common protocols used for point to point access is PPP. The long form of PPP is point to point protocol.
- This protocol is used by a lot of Internet users to connect their home computers to the server of an Internet Service Provider (ISP).
- Most of these users have a traditional modem and they are connected to the Internet through a telephone line or a TV cable.
- The PPP is used for controlling and managing the data transfer.

2.15.1 Services Provided by PPP :

- Following are some of the services provided by PPP :
 - To define the frame format.
 - It defines how the link between two devices is to be established and how the data exchange should take place.
 - It decides the encapsulation of network layer data into the data link frame.
 - It defines the way in which the two devices can authenticate each other.
- This protocol was designed for users who wanted to connect their computer system through a telephone line to the computer of an Internet service provider to access internet.
- The PPP protocol can operate over a variety of point to point transmission links such as ADSL and SONET.
- The PPP was an improvement over the Serial Line Internet Protocol (SLIP).

2.15.2 Frame Format of PPP :

- The PPP protocol uses an HDLC like frame format as shown in Fig. 2.15.1.



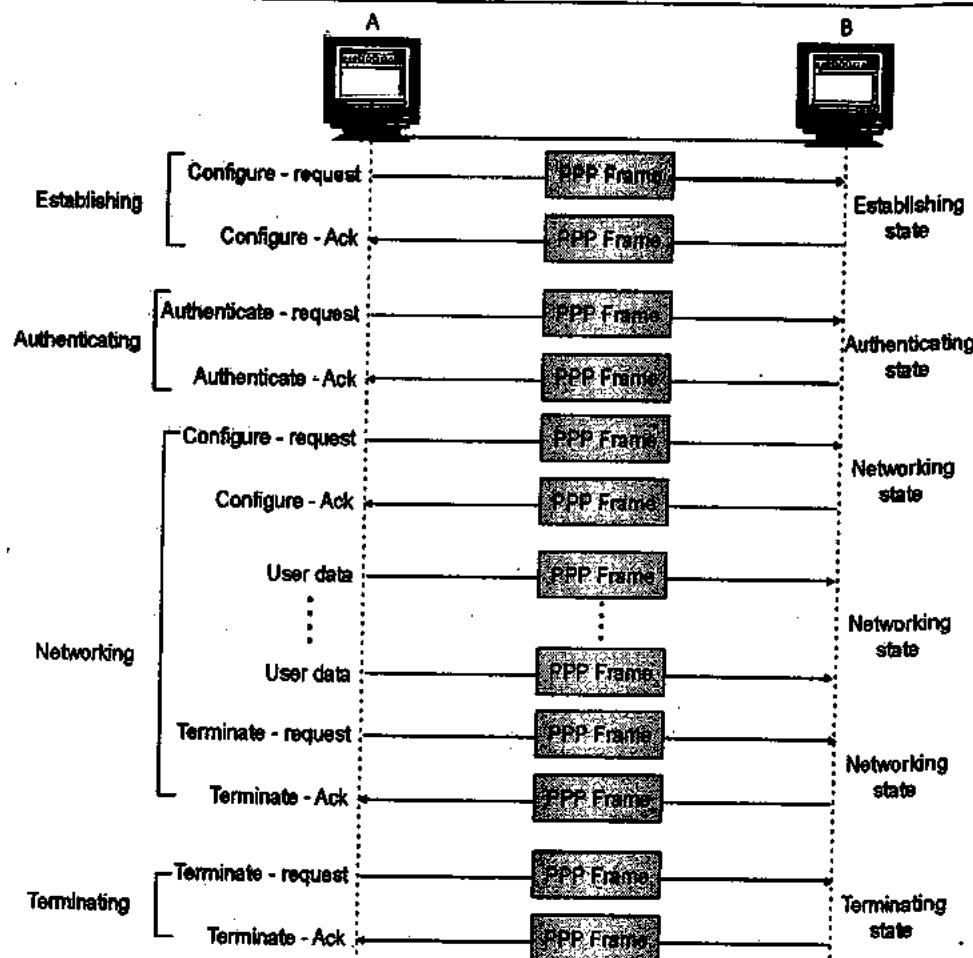
(G-256)Fig. 2.15.1 : Frame format of PPP



The descriptions of various fields is as follows :

1. **Flag** : The PPP frame always begins and ends with the standard HDLC flag i.e. 01111110.
2. **Address** : Since PPP is used for a point-to-point connection, it uses the broadcast address of HDLC i.e. 11111111, to avoid a data link address in the protocol. All 1's in the address field indicates that all stations are to accept the frame.
3. **Control** : This field has the same format as that of the U-frame in HDLC. The value is 00000011 in this field indicates that the frame does not contain any sequence numbers and that there is no flow or error control.
4. **Protocol** : It defines the nature of contents of the data field, i.e. user data or other information.
5. **Data field** : It carries either the user data or other information.
6. **FCS (Frame Check Field)** :
 - This field is a 2 or 4 byte CRC. It can use the CCITT 16 or CCITT 32 generator polynomial.

- The PPP protocol provides many useful capabilities if used alongwith two protocols namely a Link Control Protocol (LCP) and the Network Control Protocol (NCP).
- The Link Control Protocol (LCP) is used to carry out various tasks such as to set-up, configure, test, maintain and terminate a link connection.
- After authentication has been completed a Network Control Protocol (NCP) is used.
- The NCP consists of multiple control protocols. It help in the encapsulation of data coming from network layer protocols such as IP, IPX, Decent, Apple Talk in the PPP frame.
- The PPP connection will have to go through different states, such as establishing, authenticating, networking and terminating state as shown in Fig. 2.15.2(a).



(G-257) Fig. 2.15.2(a) : States of PPP connection

2.15.3 Transition Phases :

- The PPP connection goes through different phases. These states and their interrelation is shown in the transition state diagram of Fig. 2.15.2(b).

Figs. 2.15.2(a) and (b) shows the following states of a PPP connection :

- Idle** : It means that the link or the transmission medium is not being used. It also means that any active carrier is absent on the line.
- Establishing** : When one of the end users starts the communication, the connection goes into the establishing state. In this state the user sends the configure request packet so as to negotiate the options for establishing the link. If negotiation is successful the system goes to the next state which is authenticating. The LCP packets are used for this purpose.
- Authenticating** : The user sends the authenticate request packet and includes the user name and password in it. After it receives the configure-Ack packet the authentication process is over. When authentication is successful, the system goes to the next state i.e. the networking state.
- Networking** : When a connection reaches this state of user control and data packets exchanging can start

taking place. The connection remains in this state until one of the end users want to stop communicating.

- Terminating** : The user sends the terminate packet to terminate the link. With the reception of the terminate Ack packet, the link is terminated.

2.15.4 Multiplexing :

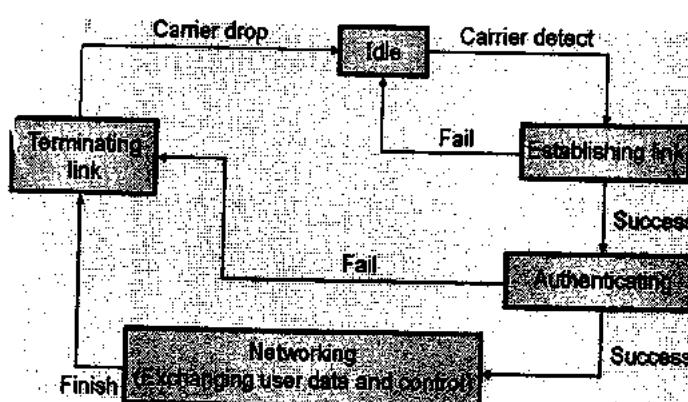
- PPP is a data link layer protocol. However it uses a set of other protocols in order to carry out the following operations :

- Link-establishment
- Authenticating the involved parties
- Carry the network layer data.

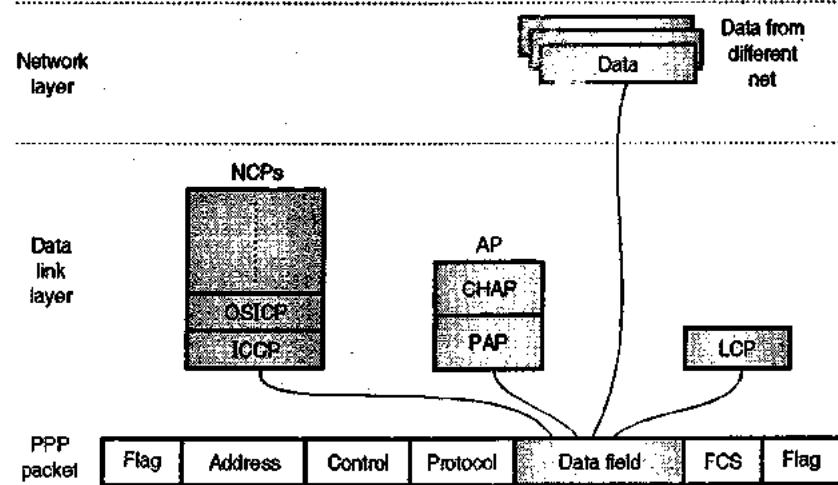
Following three sets of protocols are defined to make the PPP more powerful in its operation :

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

As shown in Fig. 2.15.3, at any instant of time the data field of a PPP packet can carry data from one of these three protocols. This is called as multiplexing in PPP.



(G-258)Fig. 2.15.2(b) : Flow diagram for PPP connection



(G-259)Fig. 2.15.3 : Multiplexing in PPP

2.15.5 PPP Stack :

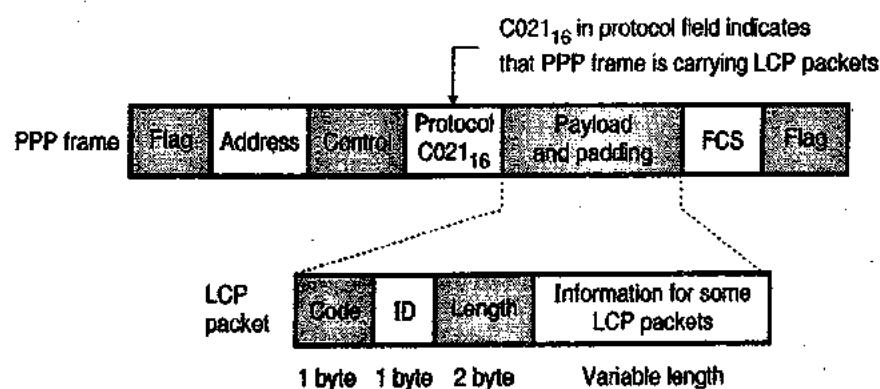
- PPP is a data link protocol. But it uses stack of other protocols in order to perform function such as to establish the link, to authenticate the users and to carry the network layer data.
- PPP uses three sets of protocols namely :
 1. Link Control Protocol (LCP)
 2. Authentication protocols
 3. Network Control Protocols (NCP).
- Fig. 2.15.4 shows the protocol stack for PPP. It shows that at any instant of time, the data field in a PPP packet can carry the packets related to one of the protocols mentioned above.

2.15.6 Link Control Protocol (LCP) :

- Link Control Protocol (LCP) is one of three important protocols shown in the protocol stack.
- The responsibilities of LCP are as follows :
 1. To establish links
 2. To maintain the established links.
 3. To configure the links and
 4. Termination of the links.
- It also provides negotiation mechanisms. Note that both the users should agree on the various options before establishing a link via a negotiation mechanism (option) available on LCP.
- Hence the PPP is carrying the LCP packet indicates that, it is in the link establishing state or in the link terminating state and therefore PPP cannot carry user data during these states.



(G-260)Fig. 2.15.4 : Protocol stack



(G-261)Fig. 2.15.5 : LCP packet

LCP packet :

- The data field of PPP frame is used for carrying all the LCP packets.
- The value $C021_{16}$ in the protocol field indicates that the data field is carrying the LCP packets.
- The format of an LCP packet is shown in Fig. 2.15.5.
- Various fields in LCP packet are as follows :
 - Code :** It is a one byte length field which defines the type of LCP packet.
 - ID :** It is a one byte length field which holds a value used for matching a request with the reply.
 - Length :** It is a two byte long field which is used for defining the length of entire LCP packet.
 - Information :** It contains extra information needed by some LCP packets.

Types of LCP packets :

- The LCP packets are broadly classified into three types as follows :
 - Configuration packets
 - Link termination packets
 - Link monitoring and debugging packets.

2.15.7 Authentication Protocols :

- Meaning of authentication is to validate the identity of a user who wants an access to the resources.

- There are two protocols created by PPP for authentication purpose namely :

1. Password Authentication Protocol (PAP)
2. Challenge Handshake Authentication Protocol (CHAP).

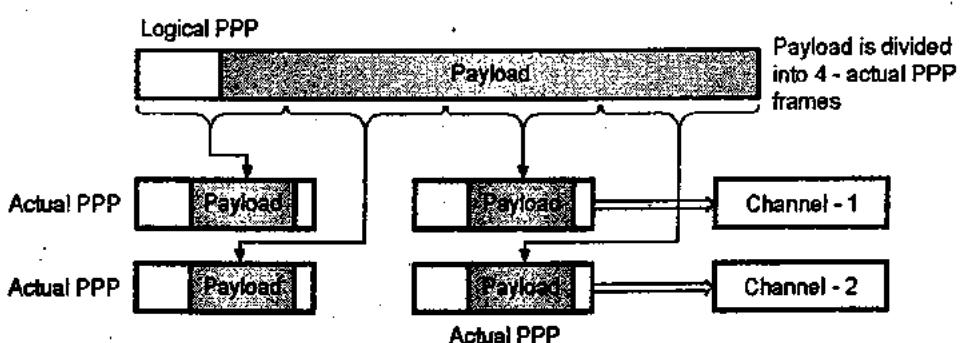
- These protocols are used during authenticating state and during this state no user data are exchanged.

2.15.8 Network Control Protocol (NCP) :

- The next step after link establishment and authentication is getting connected to the network layer.
- For this state PPP makes use of one of the three protocols in its stack called Network Control Protocol (NCP).
- NCP is a set of control protocols which helps to encapsulate the data coming from network layer protocols into the PPP frame.

2.15.9 Multilink PPP :

- The original design of PPP was done to operate for a single channel point to point physical link.
- But as multiple channels are available in a single point to point link, the Multilink PPP was developed.
- In Multilink PPP a logical PPP frame is divided into many actual PPP frames. A segment of the logical frame is carried in the payload of the actual PPP frame, as shown in Fig. 2.15.6.



(G-262) Fig. 2.15.6



2.15.10 Difference between SLIP and PPP :

No.	SLIP	PPP
1.	Error detection and correction is not possible.	Error detection and correction is possible
2.	SLIP supports only IP	IP and other protocols are supported
3.	Does not provide any authentication	Provides authentication and security
4.	SLIP is not an approved Internet standard	PPP is an approved Internet standard
5.	IP address is assigned statically to the user.	Assignment of IP address is done dynamically.

2.16 Solved Examples :

Ex. 2.16.1 : 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 = Propagation delay

= 270 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 = 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. 2.16.2 : A 100 km long cable runs at T₁ 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. = $1.544 \times 10^6 \text{ bits}$

Distance covered in 1 sec = $2 \times 10^8 \text{ m}$

∴ Number of bits corresponding to 10^5 m cable is given by,

$$X = \frac{1.544 \times 10^6}{2 \times 10^8} \times 10^5 \\ = 772 \text{ bits} \quad \dots \text{Ans.}$$

$$\rightarrow v = 2 \times 10^8 \text{ m/S}, R = 1.544 \text{ Mb/S}$$

$$100 \text{ km} = 10^5 \text{ m}$$

(G-262(a)) Fig. P. 2.16.2

Ex. 2.16.3 : 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 :

$$t_f = \frac{\text{Frame size}}{\text{Bit rate}} = \frac{1000}{1 \times 10^6} \\ = 1 \times 10^{-3} \text{ s i.e. } 1 \text{ mS.}$$

t_p = 270 mS propagation delay for a satellite channel

$$\therefore A = \frac{t_p}{t_f} = \frac{270}{1} = 270$$

$$\therefore \eta = \frac{1}{1 + 2A} = \frac{1}{1 + 2(270)} = 1.848 \times 10^{-3} \\ = 0.1848\% \quad \dots \text{Ans.}$$

2. For continuous ARQ with $W = 7$:

$$\eta = \frac{W}{1 + 2A} = \frac{7}{1 + (2 \times 270)} \\ = 1.2936\% \quad \dots \text{Ans.}$$

3. Continuous ARQ with $W = 127$:

$$\eta = \frac{127}{1 + (2 \times 270)} \\ = 23.4696\% \quad \dots \text{Ans.}$$

Ex. 2.16.4 : 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 :

$$\text{Bit rate } R = 19.2 \text{ kbps} = 19.2 \times 10^3 \text{ bps}$$

$$\text{Frame size } N = 960 \text{ bits}$$

$$\text{Propagation time } t_p = 0.06 \text{ sec.}$$

$$\text{Window size } W = 3 \text{ and } 7.$$

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 $W = 3$,

$$\eta = \frac{W}{1+2A}$$

Where $W = \text{Window size}$

$$\therefore \eta = \frac{3}{1+(2 \times 1.2)} \\ = 0.8823$$

...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. 2.16.5 : 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 :

$$\eta = \frac{t_f}{t_f + 2t_p}$$

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. 2.16.5

Review Questions

- Q. 1 State the various design issues for the data link layer.
- Q. 2 State and explain the various services provided to the Network layer.
- Q. 3 What are the different framing methods ?
- Q. 4 Explain character stuffing.
- Q. 5 What is bit stuffing ?
- Q. 6 Explain the function of timer.
- Q. 7 Write a note on error control.
- Q. 8 Explain the simplex protocol for noisy channel.
- Q. 9 What is piggybacking ?
- Q. 10 Write a note on sliding window protocols.
- Q. 11 Explain the stop and wait protocol.
- Q. 12 State drawbacks of stop and wait protocol.
- Q. 13 Explain the Go back n protocol.
- Q. 14 What is pipelining ?
- Q. 15 Write a note on : Selective repeat ARQ.
- Q. 16 Define throughput efficiency and explain how it can be increased ?
- Q. 17 Write a note on : HDLC protocol.
- Q. 18 Draw and explain the frame structure of HDLC.
- Q. 19 State and explain various frame types in HDLC.
- Q. 20 Explain transparency and bit stuffing in HDLC.
- Q. 21 Write a note on : SDLC.
- Q. 22 Write a note on : PPP.
- Q. 23 Explain the frame format of PPP.
- Q. 24 Explain the flow diagram for PPP connection.
- Q. 25 What is LCP and NCP ?

□□□

CHAPTER

3

Unit III

Medium Access Control

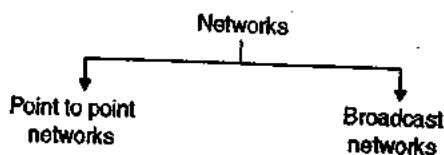
Syllabus :

Channel allocation: Static and Dynamic, Multiple Access Protocols: Pure and Slotted ALOHA, CSMA, WDMA, IEEE 802.3, Standards and Frame Formats, CSMA/CD, Binary Exponential Back-off algorithm, Fast Ethernet, Gigabit Ethernet, IEEE 802.11a/b/g/n and IEEE 802.15 and IEEE 802.16 Standards, Frame formats, CSMA/CA.

3.1 Introduction :

- We can classify the networks into two categories as shown in Fig. 3.1.1.
- 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.

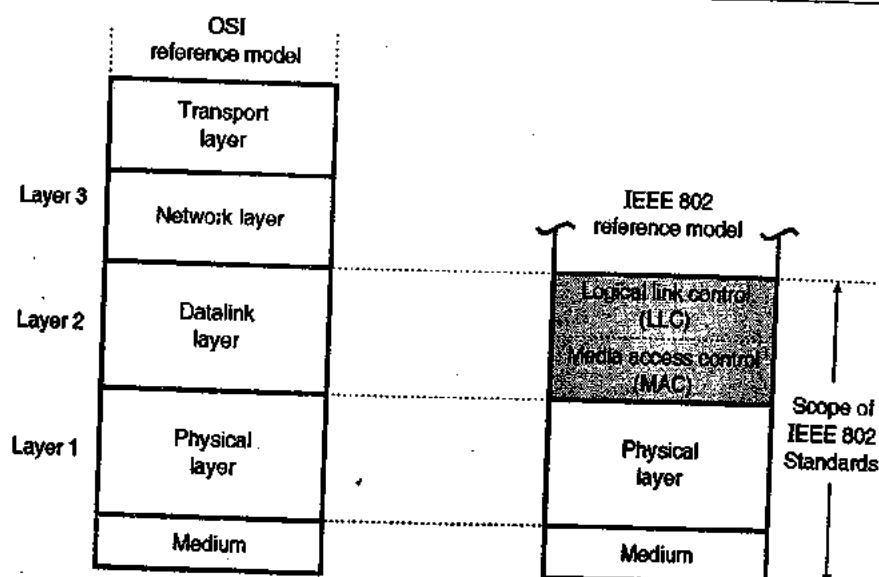
- The MAC sublayer is very important in LANs because it is a broadcast network.



(G-264) Fig. 3.1.1

3.1.1 MAC and LLC Sublayers :

- Fig. 3.1.2 shows the layered OSI model (partial) to show the position of MAC and LLC sublayers.
- We will discuss the broadcast protocols corresponding to the lower layers (1 and 2) of the OSI model as shown in Fig. 3.1.2.



(G-265) Fig. 3.1.2 : IEEE 802 protocol layers compared to OSI model

- Fig. 3.1.2 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 :

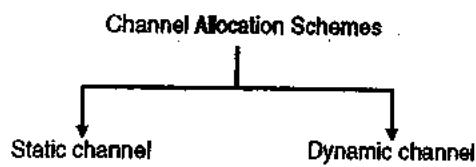
- To perform the control of access to media.
- It performs the unique addressing to stations directly connected to LAN.
- Detection of errors.

Functions of Logical Link Control (LLC) sublayer :

- Error recovery
- It performs the flow control operation
- User addressing.

3.2 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. 3.2.1.



(G-26) Fig. 3.2.1

3.2.1 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.

3.2.2 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. 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.

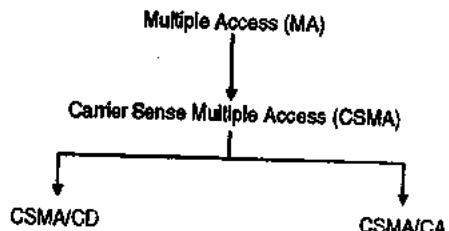


3.3 Multiple Access :

- 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 :
 - Random Access
 - Controlled Access
 - Channelization.
- Let us discuss them one by one.

3.3.1 Random Access :

- 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. 3.3.1.



(G-267)Fig. 3.3.1 : Evolution of random access methods

3.3.2 Evolution of Random Access Methods :

- The first method in the evolution ladder of Fig. 3.3.1, 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.

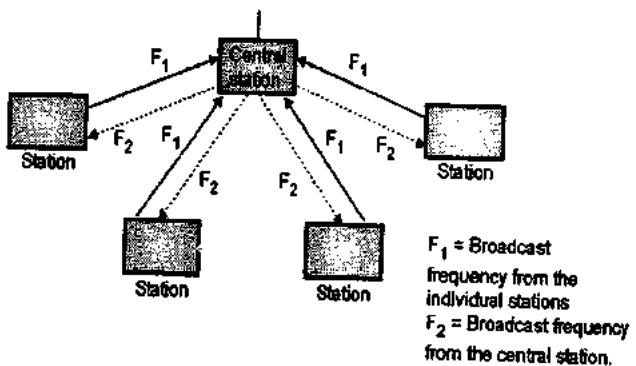
3.4 Multiple Access (ALOHA System) :

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 :
 - Pure ALOHA – does not require global time synchronisation.
 - Slotted ALOHA – requires time synchronisation.

3.4.1 Pure ALOHA :

- 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. 3.4.1, when the central station receives a frame it sends an acknowledgement on a different frequency.

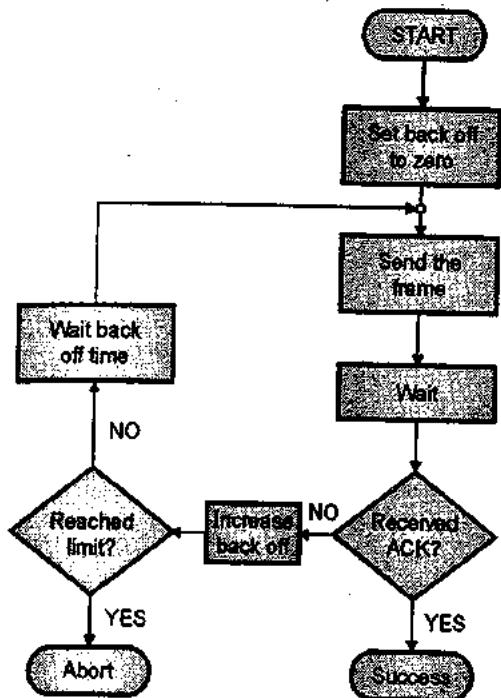


(G-268)Fig. 3.4.1 : Pure ALOHA system

- If a user station receives an acknowledgement it assumes that the transmitted frame was successfully received and if it does not 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.

3.4.2 Protocol Flow Chart for ALOHA :

- Fig. 3.4.2 shows the protocol flow chart for ALOHA.



(G-26) Fig. 3.4.2 : Protocol flow chart for ALOHA

Explanation :

- A station which has a frame ready for transmission will send it.
- Then it waits for some time.
- 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.

3.4.3 Efficiency of an ALOHA Channel :

- 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 times 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

$$\text{Frame time} = \frac{\text{Frame length}}{\text{Bit rate}}$$

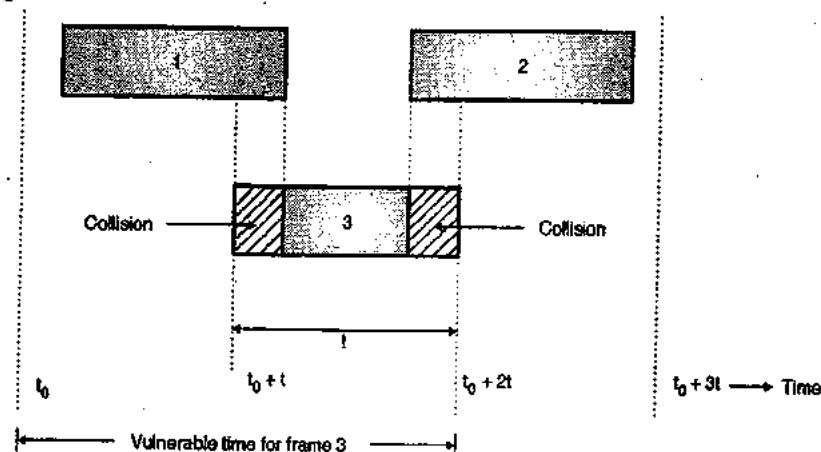
- We assume that ∞ number of users generate new frames according to the Poisson's distribution with an average N frames per frame time.
- The value of $N > 1$ indicates that the users are generating frames at a rate higher than that can be handled by the channel. So most of the frames will face collision. 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. 3.4.3.



- What is the condition for frame 3 in Fig. 3.4.3 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

$$P_0 = \frac{G^0 e^{-G}}{0!} = e^{-G}$$

- 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 $S = G P_0$

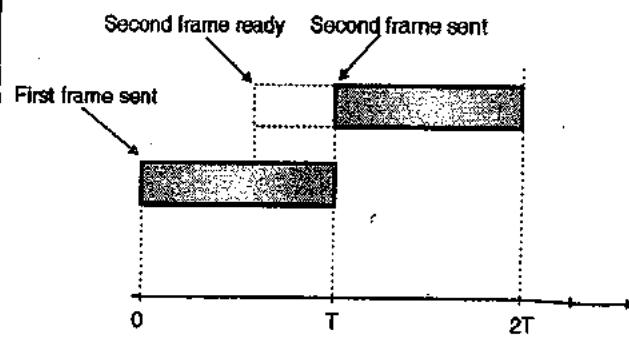
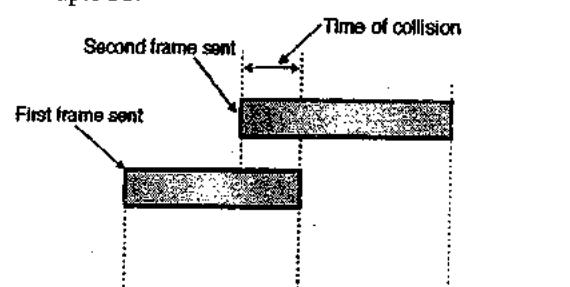
$$\therefore S = G e^{-2G}$$

- Fig. 3.4.5 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.

3.4.4 Slotted ALOHA :

- 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. 3.4.4. In case of pure ALOHA allowing a station to transmit at arbitrary times can waste time upto $2T$.



(G-271) Fig. 3.4.4

- 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. 3.4.4(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. 3.4.5. 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.

3.4.5 Comparison of Pure and Slotted ALOHA :

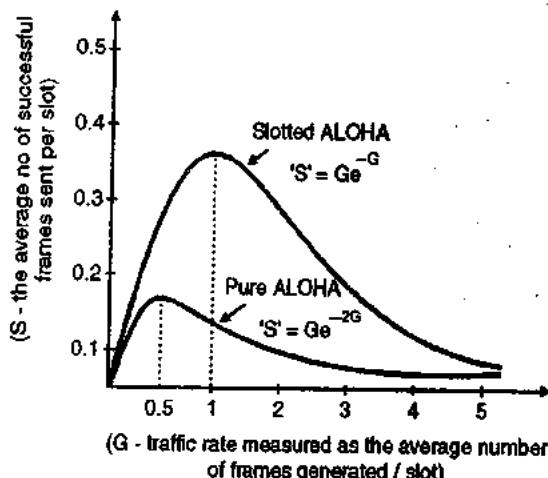
- A mathematical model can be created for the relationship between the number of frames transmitted and the number of frames transmitted successfully.
- Let G represent the traffic measured as the average number of frames generated per slot.
- Let S be the success rate measured as the average number of frames sent successfully per slot.
- The relationship between G and S for both pure and slotted ALOHA is given as follows :

$$\text{Pure ALOHA} \rightarrow S = Ge^{-2G}$$

$$\text{Slotted ALOHA} \rightarrow S = Ge^{-G}$$

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. 3.4.5.
- As seen in the Fig. 3.4.5 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. 3.4.5 : 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.

3.5 Carrier Sense Multiple Access (CSMA) :

- 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 transmit 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 :

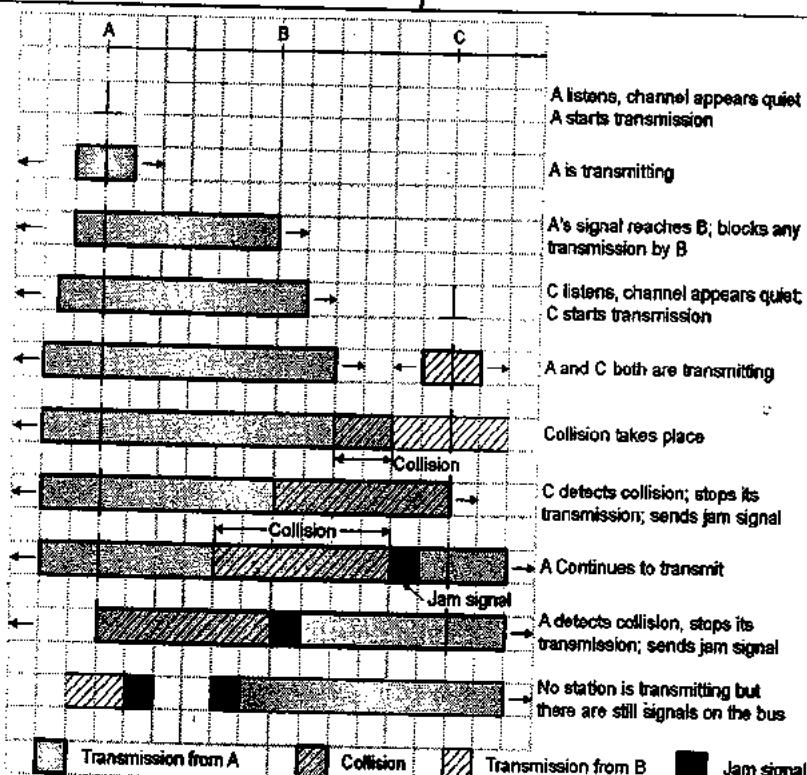
- The possibility of such collisions and retransmissions is reduced in the p-persistent CSMA. In this scheme all the waiting stations are not allowed to transmit simultaneously as soon as the channel becomes idle.
- A station is assumed to be transmitting with a probability "p". For example if $p = 1/6$ and if 6 stations are waiting then on an average only one station will transmit and others will wait.

3.5.1 Carrier Sense Multiple Access/Collision Detection (CSMA/CD) :

- The CSMA/CD specifications have been standardized by IEEE 802.3 standard. It is a very widely used MAC protocol.

Media access control :

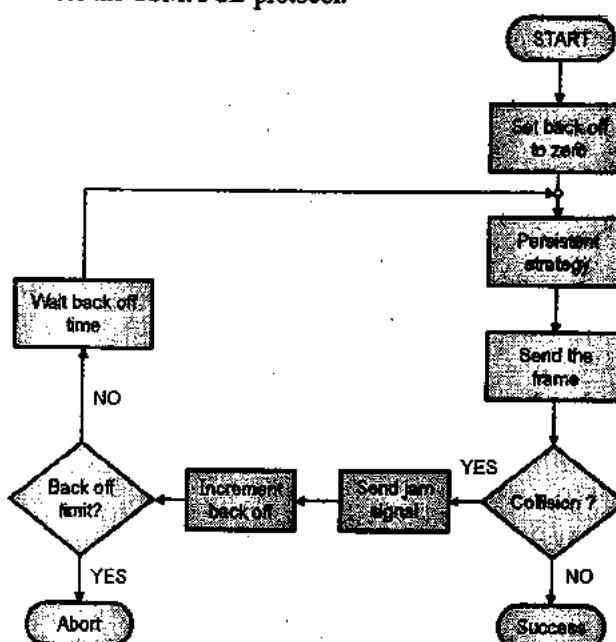
- The problem in CSMA explained earlier is that a transmitting station continues to transmit its frame even though a collision occurs.
- The channel time is unnecessarily wasted due to this. In CSMA/CD, if a station receives other transmissions when it is transmitting, then a collision can be detected 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. 3.5.1.



(G-273)Fig. 3.5.1 : CSMA/CD scheme

2 CSMA/CD Procedure :

Fig. 3.5.2 shows a flow chart for the CSMA/CD protocol.



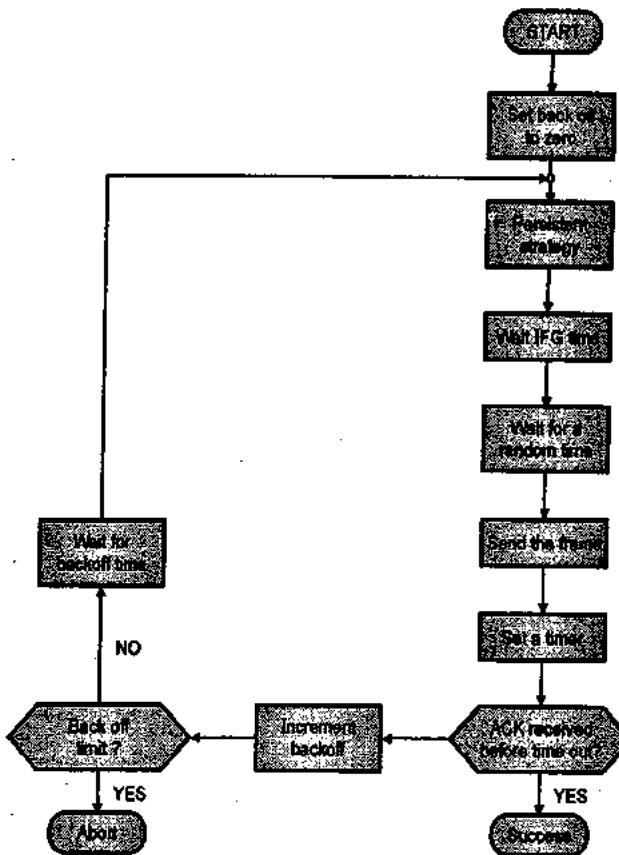
(G-276)Fig. 3.5.2 : CSMA/CD procedure

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.

3.5.3 CSMA/CA :

- The long form of CSMA/CA is CSMA protocol with collision avoidance.
- Fig. 3.5.3 shows the flow chart explaining the principle of CSMA/CA.



(G-277)Fig. 3.5.3 : 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.

3.6 Collision Free Protocols :

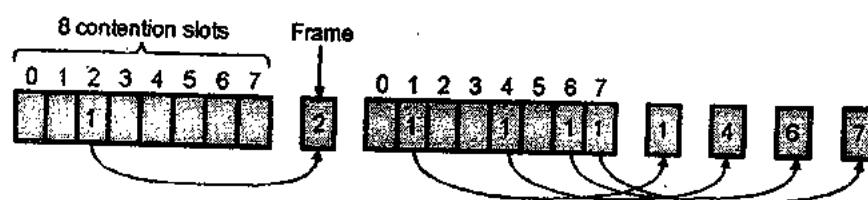
- As we have seen that almost collisions can be avoided in CSMA/CD, they can still occur during the contention period.
- The collision during contention period affects the system's performance adversely. This happens when

the cable is long and length of frames are short. This problem becomes serious as fiber optic network come into use.

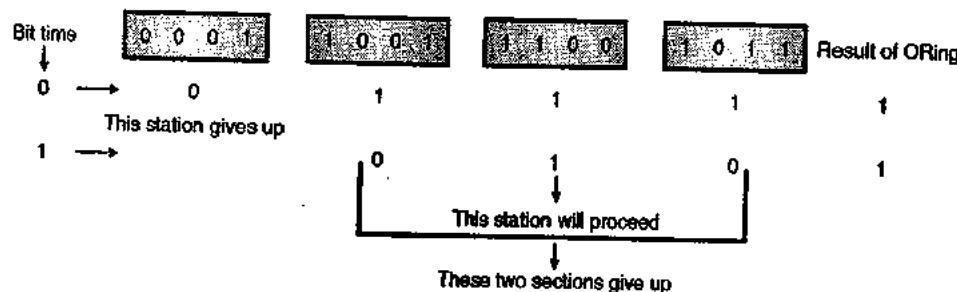
- Here we will discuss some protocols that resolve the collisions during the contention period.

3.6.1 Bit-map Protocol :

- 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. Refer Fig. 3.6.1



(G-278)Fig. 3.6.1 : A bit-map protocol



(G-279)Fig. 3.6.2 : Binary countdown

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 protracted 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 $1.5N$ slots.

3.6.2 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.
- 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. Refer Fig. 3.6.2.

3.6.3 Limited Contention Protocols :

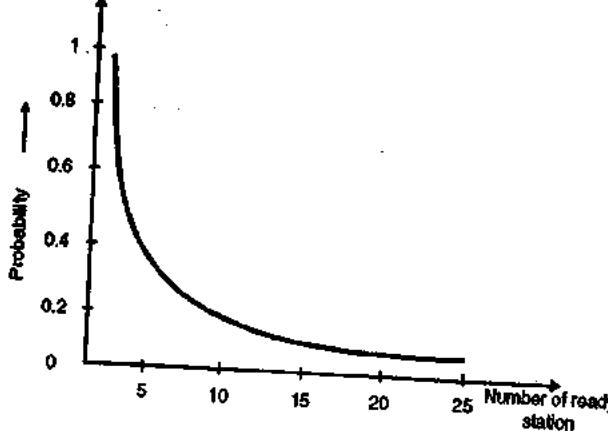
Meaning of contention system :

- 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 :
 1. Contention (such as CSMA) protocols
 2. 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 at 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. 3.6.3 shows the graph of probability plotted against number of stations ready to transmit their frames.

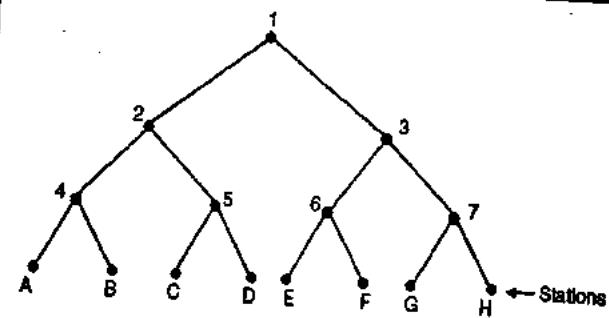


(G-268)Fig. 3.6.3

- 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.

3.6.4 The Adaptive Tree Walk Protocol :

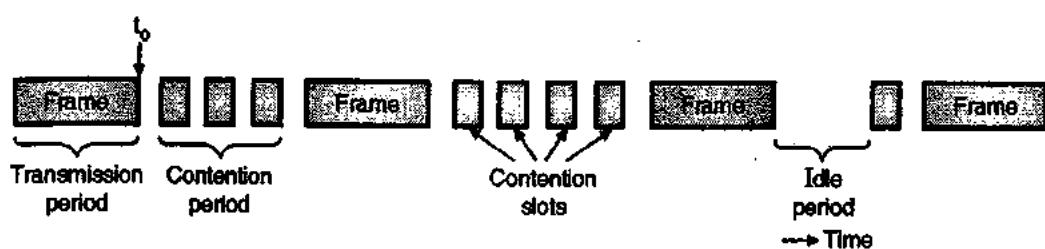
- The assignment of stations to the slots can be done with the help of a simple algorithm called adaptive tree walk protocol.
- It is imagined that the stations are leaves of a binary tree as shown in Fig. 3.6.4.
- The tree for eight stations is shown in Fig. 3.6.4. In the first contention slot which 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.



(G-281)Fig. 3.6.4 : Adaptive tree walk protocol

3.7 Binary Exponential Back off Algorithm :

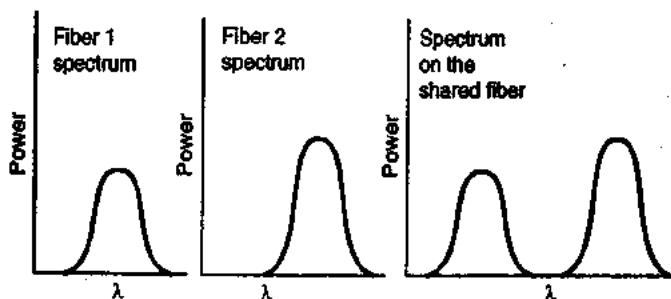
- Refer the model of Fig. 3.7.1.
- After a collision, the time is divided into discrete slots whose length is equal to the worst-case round trip propagation time on the Ether ($2t$).
- In order to accommodate the longest path allowed by the Ethernet, the slot time is fixed to be equal to 512 bit times or 51.2 μ sec.
- After the first collision takes place, each station will wait either 0 or 1 slot times before trying again.
- If two stations collide and each one picks up the same random number, then they will collide again.
- After the second collision takes place, each station picks up either 0, 1, 2 or 3 at random and then waits for those many number of slots (i.e. from 0 to $2^2 - 1$ slots).
- If the third collision takes place the probability of which is about 0.25 then, the next time each station waits for the randomly chosen number of slots from interval 0 to $2^3 - 1$.
- In general after "n" collisions, a random number between 0 and $2^n - 1$ is chosen and those many slots are skipped.
- But after 10 collisions the randomization interval is restricted to a maximum of 1023 slots.
- This algorithm is called as **binary exponential backoff**.
- It was selected to dynamically adapt the number of stations trying to send.
- If the randomization interval for all the collisions was 1023 i.e. constant, then the chance of second collision between two stations would be negligible. But then the average waiting time after the collision will also be very long (hundreds of slot times). This will introduce a lot of delay.
- In the binary exponential algorithm, the randomization interval increases exponentially as more and more consecutive collisions take place. This ensures that the delay is kept low when only a few stations collide and the collisions are resolved in a reasonable amount of time, when many stations collide.



(G-1275) Fig. 3.7.1

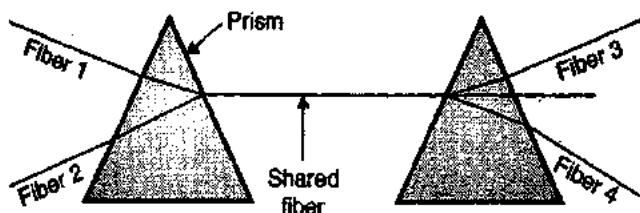
3.7.1 Wavelength Division Multiplexing :

- WDM is the variation of FDM, for fiber optic channels.



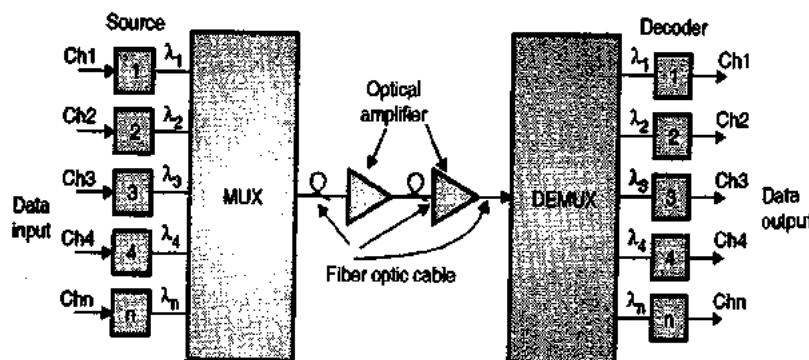
(G-1242) Fig. 3.7.2(a)

As shown in Figs. 3.7.2(a) and (b) 2 fibres come together at a prism, each having energy in a different band. After passing through the prism, beams are combined onto a single shared fiber. For transmission to a distant destination, where they are split again.

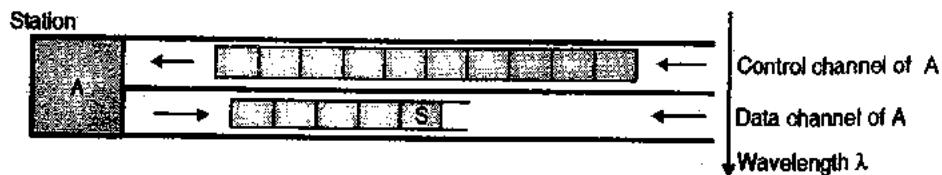


(G-1243) Fig. 3.7.2(b)

- Channels having different frequency ranges can be multiplexed on a long fiber.
- The only difference with 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 channels together over long routes. Necessary condition is that incoming channels use different frequency.
- Potential application of WDM is in the FTTC (Fiber To The Curb) systems.
- In the Fig. 3.7.2(a) we have a fixed wavelength system bits from fiber 1 go to fiber 3 and bits from fiber 2 go to fiber 4.
- It is not possible to have bits go 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 tunable filters.
- Alternatively, input fibers could be tunable and output ones fixed. Having both to be tunable is unnecessary expense.
- A simple block diagram of WDM transmitter and receiver system with different channels is as shown in Fig. 3.7.3.



(G-166) Fig. 3.7.3 : WDM system



(G-1244) Fig. 3.7.4 : WDMA principle

3.7.2 Wavelength Division Multiple Access Protocols (WDMA) :

- A different approach to channel allocation is to divide the channel into sub channels using FDM, TDM, or both, and dynamically allocate them as needed.
- Schemes like this are commonly used on fiber optic LANs in order to permit different conversations to use different wavelengths at the same time.
- A simple way to build an all-optical LAN is to use a passive star coupler.
- In effect, two fibers from each station are fused to a glass cylinder. One fiber is for output to the cylinder and one for input from the cylinder. Passive stars can handle hundreds of stations.
- To allow multiple transmissions at the same time, the spectrum is divided up into channels (wavelength bands). In this protocol, WDMA (Wavelength Division Multiple Access), each station is assigned two channels.
- A narrow channel is provided as a control channel to signal the station, and wide channel is provided so the station can output data frames.
- Each channel is divided into groups of time slots as shown in Fig. 3.7.4.
- The control channel of station A is used by the other stations to contact station A.

- Whereas the wide data channel is used by station A to send its data to other stations.
- All the channels are synchronized by a single global clock.
- This protocol can be used for three types of traffic as follows :
 1. Constant data rate connection-oriented traffic, such as uncompressed video.
 2. Variable data rate connection-oriented traffic, such as a file transfer.
 3. Datagram traffic, such as UDP packets (User Datagram Protocol).
- For the two connection oriented protocols, if station A is to communicate with B then it should first insert a connection request frame on B's control channel.
- If B accepts this request, then A should send data on the data channel of B.
- Each station has two transmitters and two receivers, as follows :
 1. A fixed-wavelength receiver for listening to its own control channel.
 2. A tunable transmitter for sending on other station's control channel.
 3. A fixed-wavelength transmitter for outputting data frames.
 4. A tunable receiver for selecting a data transmitter to listen to.

- Every station will listen to its own control station in order to know about the incoming requests but it has to tune to the transmitter's wavelength to acquire data.
- Various types of WDMA protocol are possible. One of the variations can be to give each station a slot in a common control channel instead of giving a separate control channel.
- Another variation is to use a single tunable transmitter and a single tunable receiver per station with each station's channel being divided up into control slots followed by $(n + 1)$ data slots.
- When a large number of frequencies are being used, the system is sometimes called DWDM (Dense Wavelength Division Multiplexing).

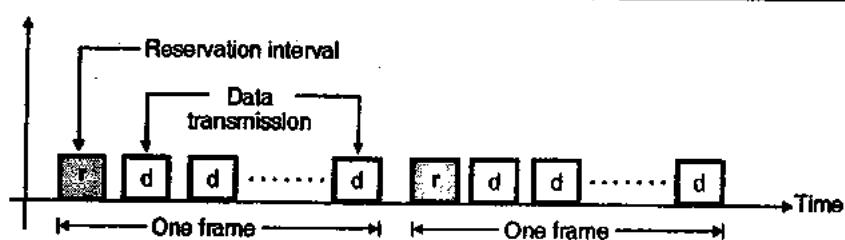
3.8 Controlled Access :

- 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.

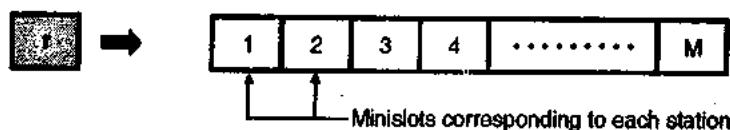
- In this section we will discuss the scheduling approaches to the medium access control.
- There are three important approaches in the scheduling approach as follows :
 - Reservation system
 - Polling system
 - Token passing ring networks.

3.8.1 Reservation Systems :

- The principle of reservation system can be understood from Fig. 3.8.1.
- 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. 3.8.1(a).

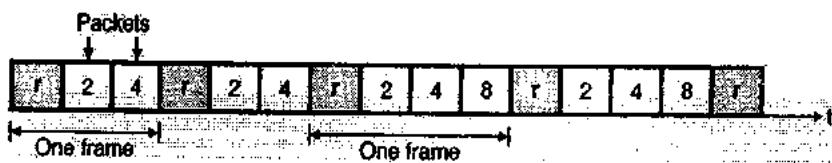


(a) Transmission in reservation systems



(b) Details of reservation interval

(L-733)Fig. 3.8.1 : Basic reservation system



(a) Negligible propagation delay



(b) Non negligible propagation delay

(L-734)Fig. 3.8.2 : Operation of reservation system with negligible and non-negligible delays



- Fig. 3.8.1(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 minislot.
- 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. 3.8.2.
- Refer Fig. 3.8.2(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,

$$\rho_{\max} = \frac{1}{1+v} \dots \text{for one packet reservation/minislot}$$

- If $v \ll 1$ then the value of ρ_{\max} can be very high.
- Now refer Fig. 3.8.2(b) which shows a reservation system with some finite non zero propagation delay which cannot 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,

$$\rho_{\max} = \frac{1}{1+(v/k)} \dots \text{for k packet reservation/minislot}$$

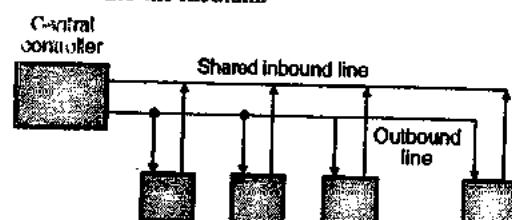
- Note that this value of ρ_{\max} will be higher than that for the single packet reservation/minislot.

Effect of number of stations (M) :

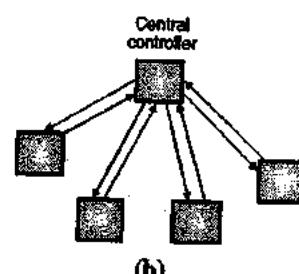
- The reservation intervals introduce overhead which is proportional to M. That means the reservation interval becomes $M \times v$.
- As the number of stations (M) become very large, this overhead will become significant. This then becomes a serious problem.
- This problem can be sorted out by not allocating 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.

3.8.2 Polling :

- Now consider polling system shown in Fig. 3.8.3. 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.



(a)



(b)

(L-73) Fig. 3.8.3 : 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. 3.8.3(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. 3.8.3(b) shows another system where it is possible to use polling. The central controller of this system can make use of radio transmission.
- Fig. 3.8.4 shows the sequence of polling messages.
- 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 T' is the sum of walk time corresponding to each station.

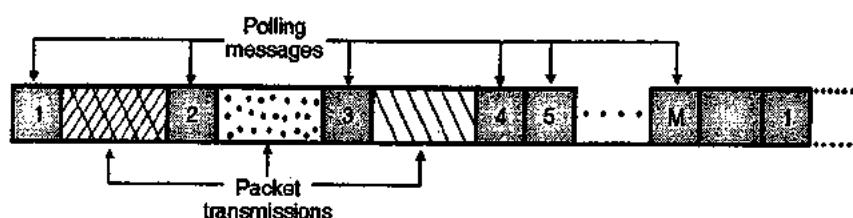
3.8.3 Token Passing :

- 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.

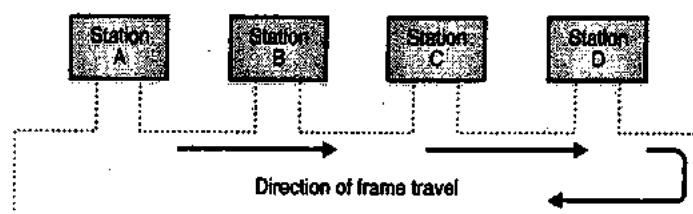
- In a token passing network, each station has a predecessor and successor as shown in Fig. 3.8.5.
- The frames travel in one direction. They come from the predecessor and go to the successor as shown in Fig. 3.8.5.
- A token frame is circulated around the ring when no data is being transmitted and the 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.

3.9 Channelization :

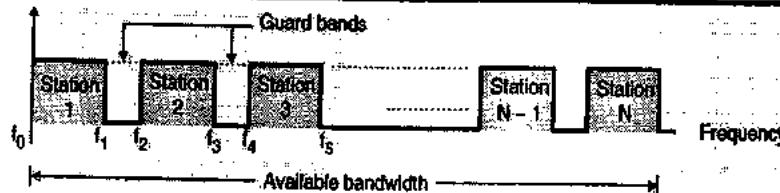
- This is a multiple access method in which the total bandwidth of the common link is shared in the frequency domain, the time domain or through codes.
- Depending on the method of sharing there are three channelization techniques :
 1. FDMA : Frequency Division Multiple Access
 2. TDMA : Time Division Multiple Access
 3. CDMA : Code Division Multiple Access.



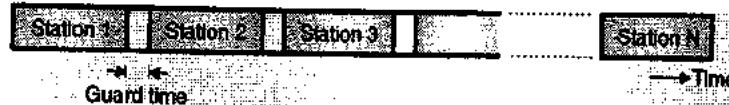
(L-736) Fig. 3.8.4 : Polling messages and transmissions in a polling system



(L-737) Fig. 3.8.5 : Token passing network



(L-739) Fig. 3.9.1 : Concept of FDMA



(L-740) Fig. 3.9.2 : Concept of TDMA

3.9.1 FDMA :

- 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.
- The concept of FDMA is illustrated in Fig. 3.9.1.
- FDMA is a data link layer protocol which uses FDM at the physical layer.
- 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.

Advantages 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.

Disadvantages of FDMA :

1. Each channel or earth station can use only a part of the total satellite bandwidth.
2. Inspite of guard bands being provided, there is some adjacent channel interference present.
3. As FM is used, it requires larger bandwidth, hence less number of channels will be accommodated in the bandwidth of a satellite.
4. Due to the nonlinearity of companders, the intermodulation products are generated.

3.9.2 TDMA :

- 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. 3.9.2 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.
- TDMA is a data link layer protocol which uses TDM at the physical layer.
- TDMA finds its application in cellular phones and satellite networks.

Advantage of TDMA :

Since only one station is present at any given time, the generation of intermodulation products will not take place.

Disadvantage of TDMA :

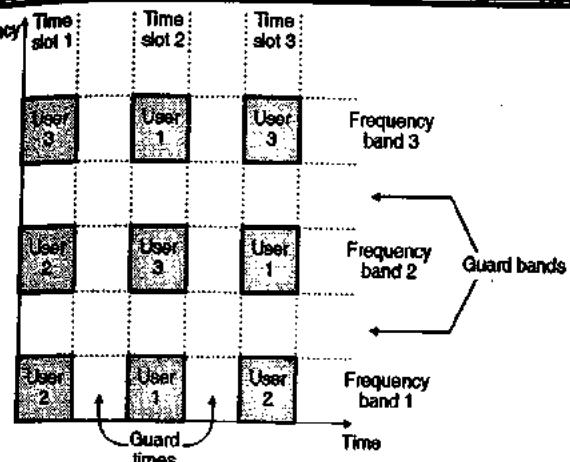
TDMA needs synchronization which makes it more complicated as compared to FDMA.

3.9.3 Code Division Multiple Access (CDMA) :

- 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. 3.9.3 : 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. 3.9.3.
- CDMA does not need any synchronization, but the code sequences or signature waveforms are required to be used.

3.9.4 Comparison of FDMA, TDMA and CDMA :

Sl. No.	FDMA	TDMA	CDMA
1.	Overall bandwidth is shared among many stations.	Time sharing takes place.	Sharing of bandwidth and time both takes place.
2.	Due to nonlinearity of devices 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 is not necessary.	Synchronization is essential.	Synchronization is not necessary.
4.	Code word is not	Code word is not	Code words are

Sl. No.	FDMA	TDMA	CDMA
5.	required.	required	required.

3.10 Ethernet :

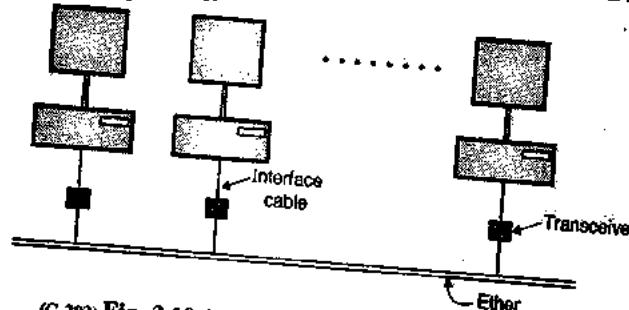
- Both Internet and ATM were designed for wide area networking. But in many applications, a large number of computers are to be connected to each other.
- For this the local area network (LAN) was introduced. The most popular LAN is called Ethernet.
- The IEEE 802.3 standard is popularly called as Ethernet. 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 :
 - Traditional Ethernet (10 Mbps)
 - Fast Ethernet (100 Mbps)
 - Gigabit Ethernet (1000 Mbps)
- Traditional Ethernet was created in 1976 and has a data rate of 10 Mbps.
- The fast Ethernet is its next version and has a data rate of 100 Mbps.
- The Gigabit Ethernet operates at the data rate of 1000 Mbps or 1 Gbps.

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.
- The architecture of the original Ethernet is shown in Fig. 3.10.1.



(G-293) Fig. 3.10.1 : Architecture of original Ethernet

- 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.

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.

3.10.1 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.

3.10.2 Bridged Ethernet :

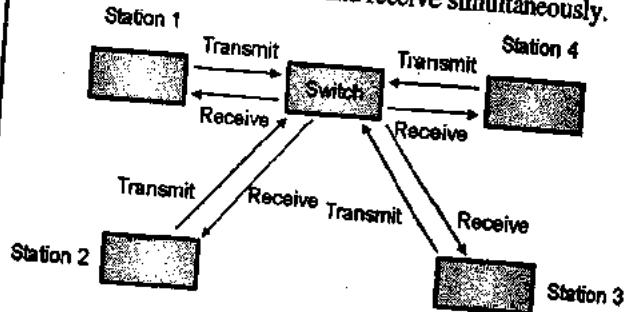
- We can divide a LAN into smaller segments by inserting bridges in between.
- Bridges affect the Ethernet LAN in the following two ways :
 1. The bandwidth requirement increases.
 2. The collision domains get separated.

3.10.3 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.

3.10.4 Full Duplex Ethernet :

- The 10 Base 5 and 10 Base 2 Ethernets have a serious limitations. 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.



(G-294) Fig. 3.10.2 : Full duplex switched Ethernet

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. 3.10.2 shows the 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.

3.10.5 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.

3.10.6 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.

3.11 IEEE Standards :

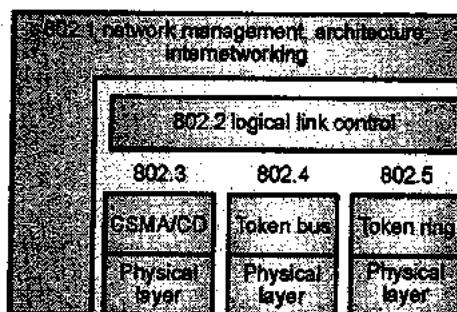
The Institution of Electrical and Electronics Engineers (IEEE) has developed the layered architecture and other standards of LAN, under their project 802 set up in 1980. The IEEE 802 standards are as follows :

- 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 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 :

- Carrier sense multiple access/collision detection (CSMA/CD)
- Token bus and
- 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. 3.11.1.
- 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 IEEE802.2.



(G-29) Fig. 3.11.1 : IEEE LAN and related standards

3.12 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.

3.12.1 Traditional Ethernet Frame :

Fig. 3.12.1 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. 3.12.1 : Traditional Ethernet frame

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. 3.12.2 : Minimum and Maximum length frame formats of traditional Ethernet

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 64 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 SFD 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.

3.12.2 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. 3.12.2(a) and that of the maximum length frame is shown in Fig. 3.12.2(b).
- 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.

3.12.3 Addressing :

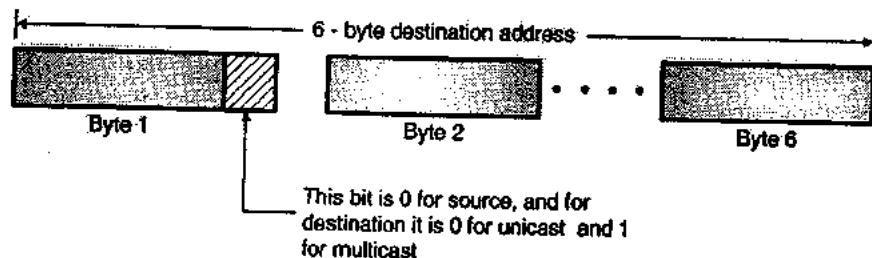
- There can be various types of stations connected on an Ethernet network such as PC on workstation or printer.
- Each station has its own Network Interface Card (NIC) which fits inside the station to contain the 6 byte physical address of the station.
- Fig. 3.12.3 shows a 6-byte Ethernet address in the hexadecimal notation.

04 – 02 – 01 – 06 – 1C – 5B

(G-307) Fig. 3.12.3 : Ethernet address

3.12.4 Types of Addresses :

- A source address is only unicast address. This is because the frame comes from only one source.



(G-308) Fig. 3.12.4 : Difference between unicast and multicast addresses



(G-312) Fig. 3.12.5 : Categories of traditional Ethernet

- The destination address can be one of the following three types :
 1. Unicast
 2. Multicast
 3. Broadcast
- Fig. 3.12.4 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 :

- Broadcasting process is the process in which the sender transmit and all others receive or listen.
- This type of destination address is a special case of multicast address in which all stations are destinations.

3.12.5 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.

3.12.6 Physical Layer Implementation of Traditional Ethernet :

The standard has defined four different implementations for the baseband (digital) 10 Mbps Ethernet as shown in Fig. 3.12.5.

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 :
 - 10 BASE FP (P for passive)
 - 10 BASE FL (L for link)
 - 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.

3.13 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.

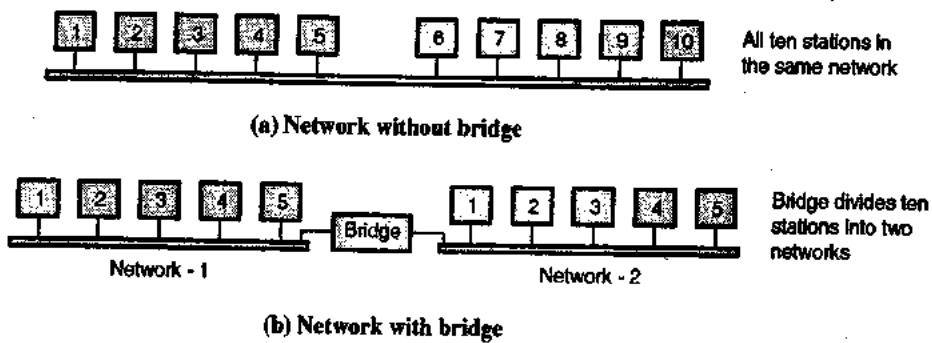
3.14 Bridged Ethernet :

- 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 :

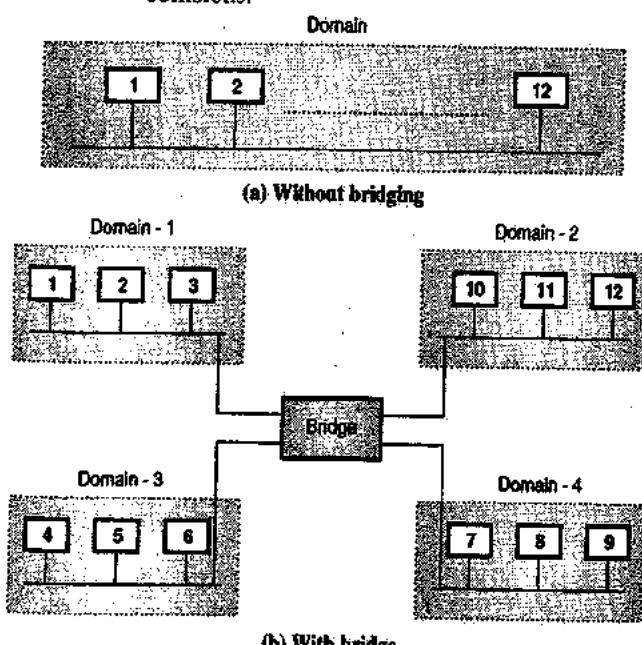
- In the traditional Ethernet the total capacity the network is 10 Mbps and it is shared among all the stations when a frame is to be sent. The stations share the bandwidth of the network.
- If only one station has frames to send, then it can use the entire bandwidth 10 Mbps for itself. But if there 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. 3.14.1 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. 3.14.1 : Increase in bandwidth due to bridge

2. Separation of collision domain :

- Fig. 3.14.2 explains the concept of separation of collision domains. Fig. 3.14.2(a) shows the collision domains for the original network without bridge whereas Fig. 3.14.2(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.

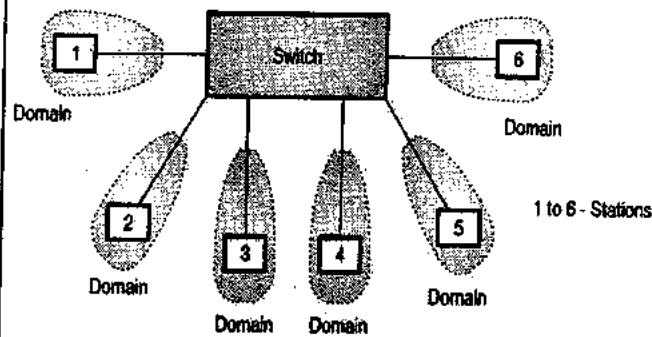


(G-314)Fig. 3.14.2 : Collision domains in the nonbridged and bridged network

3.15 Switched and Full Duplex Ethernet :

3.15.1 Switched Ethernet :

- The concept of bridged LAN can be extended to form the switched LAN.



(G-315)Fig. 3.15.1 : Switched Ethernet

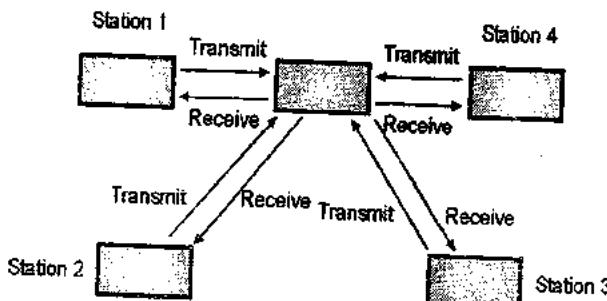
- An N port switch is used to connect N number of stations on the LAN. Each member of the LAN is connected to a port of the switch.
- The entire bandwidth is shared only between the stations and the switch. The collision domain is divided into N domains. This reduces the possibility of collisions in 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. 3.15.1.

3.15.2 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. 3.15.2 shows the 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.



(G-316)Fig. 3.15.2 : Full duplex switched Ethernet

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.

3.16 Fast Ethernet :

- 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.

3.16.1 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.

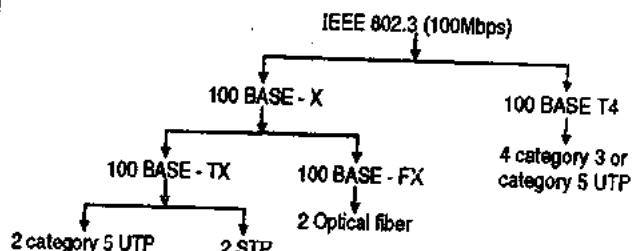
Features of the autonegotiation :

The important features of autonegotiation are :

- The non-compatible devices can be connected to each other.
- One device can be allowed to have multiple capabilities.
- A station can check hub's capabilities.

3.16.2 Physical Layer Implementation :

- Fig. 3.16.1 shows the various types of cables used for the fast Ethernet. 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.



(G-318) Fig. 3.16.1 : IEEE 802.3 100 BASE - T options

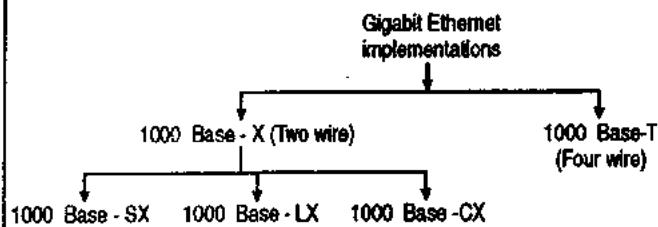
- All of the 100 BASE - T options shown in Fig. 3.16.1 use the IEEE 802.3 MAC protocol and frame format.
- 100 BASE - X indicates the options which use the medium specifications defined by FDDI.
- All the 100 BASE - X types use two physical links between any two nodes, one of them is used for transmission and the other one for the reception.
- Refer Fig. 3.16.1. 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.

3.17 Gigabit Ethernet :

- 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.

3.17.1 Physical Layer Implementation :

- 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. 3.17.1 shows the physical layer implementations for the Gigabit Ethernet.



(G-323) Fig. 3.17.1 : 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.

3.17.2 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 :
 - Data rate is to be upgraded to 10 Gbps.
 - This Ethernet should be downward compatible to the standard, fast and gigabit Ethernet.
 - Frame format and 48-bit address should be same as the older versions.
 - Minimum and maximum frame lengths should remain same.
 - This Ethernet should be connectable to the existing LAN, WAN and MAN.
 - This Ethernet should be mode compatible with the technologies like Frame Relay and ATM.

**MAC sublayer :**

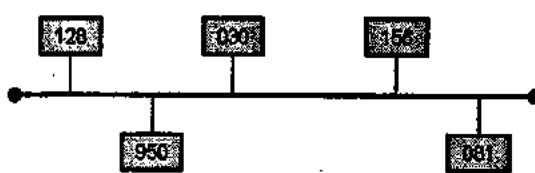
- This Ethernet operates only in the full duplex mode. Hence there is no possibility of contention. So CDMA/CD is not used in this Ethernet.

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

3.18 Token Bus : IEEE 802.4 :

- 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. 3.18.1. The physical topology is bus topology as shown in Fig. 3.18.1.
- 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.



(G-326) Fig. 3.18.1 : Physical topology in token passing

Frame format :

The frame format as specified by IEEE 802.4 is as shown in Fig. 3.18.3.

Number of bytes →	1(min)	1	1	2-6	2-6	4	1	
	Preamble	SD	FC	DA	SA	DATA	FCS	ED

Preamble : Bit synchronization

SA : Source address

SD : Frame Start Delimiter

DATA : Data field

FC : Frame Control (Type)

FCS : Frame check sequence

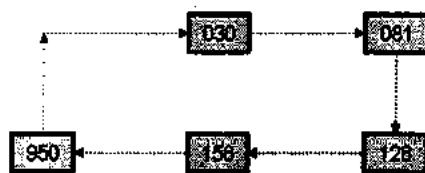
DA : Destination Address

ED : End delimiter

- Look at the sequence of stations in the logical sequence of token passing, shown in Fig. 3.18.2. 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. 3.18.2 : Logical sequence of token passing

Media access control :

- 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.

Fig. 3.18.3 : 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.

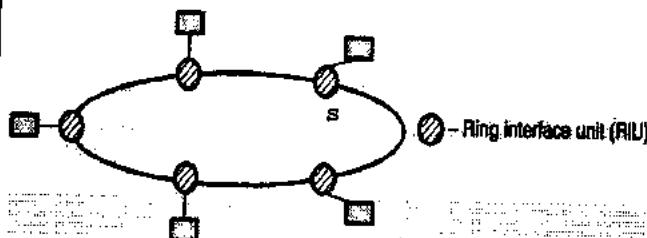
Physical specifications :

- 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.

3.19 Token Ring System [IEEE 802.5] :

- A token ring system is as shown in Fig. 3.19.1. 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.



(G-329) Fig. 3.19.1

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. 3.19.2.

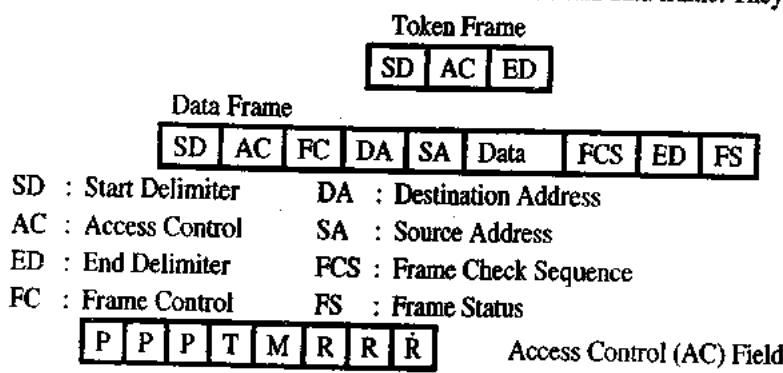
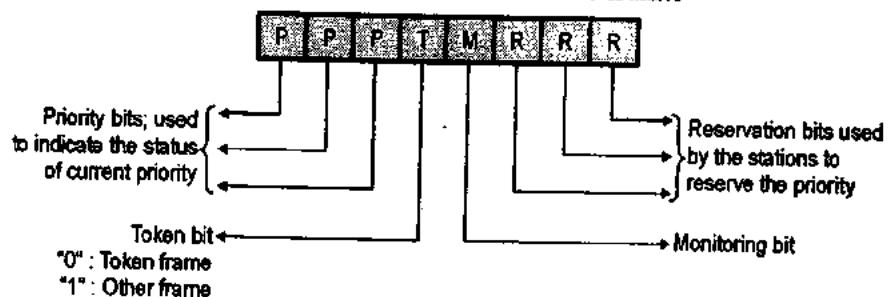


Fig. 3.19.2 : Formats of IEEE 802.5 frames



(G-33) Fig. 3.19.3 : Format of the access control (AC) field

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. 3.19.2.
- 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.

9. Frame Status (FS) : The details of this one byte long field are as shown in Fig. 3.19.2. 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.

Priority management :

As shown in Fig. 3.19.3 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.

3.19.1 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.

3.19.2 Comparison of 802.3, 802.4 and 802.5 IEEE Standard :

Sr. No.	Parameters	802.3 Ethernet	802.4 Token Bus	802.5 Token Ring
1.	Physical topology	Linear	Linear	Ring
2.	Logical topology	None	Ring	Ring
3.	Contention	Random chance	By token	By token
4.	Adding stations	A new station can be added almost anywhere on the cable at any time.	Distributed algorithms are needed to add new stations	Must be added between two specified stations.
5.	Performance	Stations often transmit immediately under light loads, but heavy traffic can reduce the effective data to nearly 0.	Stations must wait for the token even if no other station is transmitting. Under heavy load, token passing provides fair access to all stations.	Stations must wait for the token even if no other station is transmitting. Under heavy loads, token passing provides fair access to all stations.
6.	Maximum delay before transmitting	None	Bounded, depending on distance spanned and number of stations.	Bounded, depending on distance spanned and number of stations. However if priorities are used, a low priority station may have no maximum delay.
7.	Maintenance	No central maintenance	Distributed algorithm provide maintenance.	A designated monitor station performs maintenance.
8.	Cable used	Twisted pair; co-axial fiber optic	Co-axial	Twisted pair and fiber optic.
9.	Cable length	50 m to 2000 m	200 m to 500 m	50 m to 1000 m
10.	Frequency	10 Mbps to 100 Mbps	10 Mbps	4 to 100 Mbps
11.	Frame structure	1500 bytes	8191 bytes	5000 bytes

- 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.



3.19.3 Why can't Ethernet and Token Ring be used in a WAN?

- The Ethernet and token ring are not appropriate for use in WAN due to following reasons :
 1. Ethernet has a substantial analog component.
 2. It has no priorities.
 3. The cable length is limited.
 4. With increase in speed, efficiency decreases.
 5. At higher loads, the collision becomes a major problem and it reduces the throughput.
 6. In the token ring if one node or site fails then the whole network goes down.
 7. Installation and maintenance of token ring is difficult.
 8. Token ring supports only point to point link.

Ex. 3.19.1 : 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 :**

$$\text{For a slotted ALOHA, } P_0 = e^{-G}$$

$$\text{But } P_0 = 10\% \text{ i.e. } 0.1$$

$$\therefore 0.1 = e^{-G}$$

$$\therefore -2.3 = -G \quad \therefore G = 2.3$$

2. **Throughput :**

$$S = G e^{-G} = 2.3 e^{-2.3} = 0.23$$

3. Since G is beyond 1 the channel is overloaded.

Ex. 3.19.2 : Consider building a CSMA/CD network running at 1 Gbps 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 $\tau = 5 \mu\text{sec}$. $\therefore 2\tau = 10 \mu\text{sec}$.

3. To make CSMA/CD work, it must be ensured that the minimum frame size should be equal to $2\tau = 10 \mu\text{sec}$.

$$\text{But } R = 1 \times 10^9 \text{ bits/sec}$$

$$\therefore 1 \text{ sec} = 1 \times 10^9 \text{ bits}$$

$$\therefore 10 \times 10^{-6} \text{ sec} = ? \text{ bits}$$

$$\therefore \frac{1}{10 \times 10^{-6}} = \frac{1 \times 10^9}{x}$$

$$\therefore x = 1 \times 10^9 \times 10 \times 10^{-6}$$

$$= 10 \times 10^3 = 10,000 \text{ bits.}$$

Soln. : Minimum frame size = 10,000 bits or 1250 bytes.

Ex. 3.19.3 : 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.

$$1 \text{ sec} = 50 \text{ requests (transmissions)}$$

$$\therefore 40 \text{ msec} = x \text{ transmissions.}$$

$$\therefore \frac{1}{40 \times 10^{-3}} = \frac{50}{x} \quad \therefore x = 50 \times 40 \times 10^{-3}$$

$$\therefore x = 2$$

2. But number of transmissions (x) = e^G

$$\therefore 2 = e^G \quad \therefore G = 0.693$$

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 $G e^{-G}$

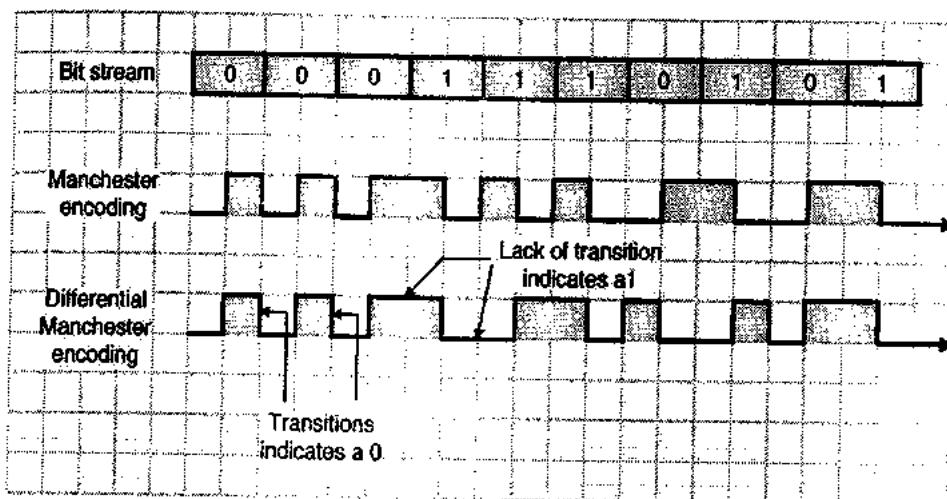
$$\text{i.e. } 0.693 e^{-0.693} = 0.3465 \text{ or } 34.65\%.$$

Ex. 3.19.4 : Sketch Manchester encoding and differential Manchester encoding for bit stream.

1. 0 0 0 1 1 1 0 1 0 1

Soln. :

The required waveforms are as shown in Fig. P. 3.19.4.



(G-337) Fig. P. 3.19.4

Ex. 3.19.5 : 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) :

$$\text{For the slotted ALOHA, } P_0 = e^{-G}$$

$$\therefore 0.2 = e^{-G}$$

$$\therefore G = 1.6094 \quad \dots \text{Ans.}$$

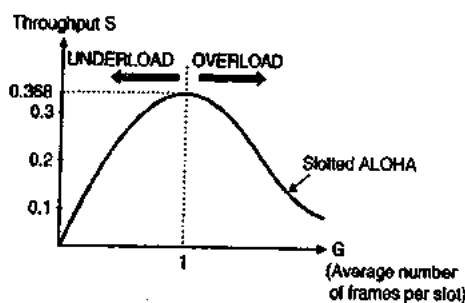
2. Throughput (S) :

$$S = Ge^{-G} = P_0 G = 0.2 \times 1.6094$$

$$\therefore S = 0.3218 \quad \dots \text{Ans.}$$

3. Status of the channel :

- From Fig. P. 3.19.5 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.



(G-338) Fig. P. 3.19.5 : Graph for slotted ALOHA

Ex. 3.19.6 : Using the binary countdown protocol find the highest priority station. The station addresses are as follows :

Station	Address
A	0010
B	0100
C	1010
D	1001
E	1011

Soln. :

Step 1 : All stations broadcast their MSBs :

Station	A	B	C	D	E
MSB	0	0	1	1	1

Stations A and B will give up.

Step 2 : Stations C, D, E broadcast their next bit :

Station	C	D	E
Next bit	0	0	0

Step 3 : Stations C, D, E broadcast their next bit :

Station	C	D	E
Next bit	1	0	1

Station D will give up.

Step 4 : Stations C and E broadcast their LSBs :

Station	C	E
LSB	0	1

Station C will give up.

So station E has the highest priority. Its station address is 1011.



Ex. 3.19.7 : An Aloha network user 19.2 kbps channel for sending message packets of 100 bits long size. Calculate the maximum throughput for pure ALOHA network.

Soln. :

Given : Rate of transmission = 19200 bits.

Frame length = 100 bits

∴ Number of frames per second

$$\begin{aligned} &= \frac{\text{Rate of transmission}}{\text{Frame length}} = \frac{19200}{100} \\ &= 192 \text{ frames/sec} \end{aligned}$$

The maximum throughput for a pure ALOHA system is 0.184.

$$\begin{aligned} \therefore \text{Throughput} &= 0.184 \times \text{Number of frames/sec.} \\ &= 0.184 \times 192 \\ &= 35.328 \text{ frames/sec.} \quad \dots \text{Ans.} \end{aligned}$$

Ex. 3.19.8 : 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 $d = 100 \text{ m}$

Propagation speed $V = 2 \times 10^8 \text{ m/sec.}$

Rate of transmission $R = 4 \text{ Mbps.}$

Delay introduced by each station = $b = 2.5 \text{ bits.}$

Step 1 : Calculate the total delay :

Delay introduced by N stations

$$\begin{aligned} &= \frac{N \times b}{R} = \frac{20 \times 2.5}{4 \times 10^6} \\ &= 12.5 \mu \text{sec} \quad \dots(1) \end{aligned}$$

Additional delay introduced by the ring

$$\begin{aligned} &= \frac{d}{V} = \frac{100 \text{ m}}{2 \times 10^8 \text{ m/S}} \\ &= 0.5 \mu \text{S} \quad \dots(2) \end{aligned}$$

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.

$$\begin{aligned} \therefore \text{Ring latency} &= \text{Total delay} \times \text{Rate of transmission} \\ &= 13 \times 10^{-6} \times 4 \times 10^6 \\ &= 52 \text{ bits} \quad \dots \text{Ans.} \end{aligned}$$

Ex. 3.19.9 : 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 :

$$\begin{aligned} \therefore \text{Number of frames/sec.} &= \frac{56000 \text{ bits}}{1000 \text{ bits/frame}} \\ &= 56 \text{ frames/sec} \end{aligned}$$

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. 3.19.10 : 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.

$$\begin{aligned} \therefore N &= \frac{R}{\text{bits/sec}} = \frac{10.3 \text{ kbps}}{10} \\ &= 1030 \quad \dots \text{Ans.} \end{aligned}$$

Ex. 3.19.11 : 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.

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 $2^5/2 = 16$.

3.20 Introduction to WLAN and WPAN :

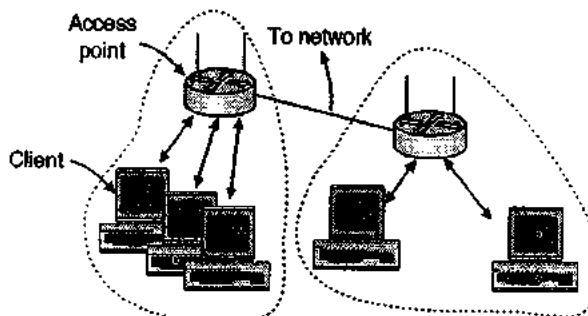
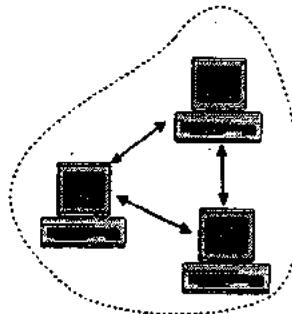
- We all know wired local area networks (LANs) very well. In order to get rid of the wiring associated with the interconnections of PCs in LANs, researchers have tried to use radio waves or infrared light as a replacement to the wires.
- Thus the wireless LANs i.e. WLANs got evolved.
- WPAN is a Wireless Personal Area Network. It is one step down from WLANs. The WPANs cover smaller areas and need to use less power for transmission.
- WPANs are used for networking of portable and very small computers, cell phones, printers, speakers, microphones, etc.

3.20.1 Wi-Fi :

- Wi-Fi is a popular technology which allows an electronic device to exchange data or to connect to the Internet using radio waves.
- We can define Wi-Fi as any Wireless Local Area Network (WLAN), product that are based on the IEEE 802.11 standards.
- The devices which can use Wi-Fi are personal computers, video game consoles, smart phones, some digital cameras, Tablet computers etc.
- Wireless communication is one of the fastest growing technologies.
- The wireless LANs are used in following applications :
 - Office buildings
 - Colleges
 - Public areas
- In this chapter we are going to discuss about two important wireless technologies for LANs :
 - IEEE 802.11 wireless LAN.
 - Bluetooth

3.21 Infrastructure and Ad-Hoc Networks :

- 802.11 networks can be used in two possible modes :
 - Infrastructure mode
 - Ad-hoc mode.
- The **infrastructure mode** is as shown in Fig. 3.21.1(a). The client such as laptop or a smart phone is connected to another network such as company Internet.
- In this mode the client is associated with an Access Point (AP) which is in turn connected to the other network as shown.
- The client sends and receives its packets via AP. Many such APs are connected together to form an extended 802.11 network.

**(a) Infrastructure mode****(b) Ad-hoc mode****(G-1527) Fig. 3.21.1 : Types of 802.11 networks**

- The other mode of operation is ad-hoc networks as shown in Fig. 3.21.1(b). In this mode a group of computers can communicate to each other directly without any access point (AP) in between.

3.21.1 The ISM Band :

- Internationally the ITU has designated some frequency bands called as the ISM (Industrial, Scientific and Medical) bands for unlimited usage. User or manufacturer does not need any licence to operate in the ISM band.
- These bands are used by wireless LANs and Wireless PANs (Bluetooth). This frequency band is



around 2.4 GHz. Parts of 900 MHz and the 5 GHz bands are also available for unlicensed use in USA and Canada.

3.22 Fundamentals of WLANs :

SPPU : May 15, Dec. 15

University Questions

Q. 1 Write short notes on Wireless LAN.
(May 15, Dec. 15, 4 Marks)

- In this section, we will discuss about the fundamental principle, concepts and requirements of WLANs.
- We will also discuss about WLAN types, their components and functionalities. During this discussion, the terms node, station and terminals are used interchangeably because they carry the same meaning.
- There are two types of terminals :
 1. Portable terminals
 2. Mobile terminals (MTs)
- Both types can move from one place to the other. But the portable terminals are accessed only when they are stationary.
- The Mobile Terminals (MTs) can be accessed even when they are in motion as they are more powerful.
- The wireless LANs are becoming more and more popular because they can satisfy the requirements like mobility, relocation of user, ad-hoc networking and coverage of locations which are difficult to connect using wires.
- Earlier the wireless LANs had many shortcomings. They were costly, could support only low data rates, a license was required. Hence there were limitations on the practical use of wireless LANs.
- But all these problems are being addressed now and the popularity of wireless LANs is increasing day by day.

3.22.1 Wireless LAN Configuration :

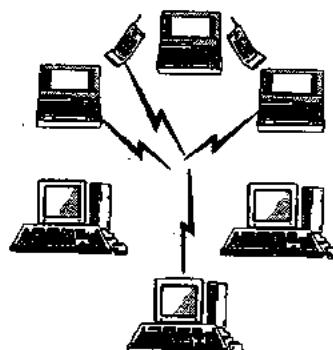
SPPU : May 15, Dec. 15

University Questions

Q. 1 Write short notes on Wireless LAN.
(May 15, Dec. 15, 4 Marks)

- Wireless LAN uses wireless communication as shown in Fig. 3.22.1.
- Devices such as workstations, laptop, computers, cordless telephones and other communication

appliances share the wireless medium such as 5 GHz radio link or infrared channel.



(G-37) Fig. 3.22.1 : Wireless LAN

3.22.2 Applications of Wireless LAN :

There are four applications of wireless LAN as follows :

1. LAN extension
2. Cross building interconnection
3. Nomadic access
4. Ad-hoc networks

3.22.3 Wireless LAN - 802.11 (Architecture) :

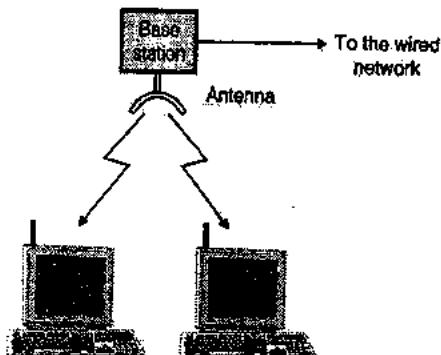
SPPU : May 15, May 16

University Questions

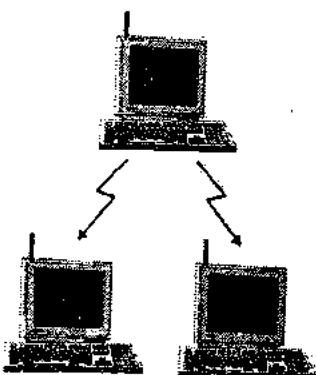
Q. 1 Explain WLAN architecture.

(May 15, 8 Marks, May 16, 6 Marks)

- In wireless LAN, each computer and note book computer is equipped with a short range transmitter and receiver to allow communication between them.
- The IEEE committee standardized the wireless LAN and the standard was 802.11.
- This standard had to work in two different modes :
 1. In the presence of a base station.
 2. In the absence of a base station.
- These two modes are shown in Fig. 3.22.2.



(a) With base station
Fig. 3.22.2(Contd...)



(b) Without base station (Ad hoc networking)

(G-371) Fig. 3.22.2 : Wireless networks

- In the network with base station, all the communication is passed through the base station. The base station (BS) is also called as the access point (AP) in 802.11 terminology.
- In the network without base station, the computers will communicate among each other as shown in Fig. 3.22.2(b). This mode is also called as Ad hoc networking.

Frequency :

- The frequency of the radio waves being used as a medium is decided by taking into consideration the following factors :
 - Frequency band which is available world wide.
 - Range to be covered.
 - Battery life and power consumed by the device.
 - Computer mobility.
 - Users privacy should be maintained.
 - System should have enough bandwidth.
 - System should be economically viable.

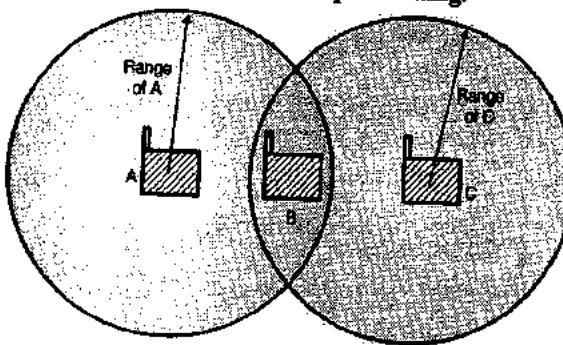
Compatibility with Ethernet :

- The 802.11 standard was designed such that it is compatible with the Ethernet (Wired LAN).
- It should be possible to send an IP packet over the wireless LAN the same way a wired computer sends an IP packet over Ethernet.

Differences between Ethernet and wireless LAN :

- The Ethernet (Wired LAN) and wireless LAN are compatible above datalink layer but they are different in the physical and data link layers. Some of the differences are as follows :
 - First is, that a computer in Ethernet first listens to the ether and transmits only if the Ether (medium) is idle. But this idea does not work in the wireless LAN at all. Refer Fig. 3.22.3.
 - The second is that a radio signal can be reflected off the solid objects. So the same signal can be received many times along

different paths. The interference resulting due to this is called as **multipath fading**.

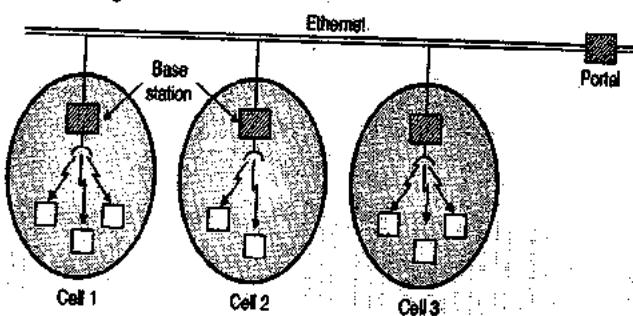


(G-372) Fig. 3.22.3 : Range of a single radio does not cover the entire system

- The third is that many softwares are not aware of the mobility. So the software used in Ethernets will not be useful in WLANs.
- If a notebook computer or a laptop is moved away from its base station which mounted on the ceiling and goes into the range of some other base station then the principle of handoff similar to cellular network needs to be used. This problem does not occur in Ethernet.

A multicell 802.11 network :

- To solve the hand off problem discussed earlier a multicell 802.11 network is designed. It consists of multiple cells and each cell has its base station connected to Ethernet as shown in Fig. 3.22.4.



(G-373) Fig. 3.22.4 : A multicell 802.11 network

- From outside the system looks like a single Ethernet. The connection between this system and the outside world is called as **portal**.
- The standard 802.11 a uses a wider frequency band and runs at a speed upto 54 Mbps. The 802.11 b standard uses the same frequency band but speed is upto 11 Mbps.
- WLANs have been widely accepted and airports, trains, hotels, shopping malls, universities are installing it.



3.23 Technical Issues :

- Here we discuss the technical issues related to design and engineering of WLANs. The differences between wireless and wired networks are also elaborated.

3.23.1 Difference between Wireless and Wired Transmission :

1. Address is not equivalent to physical location :

- In a wireless network, the address refers to a particular station. But it does not have any relation with the physical address of the device. This happens because the station need not be stationary at a particular physical address it can move.

2. Dynamic topology and restricted connectivity :

- As the mobile nodes can go out of reach of each other, the network connectivity is partial at times and not full as in case of the wired transmission.

3. Medium boundaries are not well defined :

- The exact range of a wireless signal cannot be accurately defined, because it is the function of various factors.
- Therefore it will never be possible to precisely define the boundaries or range of the medium.

4. Medium is prone to errors :

- In a wireless network, transmissions by a node are affected by simultaneous transmissions taking place from the neighbouring nodes, that are located in a close vicinity.
- Hence the error rates are high in the wireless communication as compared to those in the wired one.
- The bit error rate (typical) of a wireless channel is 10^{-4} while that of a fiber optic cable is 10^{-9} . This is a huge difference.

Conclusion :

- The four factors considered so far indicates that it is necessary to build a reliable network on top of an inherently unreliable wireless channel.
- This can be achieved in practice by using reliable MAC layer protocols.

3.23.2 Use of WLANs :

- Due to flexibility and possibility to configure in a variety of topologies, WLANs can be used in a number of varied applications. Some of them are as follows :
 1. For accessing the Internet, checking E-mails and receive/send instant messages when the user is moving.
 2. WLANs can set up networks in the locations affected by earthquakes or other disasters where no suitable infrastructure is available and wired networks have been destroyed.
 3. In places of historic importance, where wiring may not be permitted, the WLAN can be used easily and effectively.

3.24 Design Goals :

- Some of the important goals that should be achieved while designing WLANs are as follows :

1. Operational simplicity.
2. Power efficient operation.
3. Licence free operation.
4. Tolerance to interference.
5. Global usability.
6. Security.
7. Safety requirements.
8. QoS requirements.
9. Compatibility.
10. Bandwidth.
11. Mobility.
12. Reliability.
13. Scalability.
14. Ease of installation.

1. Simplicity of operation :

- A WLAN should have features which will enable a mobile user to quickly set up and access network services. The access should be easy and efficient as well.

2. Power efficient operation :

- The mobile devices operate on battery hence their operation is power constrained one.
- Hence the WLANs also should operate on minimum amount of power. The design of WLAN should include the power saving features with the necessary technology and protocols.

Licence free operation :

- The wireless access licence fee is an important factor which determines the cost of wireless access for the spectrum in which WLAN is operating.
- This cost should be as low as possible. Hence the design should consider using that portion of the spectrum (e.g. ISM band) which does not need any official licensing.

4. Tolerance to interference :

- There is a significant level of interference present in the entire the radio spectrum.
- The design of WLAN should be such that it should be able to operate satisfactorily even in the presence of this interference.
- This can be achieved by selecting an appropriate technology and protocols for the WLAN.

5. Global usability :

- By selecting the technology and operating frequency spectrum and by taking into account the existing spectrum restrictions, in various countries across the world, we can make a WLAN which can used globally.

6. Security :

- Due to the inherent broadband nature of wireless medium, special features should be included in the design of WLAN to provide adequate security.

7. Safety requirements :

- The safety requirements that should be followed by a WLAN can be classified as follows :
 - Interference to medical and other instrumental devices.
 - Increased power level of transmitter which can result in health hazards.
- WLAN design should be such that the transmitter power levels are restricted below the safe limits.

8. QoS requirements :

- WLAN should be designed to support a wide variety of traffic including the multimedia traffic.

9. Compatibility with other technologies and applications :

- Different wired and wireless LANs should be able to interact with each other.

- In addition, the interoperability with existing WAN protocols such as TCP/IP also is essential.

10. Mobility :

Wireless networks provide mobility to its users. They provide access to Internet and contact with the other users without using any wires.

11. Installation :

Installing a wireless network is simple. It eliminates the need of pulling connecting wires.

12. Reliability :

- In wireless systems, the EM waves are used to carry the information. But these waves undergo fading (loss of signals) due to various reasons.
- This will lead to reduced reliability. So some minimum level of reliability should be ensured.

13. Scalability :

- Wireless systems can be configured in different types of topologies depending on need of applications.
- It is possible to change the configuration easily right from peer to peer which is suitable for small networks to large infrastructural network used for large areas.

3.25 Network Architecture :**Classification of WLANs :**

- We can classify the WLANs broadly into two types :
 - Infrastructure networks
 - Ad-hoc LANs.

3.25.1 Infrastructure Networks :

- These WLANs contain special nodes called access points (APs) via existing networks.
- APs can interact with wireless nodes as well as wired networks. The other wireless nodes known as mobile stations (STAs) communicate via APs. The APs can also work as bridges with other networks.

3.25.2 Ad-hoc LANs :

SPPU Dec. 13

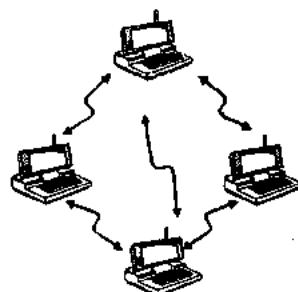
University Questions

Q.1 What are design principles of Ad-hoc routing protocols ? (Dec. 13, 8 Marks)

- These WLANs do not have any fixed architecture. They can be set up at any place. It is a



- peer-to-peer network without any centralized server.
- The ad-hoc networking scheme is as shown in Fig. 3.25.1.
- The Ad Hoc LAN is set up temporarily to meet some immediate requirements. Such as a group of people with laptops conferencing with each other in a room.
- The difference between the nomadic access and ad-hoc networking is evident from Fig. 3.25.1.
- As seen from Fig. 3.25.1 the ad-hoc LAN does not have any infrastructure.
- It is just a collection of few stations within range of each other dynamically configuring themselves into a temporary network.



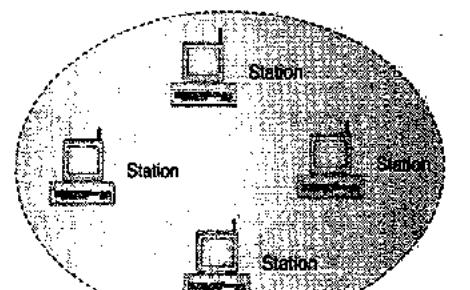
(G-376) Fig. 3.25.1 : Ad hoc networking

3.26 Components in a Typical IEEE 802.11 Network :

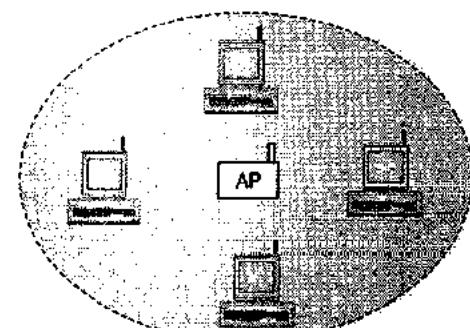
- IEEE 802.11 is the most popular WLAN standard. It defines the specifications for the physical and MAC layers.
- IEEE 802.11 defines two types of services :
 - Basic Service Set (BSS)
 - Extended Service Set (ESS)

3.26.1 Basic Service Set (BSS) :

- As per IEEE 802.11 the BSS has been defined as the basic building block of wireless LAN.
- A BSS consists of stationary or moving wireless stations and a central base station which is optional called as the access point (AP).
- Thus a BSS can be either without AP or with AP as shown in Figs. 3.26.1(a) and (b).
- The BSS without AP cannot send data to another BSS. So no data exchange can take place outside that BSS hence it is known as a stand-alone network or ad hoc architecture. However all the stations inside a BSS can exchange data among themselves.



(a) BSS Without AP

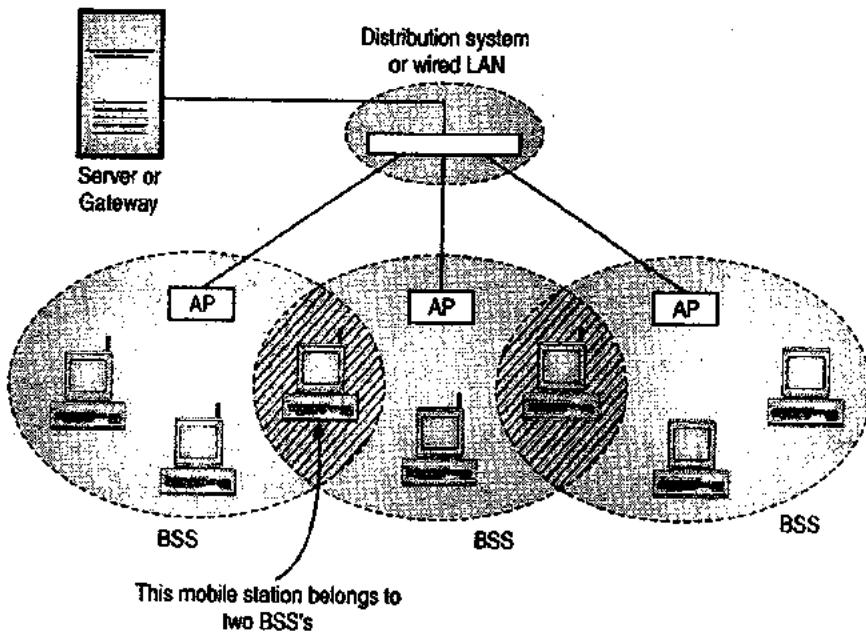


(b) BSS With an AP

(G-380)Fig. 3.26.1 : Types of BSS

Extended Service Set (ESS) :

- An Extended Service Set (ESS) consists of multiple BSSs with APs. The BSSs in this system are connected to each other via a distribution system or a wired LAN as shown in Fig. 3.26.2.
- The APs are connected to each other via the distribution system as shown. The distribution system can be any type of LAN such as Ethernet.
- The ESS contains two types of stations :
 - Mobile stations which can move and change location
 - Stationary or non-moving stations.
- Out of these, the non-moving stations are the APs which are a part of the wired LAN. Whereas the mobile stations are those contained in the BSS. Fig. 3.26.2 shows the structure of an ESS.
- The BSSs are connected to each other to form a network called **infrastructure network**. In such networks the stations close to each other can communicate without taking help of AP.
- But if two stations located in two different BSS wish to communicate with each other, than they have to do so through APs.
- This type of communication is very similar to that in the cellular communication. The BSS acts as a cell and AP as base station.
- As shown in Fig. 3.26.2 it is possible that a mobile station can belong to more than one BSSs simultaneously.



(G-381) Fig. 3.26.2 : ESS

3.26.2 Types of Stations in ESS :

- Three types of stations are defined by IEEE 802.11 depending on their mobility in the wireless LAN as :
 1. No transition
 2. BSS transition
 3. ESS transition

1. No transition mobility :

It is defined as a station which is not-moving at all (stationary) or moving inside a BSS only.

2. BSS transition mobility :

A station having BSS transition mobility is the one which can move from one BSS to the other BSS but does not move outside one ESS.

3. ESS transition mobility :

A station having ESS transition mobility is the one which can move from one ESS to any other ESS, But IEEE 802.11 does not guarantee a continuous communication when the station is moving.

3.27 Services Offered by a Typical IEEE 802.11 Network :

- The services offered by a typical IEEE 802.11 network can be divided into two categories :
 1. AP (access point) services.
 2. STA (mobile station) services.

3.27.1 AP Services :

- The AP services provided by the DS are as follows :

1. Association :

The identity and address of an STA should be known to AP before STA starts transmitting or receiving on WLAN. This process is done during association. AP then uses this information to facilitate routing of frames.

2. Re-association :

This service is used to transfer an established association from one AP to the other. This will allow STAs to move from one BSS to the other.

3. Disassociation :

It is the notification issued by the STA or AP when an existing association is terminated. Disassociation is done when nodes leave the BSS or when they shut down.

4. Distribution :

This service is used for routing frames. For destinations in the same BSS, the frames are transmitted directly to the destination. Otherwise they are sent via DS.

5. Integration :

This service is used in order to send frames through non IEEE 802.11 networks. Such networks can have different addressing schemes or frame formats.

3.27.2 STA Services :

Following are the STA services that are provided by every station including APs :



1. Authentication :

This is done in order to establish the identity of stations to each other. Different schemes of authentication ranging from simple handshake to public key encryption are used.

2. De-authentication :

This service is used when the existing authentication is to be terminated.

3. Privacy :

The messages are encrypted using the WEP algorithm to improve the privacy.

4. Data delivery :

IEEE 802.11 naturally provides a way to transmit and receive data, but the transmission is not completely reliable like Ethernet.

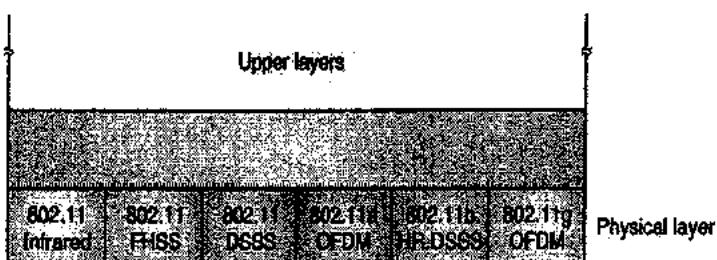
3.28 IEEE 802.11 Standard :

- The 802.11 is the prominent standard for WLANs. It has been adopted by most vendors. A later version of this standard is 802.11b which is commonly known as Wi-Fi (Wireless fidelity).
- The IEEE 802.11 standard deals with the physical and MAC layers in WLANs. It was introduced in 1997.

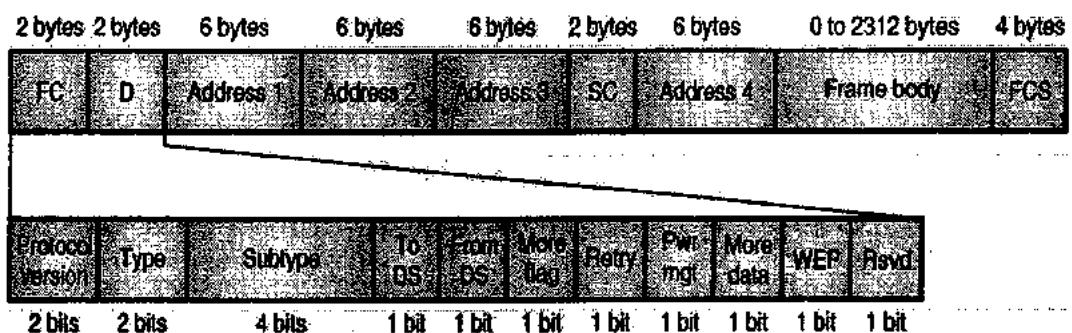
- Under the IEEE 802.11, MTs can operate in two different modes :
 - Infrastructure mode.
 - Ad-hoc mode.
- In the infrastructure mode, MTs can communicate with one or more APs whereas in the ad-hoc mode they can directly communicate with each other without an AP.

3.29 Physical Layer :

- IEEE 802.11 has defined the specification for converting bits to a signal in the physical layer. One of them is in the infra-red frequency spectrum and the other five specifications are in RF range as shown in the partial 802.11 protocol stack of Fig. 3.29.1.
- The five specifications in RF range are :
 - FHSS - Frequency Hopping Spread Spectrum (802.11).
 - DSSS - Direct Sequence Spread Spectrum (802.11)
 - OFDM - Orthogonal Frequency Division (802.11 a)
 - HR-DSS-High Rate-DSSS (802.11 b).
 - OFDM (802.11 g)



(G-382) Fig. 3.29.1 : Part of 802.11 protocol stack



(G-1916) Fig. 3.29.2 : Frame format

3.29.1 802.11 Frame Format :

SPPU : May 16

University Questions**Q.1 Explain 802.11 wireless frame format in detail.**

(May 16, 8 Marks)

- The MAC layer frame format for 802.11 wireless LAN is as shown in Fig. 3.29.2.
- This MAC layer frame consists of nine fields. They are as follows :
 - Frame control FC :** It is a 2 byte long field which defines the type of frame and some control information. As shown in Fig. 3.29.2, there are many subfields of FC. They are listed in Table 3.29.1.

Table 3.29.1 : Subfields in FC field

Field	Explanation
Version	Current version is 0
Type	Type of information : management (00), control (01) or data (10)
Subtype	Subtype of each type
ToDS	-
FromDS	-
More flag	If equal to 1, means more fragments
Retry	If equal to 1, means retransmitted frame
Pwr mgt	If equal to 1, means station is in power management mode
More data	If equal to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

- D (Duration ID) :** This is a 2 byte long which in all types of frame except one defines the duration of transmission. In one control frame it defines the frame ID.
- Addresses :** There are four address fields (Address 1 through address 4) and each field is 6 byte long. The contents of ToDS and FromDS fields will decide the meaning of the four address fields.
- SC (Sequence Control) :** This is a two byte long field which defines the sequence number of the frame being used in flow control.
- Frame body :** This is a variable length field. Its length varies between 0 and 2312 bytes. Its information contents depend on the type and the subtype defined in the FC field.

- FCS :** This is a 4 byte long field. It contains a CRC-32 error detection sequence.

3.29.2 IEEE 802.11 FHSS :

SPPU : May 15

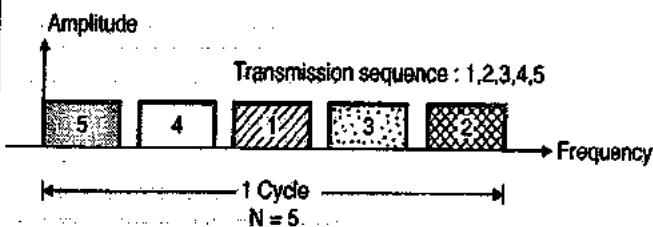
University Questions**Q.1 Explain all versions of 802.11 standard and compare.**

(May 15, 8 Marks)

- The IEEE 802.11 describes a method called FHSS i.e. Frequency Hopping Spread Spectrum for conversion of bits into a signal.
- The frequency band used for this is 2.4 GHz ISM band.

Principle of FHSS :

- In FHSS, the sender sends one carrier frequency for a short period of time. Then hops to another carrier frequency and transmits it for the same amount of time.
- Then it hops again to a new carrier frequency and transmits it for the same duration and so on.
- In all there are N-such hoppings in one cycles as shown in Fig. 3.29.3. The cycle repeats itself after N-hoppings.
- The bandwidth of FHSS signal is equal to NB Hz where B is the bandwidth of the original signal that is being converted to FHSS signal.
- The techniques of spreading used in FHSS makes it difficult for an unauthorised person to understand the transmitted data.
- The frequency of allocated bands in FHSS is decided with mutual agreement between the sender and the receiver.
- The frequency band by FHSS is 2.4 GHz ISM (industrial, scientific and medical). This band is divided in 79 equal subbands of 1 MHz each.
- The hopping frequency is selected by a pseudorandom number generator.



(G-383) Fig. 3.29.3 : Principle of FHSS



- The modulation techniques used is FSK (Frequency Shift Keying) at 1 M band /sec. And the data rate is 1 or 2 Mbps.

3.29.3 IEEE 802.11 DSSS :

SPPU : May 15

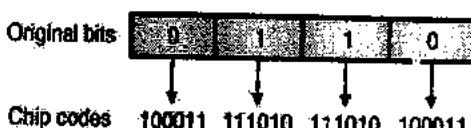
University Questions

- Q.1 Explain all versions of 802.11 standard and compare. (May 15, 8 Marks)**

IEEE 802.11 has defined the DSSS i.e. direct sequence spread spectrum technique in order to convert the bits into signal. The DSSS also uses the same frequency band as that of the FHSS i.e. 2.4 GHz. ISM band.

Principle of DSSS :

- In DSSS, each bit being sent by the sender is first converted into a group of bits called as the chip code.
- The time required to send each chip code should be equal to the time period of the original bit in order to avoid the buffering.
- Let N represent the number of bits in each chip code. Then the data rate of DSSS would be equal to N times the data rate of the original signal.
- Fig. 3.29.4 demonstrates the principle of DSSS.
- DSSS even though similar to CDMA is not a multiple access method. The bit sequence used in DSSS uses the entire frequency band of 2.4 GHz (ISM band).
- DSSS uses the BPSK (Binary PSK) or QPSK as its modulation techniques.



Bit	Chip code
0	100011
1	111010

(G-38) Fig. 3.29.4 : Principle of DSSS

3.29.4 IEEE 802.11 a OFDM :

SPPU : May 15

University Questions

- Q.1 Explain all versions of 802.11 standard and compare. (May 15, 8 Marks)**

- OFDM stands for orthogonal frequency division multiplexing. It is used by IEEE 802.11 a as the signal conversion technique.

Principle of OFDM :

- The basic principle of OFDM is same as that of FDM. But the major difference between them is that in OFDM all the frequency sub-bands are used by one source at a given time.
- OFDM uses the 5 GHz ISM band for its operation. This band is subdivided into 52 sub-bands.
- Out of these 52 sub-bands, 48 sub-bands are used for sending 48 groups of bits at a time and the remaining 4 sub-bands are used for sending the control information.
- These sub-bands can be used randomly in order to increase the security of transmitted data.
- The type of modulation used by OFDM is BPSK and QAM (Quadrature Amplitude Modulation).

3.29.5 IEEE 802.11 b HR- DSSS :

SPPU : May 15

University Questions

- Q.1 Explain all versions of 802.11 standard and compare. (May 15, 8 Marks)**

- HR-DSSS is the short form for high rate (speed) direct sequence spread spectrum. IEEE 802.11 b uses HR-DSSS method for signal generation.
- It uses the frequency band of 2.4 GHz (ISM band).
- HR-DSSS is conceptually very similar to that of a DSSS techniques. The only difference is about the encoding method used.
- HR-DSSS uses a method called Complementary Code Keying (CCK) which encodes 4 or 8 bits of original data into one CCK symbol.
- The HR-DSSS needs to be backward compatible with DSSS. Hence HR-DSSS defines four data rates : 1,2,5.5 and 11 Mbps.
- The 1 and 2 Mbps data rates are allocated for the same type of modulation techniques as used for DSSS i.e. BPSK and QPSK.
- The modulation used for 5.5 Mbps is BPSK whereas the 11 Mbps data rate is assigned for QPSK type modulation.

3.29.6 IEEE 802.11g OFDM :

SPPU : May 15

University Questions

- Q.1 Explain all versions of 802.11 standard and compare. (May 15, 8 Marks)**

It is a new specification using OFDM. The frequency band used is 2.4 GHz ISM with a complex modulation technique used. It is possible to achieve data rate of upto 54 Mbps.

3.30 Basic MAC Layer Mechanisms :

- In this section, we will describe the MAC layer as specified by the IEEE 802.11 standard. The function of MAC layer is to attribute and statistically multiplex the transmission requests of various wireless stations operating in that area.
- Wireless transmissions are broadcast in nature and therefore it is necessary to resolve any contentions to access the shared channel. This is necessary to avoid collisions or at least minimize the number of collisions.
- Some other secondary functions of the MAC layer are as follows :
 - To offer support to roaming.
 - Support authentication.
 - To take care of power conservation.
- The basic services of the MAC layer are as follows :
 - The mandatory asynchronous data service.
 - The optional real time service.
- The asynchronous data service is for communication with the unicast packets as well as the multicast packets, whereas the real time service is supported only in the infrastructure based wireless networks.

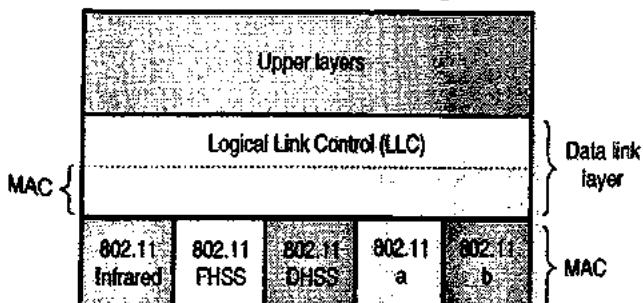
3.30.1 Distributed Foundation Wireless Medium Access Control (DFWMAC) :

SPPU : May 16

University Questions

Q. 1 Explain in detail MAC sublayer DCF (Distributed Coordination Function) used in wireless LAN.
(May 16, 6 Marks)

- The primary access method of IEEE 802.11 is by means of Distributed Co-ordinate Function (DCF). There is a second method called the Point Co-ordinate Function (PCF) which is used to provide the real time service.
- Fig. 3.30.1 shows a part of 802.11 protocol stack.



(G-386) Fig. 3.30.1 : Part of the 802.11 protocol stack

- There are five possible transmission techniques make it possible to send a MAC frame from one

station to another. They differ in the technology used and speeds available.

- The 802.11 faces the hidden station problem and the exposed station problem (discussed later). Hence it does not use the CSMA/CD as the MAC protocol.
- To deal with this problem, the 802.11 supports two modes of operation :
 - DCF (Distributed Co-ordination Function)
 - PCF (Point Co-ordination Function)
- The DCF does not use any kind of central control and PCF uses the base station to control all the activities in its cell.
- All implementations must support DCF but PCF is optional.
- When DCF is employed, 802.11 uses a protocol called CSMA/CA (CSMA with collision Avoidance).
- The other mode of CSMA/CA operation is based on MACAW and uses virtual channel sensing.

3.30.2 Inter-Frame Spacing (IFS) :

- IFS is defined as the time interval between the transmission of two successive frames by any station.
- The four types of IFS are as follows :
 - SIFS
 - PIFS
 - DIFS
 - EIFS
- These are in the order of shortest to longest. (SIFS is the shortest and EIFS is the longest).
- They have different priority levels to access the medium. SIFS has the highest priority and EIFS has the lowest.
- The four types of IFS are defined as follows :

1. Short Interframe Spacing (SIFS) :

- SIFS is the shortest type of all IFS. It has the highest priority. It is defined for the short control messages such as acknowledgements for data packets and polling responses.
- If it is sensed that the channel is idle for a minimum time period of SIFS only then the sender can transmit his packet.

2. PCF Interframe Spacing (PIFS) :

- It is used for the real time service and defined as the waiting time whose value lies between SIFS and DIFS.



3. DCF Interframe Spacing (DIFS) :

- DIFS is used by the stations operating under DCF mode for transmitting their packets.

4. Extended Interframe Spacing (EIFS) :

- This type of IFS is the longest type of IFS and has the least priority, for accessing the medium.
- EIFS is used for the purpose of resynchronization.

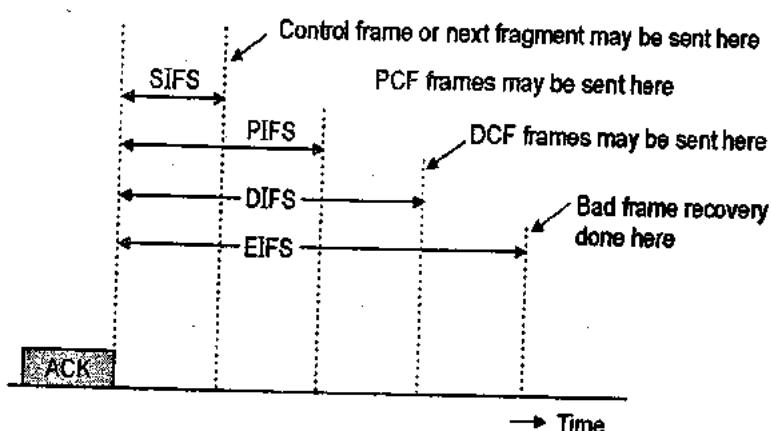
3.30.3 DCF and PCF in 802.11 :

- The PCF (Point Co-ordination Function) and DCF (Distributed Co-ordination Function) can exist simultaneously within one cell, which might seem impossible at the same time.
- But 802.11 provides a way to achieve this goal. It works by carefully defining the interframe time interval.
- After one station sending a frame a certain amount of dead time is required to be introduced before any station may send a frame.
- Four different intervals are defined as shown in Fig. 3.30.2 each for a special purpose.
- The shortest interval of all is SIFS (Short Interframe Spacing). It is used to allow the parties in a single dialog the chance to go first. During this period the receiver sends a CTS to respond to an RTS letting the receiver to send an ACK for a fragment or full data frame, and lets the sender of a fragment burst transmit the next fragment without having to send an RTS again.

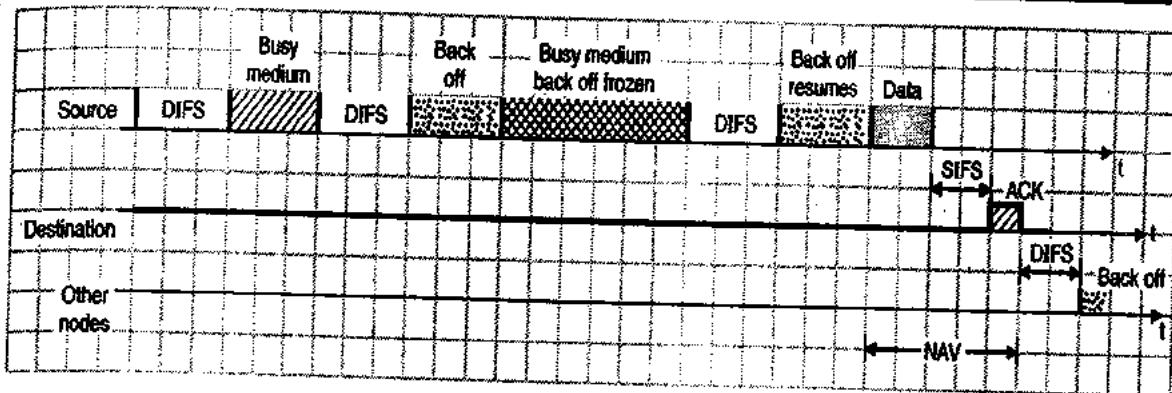
- Only one station is allowed to respond after a SIFS interval. If it is not able to make use of this chance, and a time PIFS (PCF InterFrame Spacing) elapses, then the base station may send a beacon frame or poll frame.
- This mechanism allows a station sending a data frame or a fragmented sequence to finish its frame with no one else interrupting. But it gives the base station a chance to grab the channel when the previous sender has finished its transmission.
- If the base station has nothing to say and the time interval DIFS (DCF Inter Frame Spacing) elapses then it is allowed for any station to attempt and acquire the channel to send a new frame. The usual contention rule is to be applied and the binary exponential backoff algorithm can be used in the event of a collision.
- The fourth time interval EIFS (Extended InterFrame Spacing) is used only by a station which has just received a bad or unknown frame to report the bad frame. This event has been given the lowest priority.

3.30.4 CSMA/CA Mechanism :

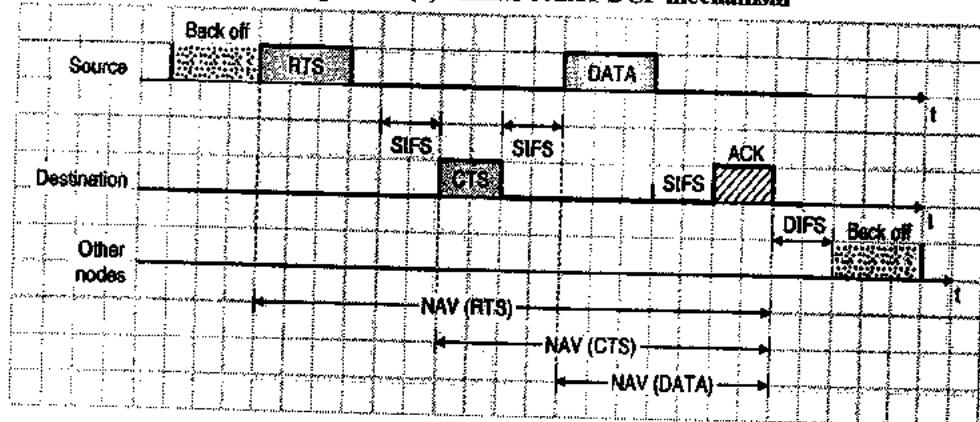
- The 802.11 WLANs use the CSMA/CA MAC layer mechanism for channel allocation. It is not possible to use CSMA/CD for WLANs because of the higher error rates existing in WLANs and also due to the fact that it is not always possible to detect collisions for the wireless medium.
- Hence the technique of Collision Avoidance (CA) is adopted for WLANs.



(G-387) Fig. 3.30.2 : Interframe spacing in 802.11



(G-1525) Fig. 3.30.3(a) : IEEE 802.11 DCF mechanism



(G-1526) Fig. 3.30.3(b) : RTS-CTS mechanism

3.30.5 The Medium Access Mechanism :

- Fig. 3.30.3(a) shows the basic channel access mechanism of IEEE 802.11. If the medium is found idle during the DIFS then the node accesses the medium for transmission.
- If the medium is busy, the node will back off. In this situation, the station defers channel access by a random amount chosen within a Contention Window (CW). The value of CW will vary between two extreme values CW_{min} and CW_{max} .
- As soon as the back-off counter expires (reaches zero), the station can access medium.
- During the back off time itself if a node detects that the channel is busy then it freezes the back off counter and the process will restart only after the channel becomes idle for a period of DIFS.

Acknowledgements :

- Acknowledgements (ACKs) should be sent for data packets so as to ensure their correct delivery.
- If the packets are unicast then the receiver receives data, waits for SIFS and sends an ACK signal as shown in Fig. 3.30.3(a). Other stations will have to

wait for DIFS plus their back-off time as shown in Fig. 3.30.3(a).

- ACK ensures that correct data is received by using the CRC (Cyclic redundancy checksum) technique. If ACK is not received, the sender will retransmit the data.
- However the number of retransmissions is limited and after a pre-decided number of retransmissions, the sender will report failure to the higher layers.

3.30.6 RTS-CTS Mechanism : SPPU : May 16

University Questions

- Q. 1** What is the purpose of NAV ? Explain

(May 16, 4 Marks)

- One of the main problems in wireless networks is the hidden station problem (discussed later). This problem can be solved by using RTS-CTS mechanism.
- Refer Fig. 3.30.3(b) to understand the working of RTS-CTS mechanism.
- As shown in Fig. 3.30.3(b), the sender sends a request to send (RTS) packet to the receiver. This short frame 30 bytes size contains the length of the data frame that will be transmitted. This packet (RTS) is received by all the stations that can hear the sender.



- Every station that receives the RTS packet will send the Network Allocation Vector (NAV) accordingly. This NAV of a station specifies the earliest time at which the station is allowed to attempt transmission.
- The intended receiver waits for SIFS and sends a clear to send (CTS) packet indicating that it is ready to receive data. (See Fig. 3.30.3(b)). The CTS frame contains the data length copied from the RTS frame. All stations receiving the CTS packet will set their NAVs.
- These stations are within the range of the receiver.
- Note an important point here that the stations receiving CTS may be different from those which received the RTS packet.
- Once the RTS packet has been sent and CTS packet has been received, all the nodes near sender and receiver understand that the medium has been reserved for one sender exclusively.
- The sender then waits for SIFS and starts data packet transmission. The receiver receives the data packet, waits for another SIFS and send ACK as shown in Fig. 3.30.3(b).
- As soon as the transmission is complete the NAV in each node will mark the medium as free and the process can repeat again.
- The collision can take place only at the beginning i.e. when RTS and CTS packets are being sent.
- Nodes which listen to the RTS or CTS packets will refrain from transmission thereby avoiding any collisions.

3.31 Problems in Wireless LAN :

SPPU : May 06, May 07, Dec. 07

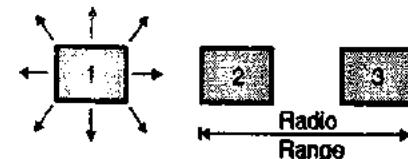
University Questions

- Q. 1** Explain hidden station problem and exposed station problem in wireless LAN. (May 06, 9 Marks)
- Q. 2** What are the various issues in wireless LAN ? (May 07, 4 Marks)
- Q. 3** Write short note on : Hidden Station Problem. (Dec. 07, 6 Marks)

If we try to use CSMA (the access method used for wired LANs) for the wireless LAN, then it uses the principle of simply listening to other transmission and only transmit if no one else is transmitting. But there are two problems in using CSMA. They are hidden station problem and exposed station problem.

Hidden station problem :

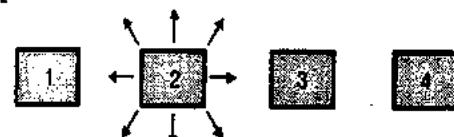
- Refer Fig. 3.31.1 where station-1 is transmitting to station 2.
- Now if station-3 checks the medium to see if anyone is transmitting, it will not hear station-1 because it is out of range. So station-3 will come to a wrong conclusion that no one is transmitting and so it can start transmitting to station-2.
- If station-3 starts transmitting, it will create an interference at station-2 and will wipe out the frames from station-1.
- This problem in which a station is not able to detect an already transmitting other station which is too far away is called as the **hidden station problem**.



(G-377)Fig. 3.31.1 : Hidden station problem

Exposed station problem :

- Now consider Fig. 3.31.2 in which station-2 is transmitting to station-1. If station-3 checks the medium, then since station-2 comes in its range, station-3 will understand that the transmission going on.
- So it will falsely decide that it should not transmit to station-4.
- Note that the station-3 can transmit to station-4, even when 2 is transmitting.
- This problem is called as the **exposed station problem**.



(G-378)Fig. 3.31.2 : Exposed station problem

3.32 Comparison of Ethernet and Wireless Network :

SPPU : Dec. 07

University Questions

- Q. 1** Give the similarities and differences between wired and wireless networks. (Dec. 07, 8 Marks)

St. No.	Ethernet	Wireless Network
1.	IEEE standard 802.3	IEEE standard 802.11
2.	Communication medium is coaxial cable	Infrared or radio frequencies act as medium

	Ethernet	Wireless Network
3.	Spread spectrum is not used.	Spread spectrum is used
4.	Uses MAC	Uses two MAC sublayers
5.	Uses CDMA/CD	Uses CSMA/CA
6.	Efficiency is high	Efficiency is low
7.	Addressing is simpler	Addressing is complicated
8.	Large range	Short range.

3.33 Wireless LAN Protocols :

SPPU : May 06, Dec. 06, Dec. 07, Dec. 09, May 13

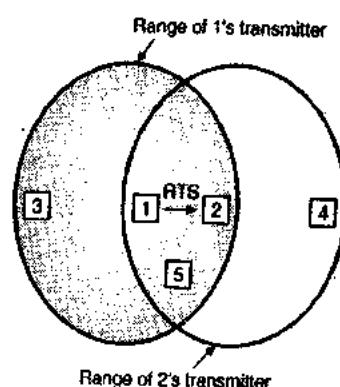
University Questions

- Q. 1 Explain wireless LAN ? (May 06, 4 Marks)
- Q. 2 Write a short note on : Wireless LAN protocol (Dec. 06, 6 Marks)
- Q. 3 Explain the working of MACA protocol. Is this protocol better than CSMA/CD. Justify your answer. (Dec. 07, 10 Marks)
- Q. 4 Write a short notes on : Wireless LAN protocol. (Dec. 09, 6 Marks)
- Q. 5 Explain working MACA and MACAW protocols with neat diagram. (May 13, 8 Marks)

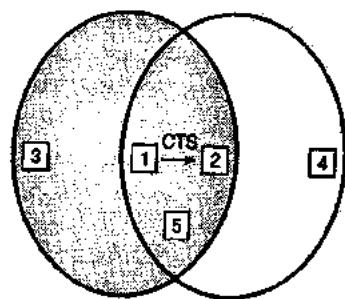
- A system of portable computers that communicate by using radio frequency (RF) or infrared waves are regarded as a wireless LAN.
- The wireless LAN require special MAC sublayer protocols. Multiple Access with Collision Avoidance (MACA) is the protocol designed for wireless LANs. It is used as the basis for the IEEE 802.11 wireless LAN standard.
- In this protocol the sender stimulates the receiver to send a short frame, so stations nearby can detect this transmission and avoid transmitting themselves for the duration when data is being transmitted.
- The MACA protocol is shown in Fig. 3.33.1 consider station 1 wants to send data to station 2. Station 1 starts by sending a request to send (RTS) frame to station 2.
- This short frame consisting of 30 bytes contains the length of the data frame that will be transmitted.
- Then station 2 replies with a clear to send (CTS) frame. The CTS frame contains the data length

copied from the RTS frame. When station 1 receives the CTS frame it starts transmission.

- As shown in the Fig. 3.33.1 station 3 is within range of 1 but not within range of 2. Therefore it hears the RTS from 1 but not the CTS from 2.
- As long as it does not interfere with the CTS, it is free to transmit while the data frame is being sent. In contrast station 4 is within the range of 2 but not 1.
- It does not hear the RTS but does hear the CTS. On hearing CTS it does not send anything until that frame is expected to be finished.
- The station 5 hears both the RTS and CTS control messages and remains silent until the data frame is complete.
- Despite the above precaution it is possible that both stations 2 and 3 may send a RTS to station 1. These will collide and will be lost.
- In this case if station 1 does not receive a CTS within a specified time, it waits for a random amount of time and then again transmits the RTS command.
- The MACA was latter fine tuned for improvement in performance and renamed as MACAW (MACA for wireless).
- In MACAW, an ACK frame is introduced after each successful data frame.
- Carrier sensing (CSMA) is also added and the back off algorithm is run separately for each data stream rather than for each station.



(a) 1 sending an RTS to 2



(b) 2 responds with a CTS to 1

(G-379) Fig. 3.33.1 : The multiple access with collision avoidance



3.34 Advantages of WLAN :

1. WLAN is cheaper than wired LAN, because wires are not required.
2. WLAN can be laid down where it is difficult to run cables e.g. Historical buildings.
3. It is possible to form WLAN using laptops.
4. Any standard Wi-Fi device can work anywhere in the world.
5. WPA2 protocol used for Wi-Fi is secure protocol so WLANs are safe.

3.34.1 Limitations of WLAN :

1. Spectrum assignment and operational conditions are not same worldwide.
2. Radiated power is limited to 100 mW. So the range will be limited.
3. Wi-Fi networks have a limited range typically 35 m or 120 ft indoor and 100 m or 300 ft outdoor.
4. There are data security risks. Wi-Fi networks are not protected thoroughly.
5. Wi-Fi connections can be easily disrupted.

3.35 Bluetooth (WPAN) :

- WLANs can be preferred for connecting infrastructure based services via a wireless carrier provider. But it does not allow the personal devices to communicate wirelessly among each other.
- Therefore a Personal Area Network (PAN) has been developed to fulfill this need.
- Bluetooth is the name given to a new technology which uses short-range radio links, that can replace the cable(s) connecting portable and/or fixed electronic devices.
- It is advantageous that it will allow the replacement of the many propriety cables that connect one device to another with one universal radio link.
- Its key features are robustness, low complexity, low power and low cost.
- Bluetooth has been designed to operate in noisy frequency environments. Therefore it uses a fast acknowledgement and frequency-hopping scheme to make the link robust.
- Bluetooth radio modules operate in the unlicensed ISM band at 2.4 GHz, and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet.
- Compared with other systems in the same frequency band, the Bluetooth radio hops faster and uses shorter wavelengths.

- Thus Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, computers, printers, cameras, etc.
- A Bluetooth LAN is an Ad hoc network. It is possible to connect the Bluetooth LAN to the Internet.
- This technology is implemented using the IEEE 802.15 standard.
- The power consumption of Bluetooth technology is low and it offers a range of operation upto ten meters. These features have made it find many applications.

3.35.1 Applications of Bluetooth Technology :

- Some of the applications of Bluetooth technology are as follows :
 1. Ad-hoc network of laptops for interactive conference.
 2. Cordless computer.
 3. Connecting a digital camera wirelessly to a mobile phone.
 4. Three in one phone where the same phone functions as an intercom, a cordless phone and a mobile phone.

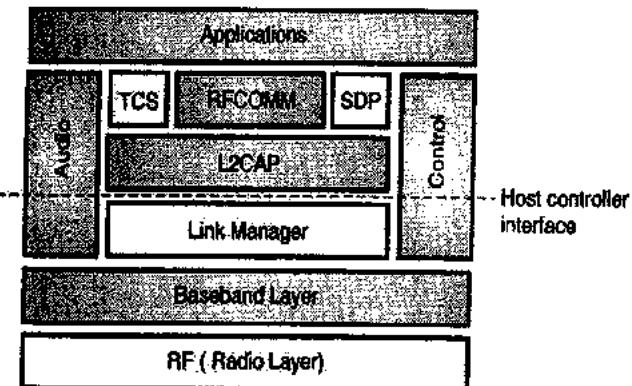
3.35.2 Bluetooth Devices :

- Every Bluetooth device consists of a built in short range radio transmitter. The current data rate is 1 Mbps and the bandwidth is 2.4 GHz.
 - So an interface between the IEEE 802.11 wireless LAN and Bluetooth LAN is possible.
 - The Bluetooth specification standard defines a short-range (10-meter) radio link.
 - The devices carrying Bluetooth-enabled chips can easily transfer data at a rate of about 1 Mbps (Megabits per second) within 10 meters (33 feet) of range through walls, clothing and luggage bags.
 - The interaction between devices occurs by itself without direct human intervention whenever they are within each other's range. In this process, the software technology embedded in the Bluetooth transceiver chip triggers an automatic connection to deliver and accept the data flow.
- Since Bluetooth is of short range with limited speed and low-power technology. It is less attractive to corporate wireless local area networks that are generally powered with the 802.11 wireless LAN technologies.

- Each Bluetooth-enabled device contains a 1.5-inch square transceiver chip operating in the ISM (Industrial, Scientific, and Medical) radio frequency band of 2.40 GHz to 2.48 GHz.
- This frequency is generally available worldwide for free without any licensing restrictions. The ISM band is divided into 79 channels with each carrying a bandwidth of 1 MHz.

3.36 Bluetooth Specifications :

- The Bluetooth specifications are divided into two parts :
 1. Core specifications
 2. Profiles specifications.
- The core specifications provides a common data link and physical layer to application protocols. It also maximizes the re-usability of existing higher layer protocols.
- The profile specification are used for classifying the Bluetooth applications into thirteen different types.
- Fig. 3.36.1 shows the protocol stack of Bluetooth technology. It is partitioned logically into three layers : transport protocol group, the middleware protocol group and the application group.



(G-1528) Fig. 3.36.1 : Bluetooth protocol stack

1. Transport protocol group :

- This group consists of the radio layer, basebank layer, link manager layer, logical link control, adaptation layer and host controller interface.

2. The middleware protocol group :

- This group consists of RFCOMM, SDP and IrDA.

3. The applications group :

- This group consists of the applications (profiles) that use Bluetooth wireless links. Some of the applications are modem dialer and web-browsing client.

3.37 Transport Protocol Group :

- The Bluetooth protocol stock performs the following functions :
 1. To locate devices.
 2. To connect other devices.
 3. To exchange data.
- The transport protocol group has got protocols which allow Bluetooth devices to locate each other and then create, configure and manage wireless connections between the located devices.
- We will study different protocols in this group in the following subsections.

3.37.1 Radio (Physical Layer) :

- The Bluetooth Radio (layer) is the lowest defined layer of the Bluetooth specification. It defines the requirements of the Bluetooth transceiver device operating in the 2.4 GHz ISM band. This band is divided into 79 channels of 1 MHz each.
- The type of frequency modulation used is GFSK. It is suitable to work with the 64 kbps voice channels and asynchronous data channels. The peak rate for data channels is 1 Mbps. The data channels can be symmetrical or asymmetrical.
- The Bluetooth transceiver uses FHSS (Frequency Hop Spread Spectrum). Each channel is 1 MHz wide. The number of channels is $m = 79$ in most of the countries. Therefore the frequency band used is from 2.4 GHz to 2.48 GHz.

3.37.2 Physical Links in Bluetooth :

- Two types of links created between the primary and secondary are as follows :
 1. SCO
 2. ACL
- 1. **SCO link :**
 - Its long form is Synchronous Connection Oriented link and it is used for those applications in which avoiding latency (delay in data delivery) is more important than the integrity (error free data delivery).
 - In any SCO link, specific slots are reserved at regular intervals.



- If a packet gets damaged, it is never retransmitted. The secondary can create up to three SCO links with the primary with a capacity of upto 64 kbps on each link.
 - The application of SCO link is the real-time audio applications.
- 2. ACL link :**

- The long form of ACL is Asynchronous Connectionless Link. It is used for those applications in which data integrity is more important than latency.
- If the payload capsule containing data in a packet is damaged then it is retransmitted.
- ACL can achieve a maximum rate of 721 kbps.

3.37.3 Baseband Layer :

- The baseband is the physical layer of the Bluetooth. It manages physical channels and links in addition to the other services like error correction, data whitening, hop selection and Bluetooth security.
- The baseband layer is placed on top of the Bluetooth radio layer in the bluetooth stack. The baseband protocol is implemented as a link controller, which works with the link manager and carries out the link level routines like link connection and power control.
- Some other functions managed by the base band layer are : Asynchronous and synchronous links, handles packets paging and inquiry because all this is necessary to access and inquire Bluetooth devices in the area.
- The baseband transceiver applies a Time Division Duplex (TDD) scheme. (alternate transmits and receives).

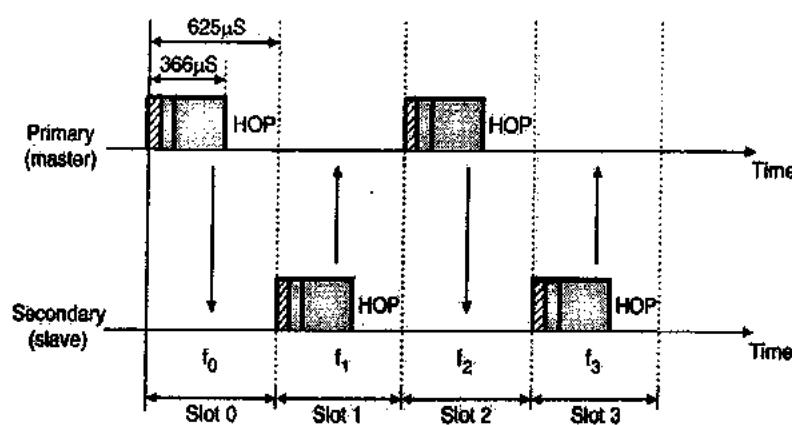
- Therefore apart from different hopping frequency (frequency division), the time is also divided into slots.
- Bluetooth communication takes place over the ad-hoc networks called as Piconets.

3.37.4 TDMA :

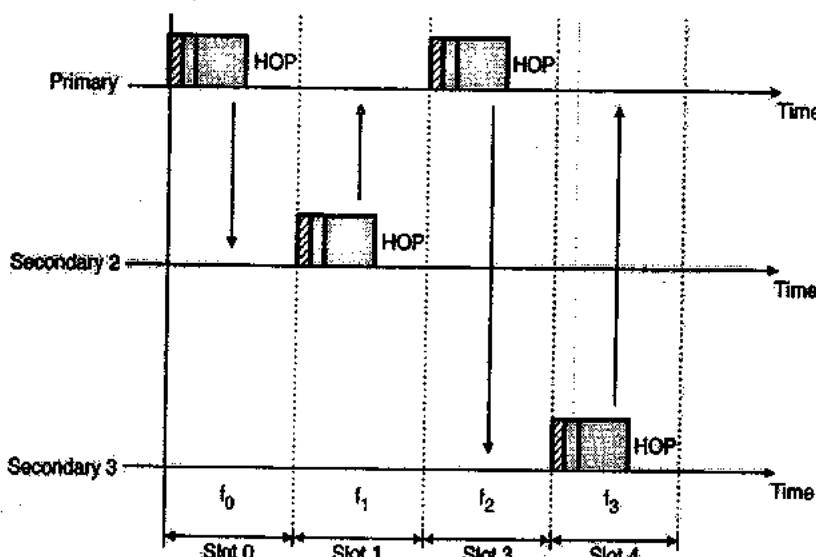
- Bluetooth uses a form of TDMA which is called as TDD-TDMA (time division duplex TDMA). TDD-TDMA is half duplex communication in which secondary and receiver will send and receive data, but they will not send and receive data at the same time.
- The communication in each direction uses different hops. This is similar to walkie-talkies using different carrier frequencies.

Single secondary communication :

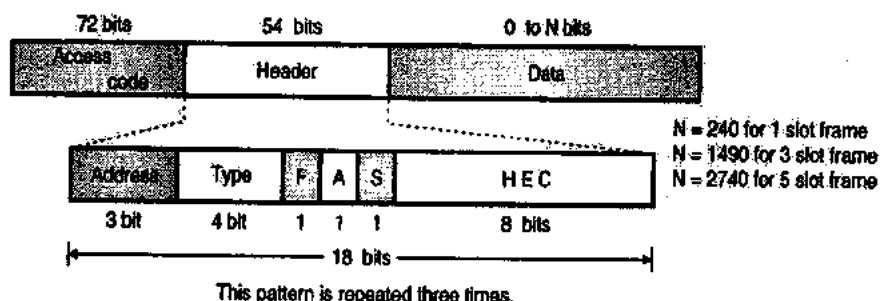
- TDMA operation is very simple, when piconet has only one secondary (slave). The time is divided into equal slots of $625 \mu\text{s}$ duration each. The master (primary) uses even numbered slots. i.e. 0, 2, 4, 6..... The secondary (slave) uses odd numbered slots i.e. 1, 3, 5, 7.....
- TDD-TDMA allows communication between primary and secondary to take place in half duplex mode.
- Single secondary communication has been illustrated in Fig. 3.37.1(a). It shows that during the slot 0, primary (master) will send and secondary will receive. During the slot 1, the secondary (slave) will send and primary will receive. The cycle is repeated as shown in Fig. 3.37.1(a).



(G-1411) Fig. 3.37.1(a) : Single secondary communication



(G-1412) Fig. 3.37.1(b) : Multiple secondary communication



(G-391) Fig. 3.37.2 : Frame format

Multiple secondary communication :

- In multiple secondary communication, piconet has more than one secondaries (slaves). In this type of communication also, primary uses even numbered slots but only that secondary will send in the next odd numbered slot for which the packet in the previous slot was addressed.
- All secondaries will listen to even numbered slots, but only one secondary sends in any odd numbered slot.
- Fig. 3.37.1(b) illustrates the multiple secondary communication.
- From Fig. 3.37.1(b) :
 - In slot 0, the primary will send frame to secondary 2.
 - In slot 1, only secondary 2 will send a frame to primary because the previous frame was addressed to secondary 2, at the same time other secondaries will remain silent.
 - In slot 2, the primary will send frame to secondary 3.
 - In slot 3, only secondary 3 will send frame to primary because previous frame was addressed to secondary 3, other secondaries will remain silent, this cycle is repeated.

- This access method is similar to poll or select operation with reservations. When primary will select secondary, it also polls it. The next time slot is reserved for the polled station which send its frame. If there is no frame to send by polled secondary, the channel is silent.

3.37.5 Frame Format in Baseband Layer (Bluetooth Frame Format) : SPPU : May 16

University Questions

- Q. 1 Explain Bluetooth frame format in detail.**

(May 16, 4 Marks)

- A frame in the baseband layer can be one of the three types :
 - One slot
 - Three slot
 - Five slot.
 - The frame format of the three frame types is shown in Fig. 3.37.2.
The description of important fields is as follows :
- 1. Access code :**
It is a 72 bits field which contains the synchronization bits. It also contains the identifier of the master so as to distinguish the frame of one piconet from another.



2. Header :

- It is a 54 bits field which contains an 18 bits pattern repeated three times. (see Fig. 3.37.2).
- Each such 18 bits pattern consists of the following fields.

Address : It is a three bit field. So it can define upto seven slaves (1 to 7). The 000 address is reserved for the broadcast communication between a master and the slaves. The other addresses from 001 to 111 define seven slaves.

Type : This is a four bit subfield used for defining the type of data, coming from the upper layers.

F : This bit is used for the flow control. F = 1 is an indication of buffer full, that means the device cannot receive more frames.

A : This bit is for acknowledgement. Since Bluetooth uses the stop-N-wait ARQ only 1 bit is sufficient to send an acknowledgement.

S : This bit is used to hold the sequence number.

HEC : This is an eight bit header error correction subfield. It contains the checksum for detection of errors in the 18 bit header section.

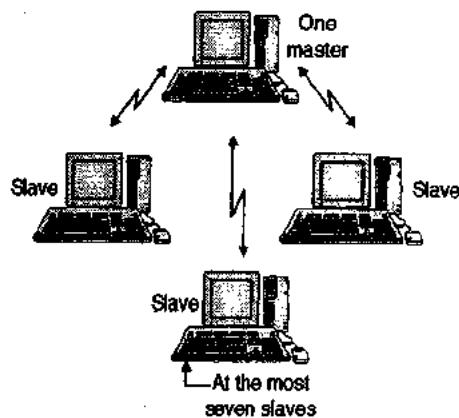
3. Data :

This subfield can be of variable length. Its length can vary from 0 to 2740 bits. It contains the data or control information obtained from the upper layers.

3.38 Piconets (Bluetooth Architecture) :

- Bluetooth defines two types of networks :
 1. Piconets and 2. Scatternets.
- The first type of Bluetooth network is called as a piconet or a small net. It can have at the most eight stations. One of them is called as a master and all others are called as slaves.
- All the slave stations are synchronised in all aspects with the master.
- A piconet can have only one master station. Fig. 3.38.1 shows a piconet. A master can also be called as a primary station and slaves are secondary station.

- The communication between a master and slaves can be one-to-one or one-to-many. Note that the communication takes place between the master and slaves but no direct communication takes place between the slaves.



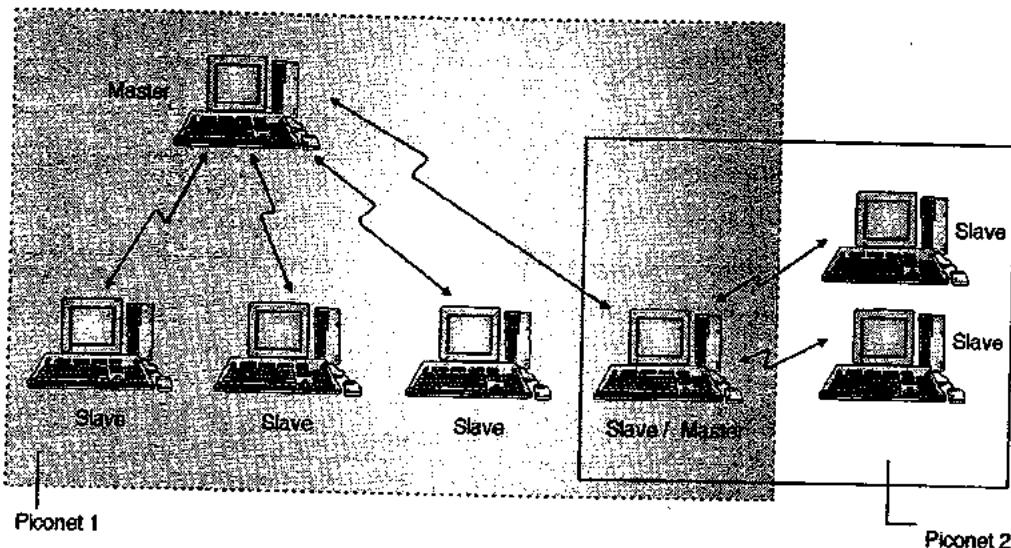
(G-38)Fig. 3.38.1 : A piconet

- The formation of a piconet is governed by two factors :

1. The address of each Bluetooth device.
 2. The clock associated with each device.
- Every device in a piconet has been assigned with a 48 bit address which is similar to an Ethernet address. The address field is divided into three parts and the Lower Address Part (LAP) is used for the purpose of piconet identification, error checking and security checks.
 - Every device has a 28-bit clock which is called as native clock. Its frequency is 3200 pulses per second i.e. once in 312.5 μS, because this is exactly twice the normal hopping rate of 1600 hops/second.
 - A piconet can have upto seven active slaves at any given instant of time. In order to identify a slave, each one is assigned a locally unique active member address AM-ADDR.
 - If a Bluetooth device is not associated with any piconet, then it is said to be in standby mode.

3.39 Scatternets (Bluetooth Architecture) and Issues :

- Many piconets may exist simultaneously in a given area and they may even overlap each other.
- A scatternet is obtained by combining piconets as shown in Fig. 3.39.1.



(G-389) Fig. 3.39.1 : Scatternet

- Fig. 3.39.1 shows a scatternet consisting of two piconets. A slave in the first piconet can act as a master in the second piconet.
- It will receive the messages from the master in the first piconet by acting as a slave and then delivers the message to the slaves in the second piconet as shown in Fig. 3.39.1. So the same device acts as a slave in the first piconet and as master in the second piconet.
- With increase in the number of piconets, the possibility of collision increases. This will result in degradation of performance.
- Therefore a device can participate in two or more piconets by means of the time sharing process. To do so it must use the associated master's address and proper clock offset.
- A Bluetooth device can act as a master in only one piconet but it can work as a slave in multiple piconets.
- One of the important issues in a scatternet is that the utilization of bandwidth is not optimal. This happens because a device changes its role and takes part in different piconets.
- Another important issue is the timing that a device would be missing when it participates in more than one piconets.
- If a master of one piconet temporarily becomes slave in some other piconet then it will be missing from its own piconet for that much time. This reduces the quality of the Bluetooth link.

3.40 Link Manager Protocol (LMP) :

- The task of the Link Manager Protocol (LMP) is to set and maintain the properties of a Bluetooth link.
- The two main functions of this layer are :
 - Power management.
 - Security management.

- It also provides the QoS support by controlling parameters like jitter and delay.
- It is possible to change the role of a master to slave and vice versa in a piconet by exchange of LMP packets.

3.40.1 Power Management :

- A Bluetooth device can be in one of the possible four modes, during its connection state. The four possible modes of operation are :
 - Active mode
 - Sniff mode
 - Hold mode
 - Park mode

1. Active mode :

In this mode, the Bluetooth device participates actively in the piconet. Various techniques of optimizations are provided for power saving. The master polls active slaves in order to initiate transmissions.

2. Sniff mode :

This is a low power mode. In this mode the listening activity of slave is reduced. The slave is told to enter into the sniff mode via LMP in the master.

3. Hold mode :

In this mode the slave temporarily stops supporting ACL packets on the channel. Instead it is made capable to perform some other functions like scanning, paging, inquiring or attending other piconets.

4. Park mode :

- This is a very low power mode. The slave does not remain active but goes into parking



- mode. To achieve this the slave will surrender its active member address and it is given an 8-bit parking member address. The slave remains synchronized in the channel.
- If a message is to be sent to such a slave then it is sent over broadcast channel with an active member address of all zeros.
- The park mode not only saves power but it also allows the master to have more than seven slaves in its piconet.

3.40.2 Bluetooth Security :

- In order to have secured communication in Bluetooth, the devices may be authenticated and links may be encrypted.
- The challenge-response mechanism is used for authenticating a device. This mechanism is based on the commonly shared secret key generator through a Personal Identification Number (PIN).
- At the beginning of authentication, the transmission of an LMP challenge packet takes place and the process ends with the verification result returned by the claimant.

3.40.3 Security Limitations in Bluetooth :

- Due to its wireless nature, experts express a security concern with Bluetooth.
- The issue can be addressed with three aspects: specific sequence of channel hopping known only to the sending and receiving devices, challenge-response authentication routine to verify the validity of the receiving unit, and the 128-bit key encryption standard for securing transmission between devices.

3.40.4 Logical Link Control and Adaptation Protocol (L2CAP) :

- The Logical Link Control and Adaptation Layer Protocol (L2CAP) is layered over the baseband protocol and resides in the data link layer.
- L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher-level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length.

- Two link types are supported for the baseband layer : Synchronous Connection-Oriented (SCO) links and Asynchronous Connection-Less (ACL) links. SCO links support real-time voice traffic using reserved bandwidth. ACL links support best effort traffic. The L2CAP specification is defined for only ACL links and no support for SCO links is planned.

3.40.5 Host Controller Interface :

- As shown by the dotted line in Fig. 3.36.1, this is an optional interface between the higher and the lower layers of the Bluetooth protocol stack. It is used for accessing the Bluetooth hardware capabilities.
- This layer is needed whenever the higher layers are implemented on the motherboard of a Bluetooth host device (Such as a personal computer).
- By doing so it is possible to utilize the spare capacity of that device.
- Different packet types related to this layer are : command packets, event packets and data packets.
- Command packets are used by the host to control the device, event packets are used by the device to inform host about any changes and data packets carry data.

3.41 Middleware Protocol Group :

- The middleware protocol group presents a basic interface to application layer. This interface may be used for communicating across the transport layer.
- This group consists of RFCOMM layer, Service Discovery Protocol (SDP), IrDA interoperability protocols, Telephone Control Specifications (TCS) and audio.
- The RFCOMM layer presents a virtual serial port for the applications that use serial interface. All the applications that use the serial interface work without any problem on Bluetooth devices.
- RFCOMM makes use of L2CAP connection in order to establish a wireless link between two devices.
- The SDP (Service Discovery Protocol) discovers the services offered by the other Bluetooth device to

which link has been established. This makes the devices self configured with no manual intervention.

The IrDA interoperability protocol is for allowing the existing IrDA applications to work on Bluetooth devices without any changes.

IrDA contains two major protocols namely IrOBEX (IrDA object exchange) which exchanges objects between two devices and IrMC (Infrared mobile communications) which is used for synchronization.

Audio is given the highest priority in Bluetooth. It is transmitted directly over baseband at 64 kbps which ensures a very good voice quality.

Audio is not actually a layer of protocol stack. Infact it is only a specific packet format which we can transmit directly over the SCO link of the baseband layer.

TCS-BIN (Telephony Control Specifications-Binary) protocol is used to implement telephony control. The three major areas of TCS functionality are :

1. Call control
2. Group management
3. Connectionless TCS

Call control is used for setting up the wireless links. On these connections we can transfer voice or data. TCS can be used for the point-to-point and point-to-multipoint configurations.

Because of the group management functionality of TCS it is possible to have multiple telephone extensions, call forwarding and group calls.

Two more functions performed by TCS are configuration distribution and fast intermember access. Configuration distribution mechanism is used for finding information about other members in a group whereas using the fast intermember access two slaves can create a new piconet.

All the exchanges discussed above need a connection oriented channel to be established. But it is wasteful if we use such a connection in order to exchange simple information such as adjustment of volume.

Instead we can use connectionless TCS to have a connectionless channel for such simple exchanges.

3.42 Bluetooth Profiles :

- These are developed in order to ensure that there is interoperability among various implementations of the Bluetooth protocol stack.
- Each Bluetooth specification is used for implementing a specific user end function. Such a Bluetooth specification provides a clear and transparent standard for implementing a specific end user function.
- There are 13 profiles listed which can be broadly classified into four categories :
 1. Generic profiles
 2. Telephony profiles
 3. Networking profiles
 4. Serial and object exchange profiles

1. Generic profiles :

A generic profile is not really an application. But it provides a way to establish and maintain secure links between the master and the slaves.

2. Telephony profiles :

- This is the cordless telephony profile designed for three-in-one phones. The three in one phones offer the following functions : intercom, cordless phone and mobile phone.
- In the intercom mode two way voice communication between two within range Bluetooth devices will be allowed to take place.
- The handset profile specifies how a Bluetooth device can be connected to a handset.

3. Networking profiles :

- The LAN Access profile enables Bluetooth devices to get connected to either a LAN through APs or to form a small wireless LAN among themselves.
- The dial-up networking profile will allow a dial up connection via Bluetooth enabled mobile phones.
- The FAX-profile is very similar to dial-up profile and it enables computers to send and receive FAX messages via a Bluetooth enabled mobile phone.



4. Serial and object exchange profiles :

- The serial port profile emulates a serial line (RS232 and USB serial ports) for those applications which need a serial line.
- Some other profiles such as generic object exchange, object push, file transfer and synchronization are used for exchanging objects between two wireless devices.

3.42.1 Limitations :

- Bluetooth communication does not support routing.
- The issues of handoffs have not been addressed.
- Due to master slave configuration, many times performance degradation takes place due to bottlenecking at the master.
- Interference with WLAN is essential as WLAN and Bluetooth both operate in the same ISM frequency band.

3.42.2 Bluetooth Advantages :

- One can create a personal area network at home or on the road with Bluetooth-enabled devices such as keyboard, mouse, scanner, PDA, laptop, cell phone, etc.
- This network can automatically help synchronize notes, calendar, address book and also print pictures, receive emails, access cell phones messages, etc. It can even help consumers pay bills with credit card through Bluetooth cash register if a Bluetooth PDA stores the card information.

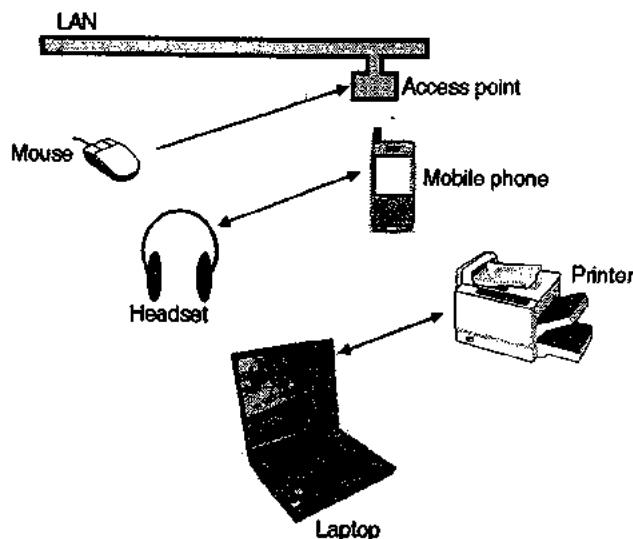
3.42.3 Comparison of Bluetooth and WLAN IEEE 802.11x :

Sr. No.	Bluetooth	IEEE 802.11x
1.	Bluetooth hop frequency is 1600 hops/second	IEEE 802.11x hop frequency is 2.5 hops/second
2.	Data transfer rate is 1 Mbps	Data transfer rate is 11 Mbps
3.	Transmission range is 10 m	Transmission range is 15-150 m indoor and 300 m outdoor
4.	Bluetooth uses lower transmission power	IEEE 802.11 uses more transmission power than Bluetooth
5.	It is used to connect devices that are in close proximity such as palm computing devices attached to smart phones, notebooks to printers.	designed to provide full network service at Ethernet data rate.
6.	Bluetooth is being a standard for short time network.	IEEE 802.11 is a standard for LAN and is for longer time network.
7.	Bluetooth uses GFSK (Gaussian Frequency Shift Keying) modulation technique	IEEE 802.11 uses CCK (Complementary Code Keying) modulation technique

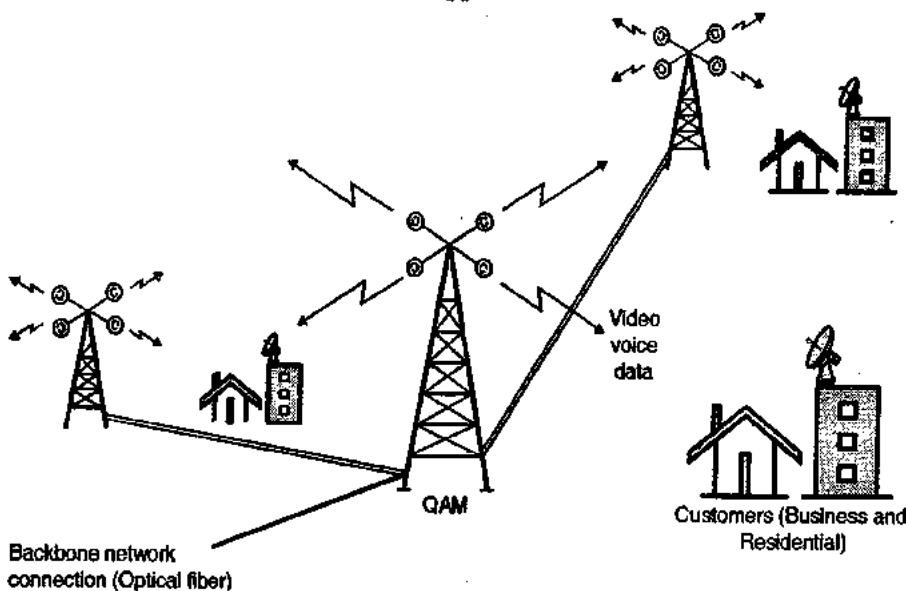
Sr. No.	Bluetooth	IEEE 802.11x
	proximity such as palm computing devices attached to smart phones, notebooks to printers.	designed to provide full network service at Ethernet data rate.
6.	Bluetooth is being a standard for short time network.	IEEE 802.11 is a standard for LAN and is for longer time network.
7.	Bluetooth uses GFSK (Gaussian Frequency Shift Keying) modulation technique	IEEE 802.11 uses CCK (Complementary Code Keying) modulation technique

3.43 Applications of Bluetooth :

- The bluetooth has done a job of "removing the wires."
- Bluetooth uses an invisible, low power short range wireless connection for providing communication.
- It is an open standard used by over 1000 manufacturers of electronic appliances. It operates on the ad-hoc approach to enable communication among various devices within a range of 10 meters.
- Bluetooth operates in the 2.4 GHz ISM band (2400-2483.5 MHz) and uses the frequency hopping TDD (Time Division Duplex) scheme for each radio channel.
- The bandwidth of each Bluetooth radio channel is 1 MHz and it hops at 1600 hops per second. The GPSK (Gaussian Phase Shift Keying) scheme is used.
- Bluetooth is capable of working in a very high interference level. It uses a number of Forward Error Correction (FEC) and Automatic Repeat Request (ARQ) error control schemes to minimize errors.
- Various countries have allocated different channels for Bluetooth applications.
- IEEE 802.15 standards committee provides standards for development of Bluetooth and other PANs (Personal Area Networks) to interconnect PCs, laptops, cellphones, light projectors and other appliances.



(G-1167) Fig. 3.43.1 : Applications of Bluetooth



(L-430) Fig. 3.44.1 : Broadband wireless MAN IEEE 802.16

Short Message Service (SMS) :

- This service offers transmission of messages upto 160 characters. SMS messages do not use the standard data channels of GSM.
- Sending and receiving of SMS via Bluetooth is possible during data or voice transmission.
- SMS can also be used for other applications such as displaying road conditions, or stock quotes. It can also be used to transfer logos, ring tones, horoscopes etc.

Enhanced Message Service (EMS) :

- EMS is the next step of SMS. It has a much larger message size (upto 760 characters). EMS can be used to transmit formatted text animated pictures, small images, ring tones etc.
- However EMS did not become as popular as SMS or MMS.

Multimedia Message Service (MMS) :

- MMS is used to transmit the larger pictures (GIF, JPG), short video clips etc. and came with mobile phones having cameras.

3.44 IEEE 802.16 (WMANs) :

- Fig. 3.44.1 shows the structure of the wireless MAN. The IEEE developed the 802.16 standard as a replacement to the local network operators.
- The 802.16 WMAN provides a standard solution for a cable free telecommunication service market.
- The IEEE 802.16 standard was published in 2002. Before this time, there were two other wireless MAN solutions already existing.
- They were :
 1. Multichannel Multipoint Distribution System (MMDS)

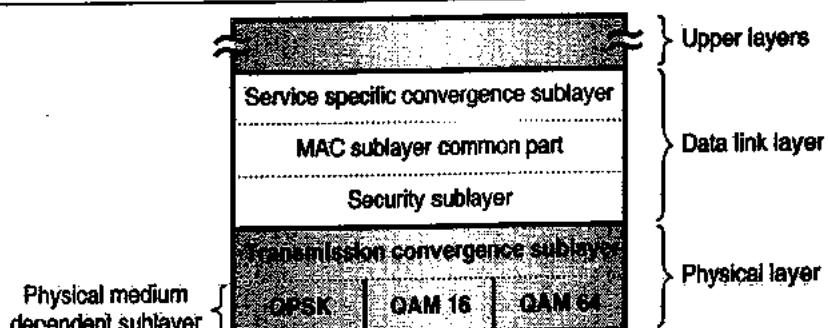


- 2. Local Multipoint Distribution System (LMDS)
- These two operated at different frequencies in the millimeter wavelength range.
- Both these WMAN solutions suffered due to lack of standardization. So their use remained restricted.
- The MMDS solution works at 2.4 GHz or 5 GHz band and has a range of upto 50 km. MMDS was designed originally for the wireless CATV solution, without a backward channel from the customer.
- But in order to make as much revenue as possible the MMDS solutions are used for voice and internet services.
- The data rates for such applications are 128 kbps upto 3 Mbps downstream from base station to subscriber and 128 kbps from subscriber to the base station.
- The subscribers can access telephony and ISP through a modem.
- 802.16 MMDS and LMDS use the frequencies in the band 2 GHz to 60 GHz.
- With increase in frequency these waves become more and more directional. They travel in a straight line and can be easily absorbed by water.
- So rain, snow, trees absorb these electromagnetic waves and create errors in the received signal.

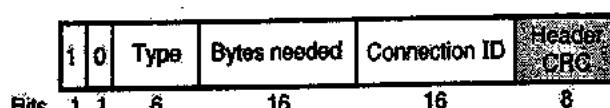
- In order to overcome this problem, the signal produced by the base station and the customer stations are encoded using Hamming codes.

3.44.1 The 802.16 Protocol Stack :

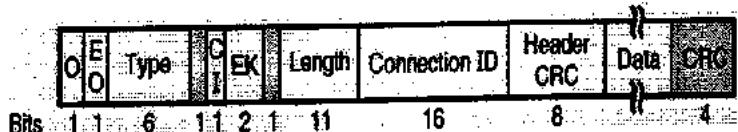
- Fig. 3.44.2 shows the 802.16 protocol stack.
- The physical layer is the lowermost layer with three modulation options i.e. QPSK (Quadrature Phase Shift Keying), 16-QAM (Quadrature Amplitude Modulation) and 64-QAM.
- These modulation schemes are used to counterbalance the range problem and the signal degradation due to absorptions.
- Above the physical layer we have the data link layer which is divided into three sublayers :
 1. Security sublayer
 2. MAC sublayer common part
 3. Service specific convergence sublayer.
- The security sublayer which supports for the data encryption. This is essential so as to protect the privacy of the data and video information carried by the WMAN.



(L-431) Fig. 3.44.2 : 802.16 protocol stack



(a) Data frame



(b) Control frame

(L-433) Fig. 3.44.3 : 802.16 Frame formats

- The MAC sublayer common part has the task of time slot allocation of the medium through the reservation mechanism.

- The service specific sublayer deals with different types of services such as voice, video and data.

3.44.2 802.16 Frame Format :

- Fig. 3.44.3 shows the frame formats of 802.16 WMAN system. There are two frames, namely the data frame and the control frame.

- In Fig. 3.44.3(a) and (b),

EO = Encryption payload.

Type = Type of frame

CI = Check sum indication

EK = Which of the 4 encryption keys used

Length = Including Header

$$\text{Header CRC} = X^8 + X^2 + X + 1$$

- The control frame is as shown in Fig. 3.44.3(b). It is used to request time slots for different types of services.

- The control frame identifies the terminal through the connection ID. The "type" field which is 6 bit long identifies the type of control packet.

- Bytes needed field identifies how much data (in terms of number of bytes) the terminal wants to transmit.

- Fig. 3.44.3(a) shows the data frame format. The first bit in the frame decides whether this frame is a data frame or control frame.

0 – Data frame

1 – Control frame

- The 6 bit type field identifies the type of frame connection ID and Header CRC fields are same as those in the control frame.

3.44.3 Difference Between IEEE 802.11 and IEEE 802.16 :

- IEEE 802.11 is a successful standard for WLAN. But it is not Broadband Wireless Access (BWA). This will be clear when the

following differences between IEEE 802.11 and IEEE 802.16 are studied.

Table 3.44.1

Sr. No.	IEEE 802.11 (WLAN)	IEEE 802.16 (BWA)
1.	This is designed for mobile terminals.	This is designed for broadband data such as digital video and telephony.
2.	Less number of users. Less usage of bandwidth per user.	Large number of users and large bandwidth usage per user.
3.	Uses ISM band of the frequency spectrum.	Uses much larger frequency band. It uses millimetre wave band and microwave band (above 1 GHz frequency).
4.	IEEE 802.11 provides some QoS support for real time data in PCF mode but it has not been designed for the QoS support for broadband usage.	IEEE 802.16 is completely connection oriented. All the transmissions are therefore QoS guaranteed.

3.44.4 Physical Layer (IEEE 802.16) :

- The physical layer makes use of narrow band radio (10-66 GHz). The conventional modulation schemes are used for transmission (QPSK, QAM-16 and QAM-64).
- The transmission convergence sublayer hides the transmission topology from the DLL.
- The modulation scheme is selected on the basis of distance between SS and BS. QAM-64 is preferred for shorter distances, QAM-16 for intermediate and QPSK for longer distances.
- The data rates of the three modulation schemes are as follows :

Scheme	QAM-64	QAM-16	QPSK
Data rate	180 Mbps	120 Mbps	60 Mbps

- With increase in distance the data rates become slower.
- For the operation in millimetre wave band, the Base Stations (BSs) can have multiple antennas. This is not possible if the microwave band is being used.



- The error rates associated with the millimetre band waves are high. Therefore Hamming codes are used to do the forward error correction.
- The voice traffic is more symmetric but other applications such as Internet access are not. There the upstream traffic is less than the downstream traffic.
- In order to successfully accommodate them, IEEE 802.16 uses either FDD (Frequency Division Duplex) or TDD (Time Division Duplex) to accommodate bandwidth.

3.44.5 Data Link Layer :

- The DLL was designed in order to use the spectrum efficiently. Very high uplink and downlink bit rates are required alongwith a range of QoS for the broadband services. Security issues also are equally important.
- The DLL of IEEE 802.16 is subdivided into three sublayers as follows :
 1. Security sublayer.
 2. MAC sublayer.
 3. Service specific convergence sublayer.

1. Security sublayer :

- Refer to the IEEE 802.16 protocol stack which shows that the security sublayer is the lowermost layer of the three sublayers in a DLL. This sublayer deals with privacy and security.
- The functions of this layer are as follows : Management of encryption, decryption and key management.
- However note that only the payloads i.e. data are encrypted and not the entire headers.

2. MAC sublayer common part :

- This part deals with the channel management and allocation of slots for various stations.
- MAC sublayer balances out two factors namely the stability of contention-less operation and the efficiency of contention-based operation using TDM/TDMA mechanism.
- TDM is used for multiplexing over the downlink and TDMA is used for medium sharing over downlink.

- IEEE 802.16 supports connection oriented services and the four classes of services given for each uplink connection are as follows :
 1. Constant bit rate service.
 2. Real time variable bit rate service.
 3. Non real time variable bit rate service.
 4. Best effort service.

3. Service specific convergence sublayer :

- This is the topmost sublayer in DLL and its task is to interface to the network layer.
- IEEE 802.16 has been designed to operate with both connection-less and connection oriented protocols.

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 Explain the FDDI system.
- Q. 7 What are the functions of a transceiver ?
- Q. 8 Why there is no need of CSMA/CD for a full duplex Ethernet LAN ?
- Q. 9 Explain CSMA/CD.
- Q. 10 What is CSMA/CA ?
- Q. 11 Write a note on : Physical layer implementation in traditional Ethernet.
- Q. 12 Compare the data rates of traditional, fast and Gigabit Ethernets.
- Q. 13 Explain the physical layer implementation in fast Ethernet.
- Q. 14 What are the common fast Ethernet implementations ?
- Q. 15 Compare the reconciliation sublayer in Fast Ethernet with the PLS sublayer in traditional Ethernet.
- Q. 16 What is GMII in Gigabit Ethernet ?
- Q. 17 Write a short note on FDDI.

- | | | | |
|-------|---|-------|--|
| Q. 18 | Write comparison of 802.3, 802.4 and 802.5 standards related to type of cable used, frame structure, cable length, frequency range. | Q. 30 | Explain the operating principle of OFDM used for IEEE 802.11 a. |
| Q. 19 | How does the Token Ring LAN operate ? | Q. 31 | Write a short note on MAC layer specification for IEEE 802.11. |
| Q. 20 | Explain the frame format of 802.3, 802.4 and 802.5. | Q. 32 | Define DCF and PCF. |
| Q. 21 | What is Fast Ethernet ? | Q. 33 | Explain the architecture of wireless LAN 802.11 with suitable diagram. |
| Q. 22 | Explain the LLC and MAC in IEEE 802 standard and explain the operation of CSMA/CD as used in LAN. | Q. 34 | Explain the term Ad hoc networking. |
| Q. 23 | Write a short note on FDDI. | Q. 35 | State and explain the wireless LAN requirements / properties. |
| Q. 24 | Explain the basic configuration of wireless LAN. | Q. 36 | Compare : Ethernet and Wireless networks. |
| Q. 25 | Define BSS and ESS. | Q. 37 | What is bluetooth ? |
| Q. 26 | Explain different types of stations in ESS. | Q. 38 | Explain the architecture of Bluetooth. |
| Q. 27 | Write a short note on physical layer specifications of IEEE 802.11. | Q. 39 | List the Bluetooth devices. |
| Q. 28 | Explain IEEE 802.11 FHSS. | Q. 40 | Explain the frame format of Bluetooth. |
| Q. 29 | Explain the principle of IEEE 802.11 DSSS. | Q. 41 | State the advantages and applications of Bluetooth. |
| | | Q. 42 | Compare : Bluetooth and wireless LAN. |

000

CHAPTER 4

Unit IV

Network Layer

Syllabus :

Switching techniques, Routing Protocols: Distance Vector, Link State, Path Vector, Congestion control.

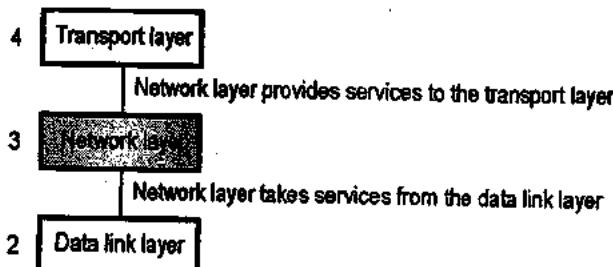
4.1 Network Layer :

- 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.

4.1.1 Position of Network Layer :

- Fig. 4.1.1 shows the position of network layer in the 5 layer internet model. It is the third layer.

Layer



(G-433) Fig. 4.1.1 : Position of network layer

- It receives services from the data link layer and provides services to the transport layer.

4.1.2 Network Layer Duties :

Fig. 4.1.2 shows the set of duties of the network layer.

1. Internetworking :

This is the main duty of network layer. It provides the logical connection between different types of networks.

2. Addressing :

- Addressing is necessary to identify each device on the Internet uniquely. This is similar to a telephone system.
- The addresses used in the network layer should uniquely and universally define the connection of a computer.

3. Routing :

- In a network, there are multiple roots available from a source to a destination and one of them is to be chosen.
- The network layer decides the root to be taken. This is called as routing and it depends on various criterions.

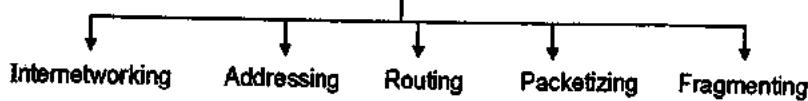
4. Packetizing :

- As discussed earlier, the network layer encapsulates the packets received from upper layer protocol and makes new packets.
- This is called as packetizing. It is done by a network layer protocol called IP (Internetworking protocol).

5. Fragmenting :

The datagram can travel through different networks. Each router decapsulates the IP datagram from the received frame. Then the datagram is processed and encapsulated in another frame.

Duties of the network layer



(G-434) Fig. 4.1.2 : Duties of the network layer

Other issues : The other issues which are not directly related to the duties of network layer but need to be discussed are :

1. Address resolution.
2. Multicasting.
3. Routing protocols.

Other supporting protocols :

The internetworking protocol (IP) needs the support of another protocol ICMP (Internet Control Message Protocol) to achieve the host-to-host delivery.

How to achieve the goals ?

- In order to achieve the goals, the network layer must know about the topology of the communication subnet i.e. the set of all routers.
- It also should choose appropriate paths for communication.
- The routes should be chosen in such a way that overloading of some routers and idle operation of others should be avoided.

4.2 Network Layer Design Issues :

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

University Questions

- Q. 1 Explain design issue of network layer.**
(Dec. 09, 8 Marks)
- Q. 2 Explain various network layer design issues.**
(Dec. 11, 4 Marks)
- Q. 3 Explain network layer issues in detail.**
(May 13, 8 Marks)

- The important network layer design issues include the service provided to the transport layer and the internal design of subnet.

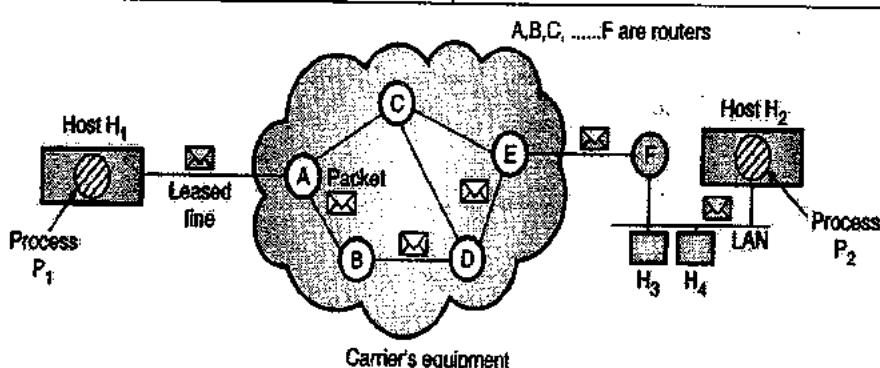
The network layer has been designed with the following goals :

- The services provided should be independent of the underlying technology. Users of the service need not know about the physical implementation of the network.
- This design goal has great importance because there is a great variety of networks in operation.

- The design of the layer must not disable us from connecting to networks of different technologies.
- The transport layer (that is the host computer) should be shielded from the number, type and different topologies of the subnets user uses. That is, all that transport layer wants is a communication link, it need not know how that link is established.
- Finally, there is a need for some uniform addressing scheme for network addresses.
- With these goals in mind, two different types of services emerged :
 1. Connection oriented Network Services
 2. Connectionless Network Services.
- A **connection-oriented service** is one in which the user is given a "reliable" end to end connection.
- To communicate, the user first makes a request for connection, then uses the connection to communicate his content, and then closes the connection.
- A telephone call is the classic example of a connection oriented service.
- In a **connectionless service**, the user simply puts his information into bundles called packets, puts an address on it, and then sends it for the destination..
- There is no guarantee that the bundle will reach the destination. So a connectionless service is one which is similar to the postal system.

4.2.1 Store and Forward Packet Switching :

- Refer Fig. 4.2.1 which demonstrates the environment of the network layer protocols.
- This system of Fig. 4.2.1 is made up of following components :
 1. Carrier equipments (routers and transmission lines).
 2. Customer's equipments.
- H_1 is host - 1 and it is directly connected to router A via a leased line. Host H_2 is on a LAN which is connected to router F.



(G-435) Fig. 4.2.1 : The environment of the network layer protocols

- Host H_1 wants to send a packet. So it communicates with its nearest router (A).
- Router A will store the packet until it has fully arrived so that the checksum can be verified.
- Then the packet is forwarded to the next router (B). This process continues till it reaches the destination host H_2 .
- This mechanism is called as the store and forward packet switching.

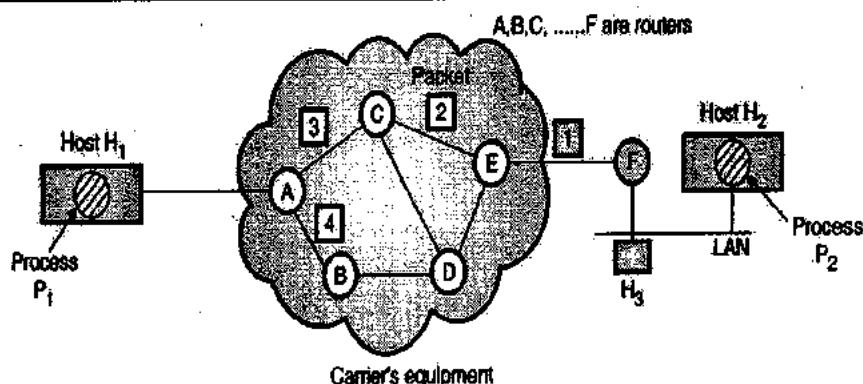
4.2.2 Services Provided to the Transport Layer :

- The network layer services are designed to achieve the following goals :
 1. The services should not be dependent on the subnet technology.
 2. Transport layer should not be exposed to the number, type and topology of the subnet.
 3. The network address which is made available to the transport layer must use a uniform numbering plan.

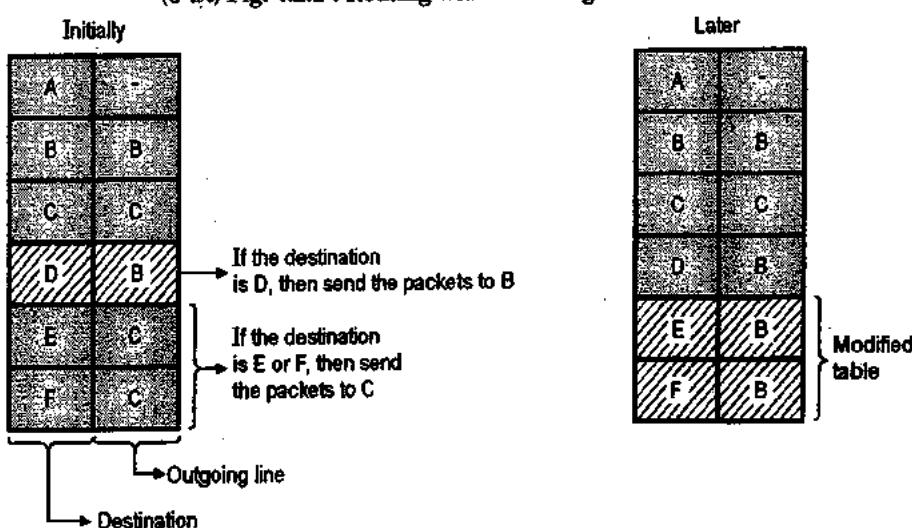
- The network service can be connectionless or connection oriented.
- The Internet has a connectionless network layer whereas the ATM networks have a connection oriented network layer.
- The connection oriented and connectionless services both have their own sets of advantages and disadvantages.
- Finally we can say that the network layer should provide a raw means to send packets from a to b and that is all.

4.2.3 Implementation of Connectionless Service :

- In the connectionless service, the packets from sending host H_1 are injected into the subnet individually and each packet is routed independently as shown in Fig. 4.2.2.
- No advanced connection establishment is required. The packets are called as **datagrams** and the subnet is called as **datagram subnet**.



(G-43) Fig. 4.2.2 : Routing within a datagram subnet

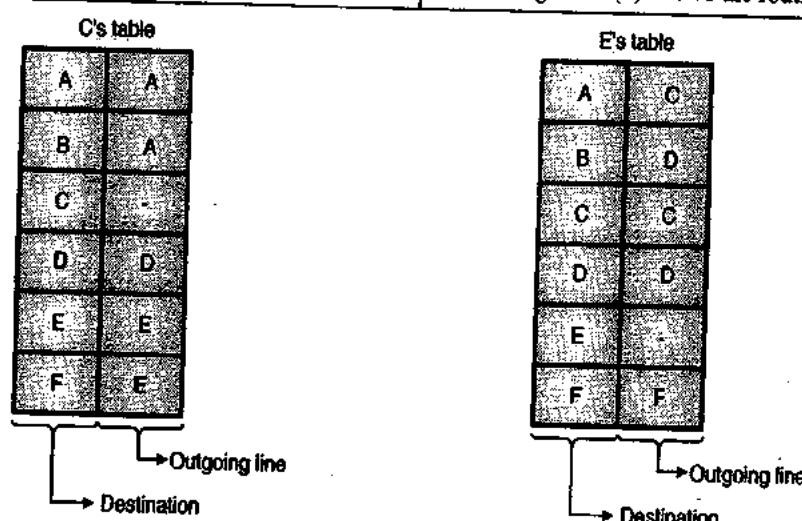


(G-43) Fig. 4.2.2(a) : Routing tables of A

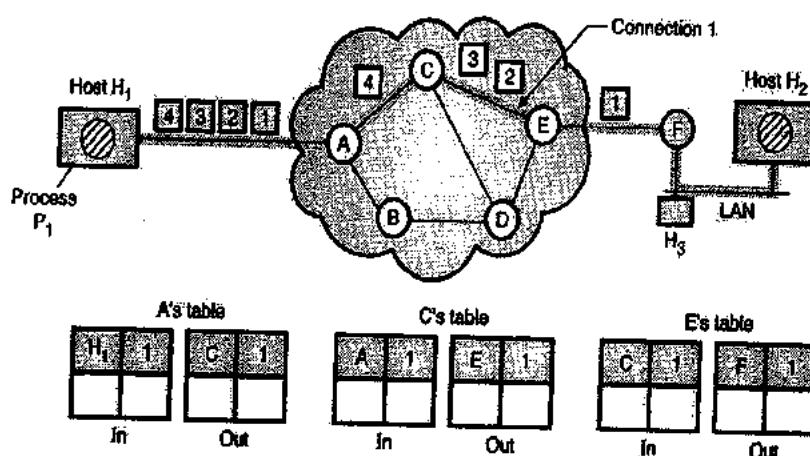
Working :

- Process P_1 on host H_1 wants to send a long message to process P_2 on host H_2 . Let this message be broken into four packets 1, 2, 3 and 4 at the network layer.
- Then all these packets are sent to router A. Every router has its internal table which tells it where to send packets for each possible destination.
- Each entry in the router's table is a pair that consists of a destination and the outgoing line to be used to send the packet for that destination.
- In Fig. 4.2.2, C has two outgoing lines E and D. So every packet coming to router C should be sent to either D or E, even if the ultimate destination is F.

- Fig. 4.2.2(a) shows the routing table of A. It has two tables named as **initially** and **later**.
- As per the **initial** routing table of A, since the destination is F the packets 1, 2 and 3 were first sent to C, then to E and finally to F.
- But when packet 4 arrived at the input of A, even though the destination was F, the packet was not sent to C instead it was sent to B. The reason can be a traffic jam along the ACE path.
- As soon as A learned about the traffic jam along the ACE path it modified its routing table as shown in Fig. 4.2.2(a) as **later** and routed the 4th packet via path ABDEF.
- Fig. 4.2.2(b) shows the routing tables for C and E.



(G-438) Fig. 4.2.2(b) : Routing tables of C and E



(G-439) Fig. 4.2.3 : Routing within a VC subnet



4.2.4 Implementation of Connection-Oriented Service :

- For the connection oriented service, a path from source to destination needs to be established before sending any data packet. This connection is called as **Virtual Circuit (VC)** and the subnet is called as the **Virtual Circuit Subnet**.
- Here all the packets will follow the same path which was established before communication.
- When the connection is opened, the virtual circuit is also terminated. In the connection oriented service, each packet carries an identifier. This identifier can tell us about the virtual circuit (VC) that this packet belongs to.
- Refer Fig. 4.2.3. Host H_1 has established connection 1 with host H_2 .
- This connection is remembered as the first entry in each routing table. As shown in Fig. 4.2.3, the first line of A's table shows that if a packet having connection identifier 1 arrives from H_1 , it should be routed to C and a connection identifier 1 should be given to it.
- Similarly the first line of C's table shows that it routes the packets to E with an identifier 1.

4.2.5 Internal Organization of the Network Layer :

- Basically there are two philosophies for organizing the subnet :
 - To use connection oriented service.
 - To use connectionless service.
- In the connection oriented service, a connection is called as **virtual circuit**. It is similar to a physical connection between the sender host and the destination host.
- In the connectionless organization, the independent packets are called as **datagrams**. They are analogous to telegrams.

Virtual circuits :

- The principle behind the virtual circuits is to choose only one route from source to destination.
- When a connection is established, it is used for sending all the traffic over this connection.

- When the connection is released, the virtual circuit is terminated.

Datagram :

- With a datagram, the routes from source to destination are not decided in advance.
- Each packet sent is routed independently. Different packets of the same message can follow different routes.
- The datagram subnets have to do more work but they are more robust and deal with failures and congestion more easily as compared to virtual circuit subnets.

Features of virtual circuits :

- In virtual circuits every router will have to maintain and update a table.
- Each packet must have a virtual circuit number field in its header in addition to sequence number checksum etc.
- It is necessary to setup a VC before communication.
- The users are charged for connect time as well as for the amount of data transported.

Features of a datagram :

- The routers do not have to maintain any tables.
- Each datagram must contain full destination address. These addresses can be very long.
- When a packet comes in, the router finds an available outgoing line and sends the packet out on that line. So that it can reach the destination.

4.2.6 Comparison of Virtual Circuit and Datagram Subnets :

Table 4.2.1 shows the comparison of VC subnet and datagram subnets.

Table 4.2.1

Sr. No.	Parameter	VC subnet	Datagram subnet
1.	Connection set up	Required	Not required.
2.	Addressing	Each packet contains a short VC number	Each packet contains the source as well as destination address.
3.	Repairs	Harder to repair	Easy to repair.

	Parameter	VC subnet	Datagram subnet
4.	State information	A table is needed to hold the state information.	Subnet does not hold state information.
5.	Routing	Route chosen is fixed. All packets follow this route. This is static routing.	Each packet is routed independently. This is dynamic routing.
6.	Congestion control	Easy	Difficult.
7.	Effect of router failure.	All VCs which passed through failed router are terminated.	No other effect except for the packets lost at the time of crash.

4.3 Delivery :

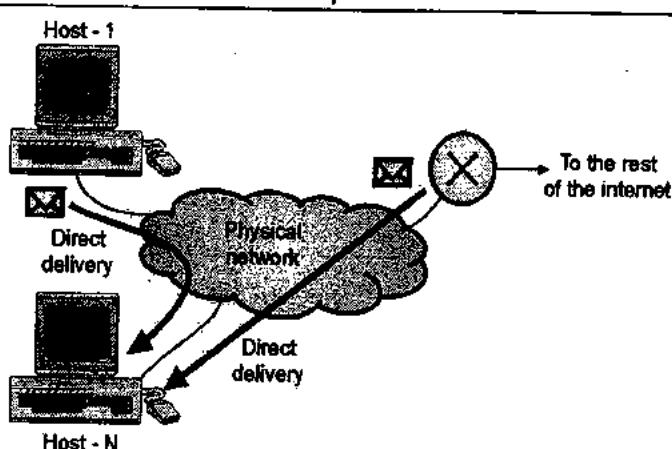
- The network layer supervises how the packets are being handled by the underlying physical networks. This handling is known as the delivery of packets.
- The two different methods of delivery are :
 1. Direct delivery
 2. Indirect delivery.

4.3.1 Direct Delivery :

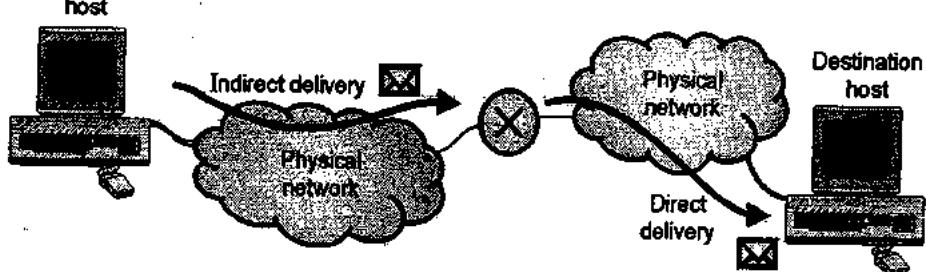
- In the direct delivery the destination host and the one who delivers the packet are in the same physical network as shown in Fig. 4.3.1(a).
- The sender can extract the network address of the destination using the mask. It then compares this address with the addresses of the networks to which it is connected. If these two addresses are identical then the delivery is direct.

4.3.2 Indirect Delivery :

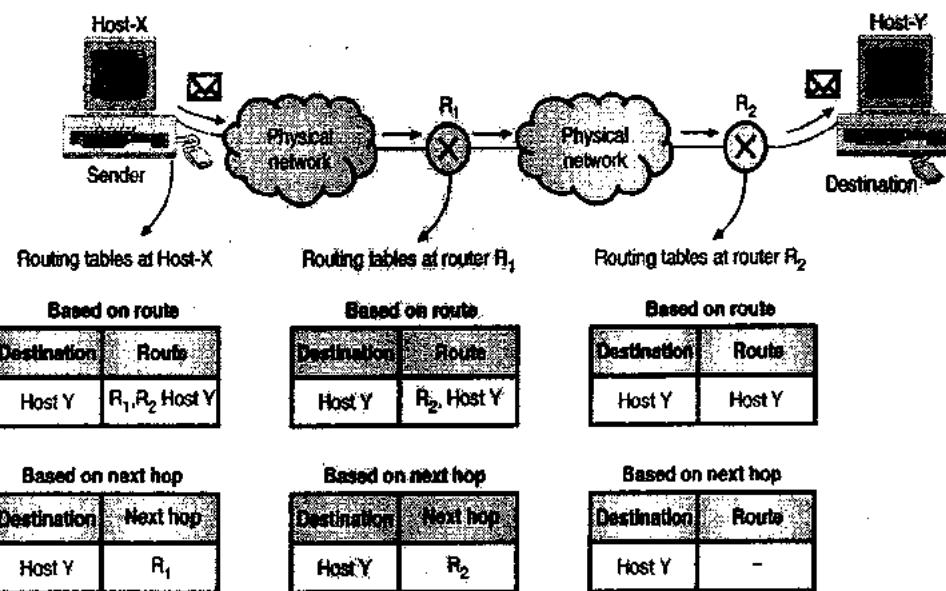
- In the indirect delivery of packets, the sender host and the destination host are not the part of the same physical network as shown in Fig. 4.3.1(b).
- In such a situation, the packets travel from one router to the other and are finally delivered to the destination host.
- The indirect delivery involves one direct and zero or more indirect deliveries. The last delivery is always a direct one.



(G-44) Fig. 4.3.1(a) : Direct delivery



(G-44) Fig. 4.3.1(b) : Indirect delivery



(G-442) Fig. 4.4.1(a) : Route method versus Next Hop method

4.4 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.

4.4.1 Forwarding Techniques :

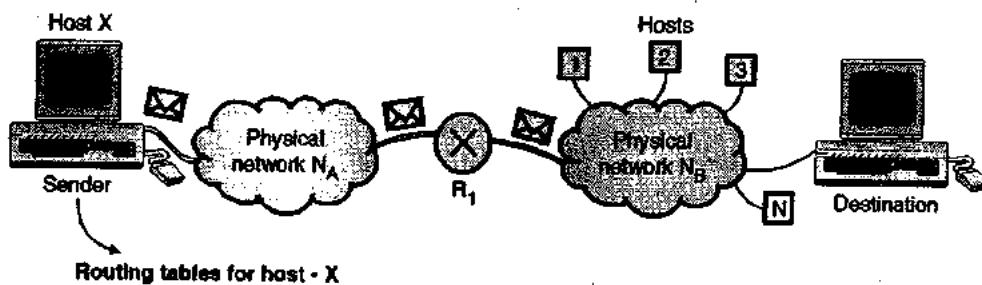
- Many techniques have been invented and tested in order to make the size of the routing tables manageable. Some of them are as follows :
 1. Next hop method versus Route method.
 2. Network specific method versus Host specific method.
 3. Default method.

4.4.2 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. 4.4.1(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. 4.4.1(a).

4.4.3 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. 4.4.1(b).
- 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.



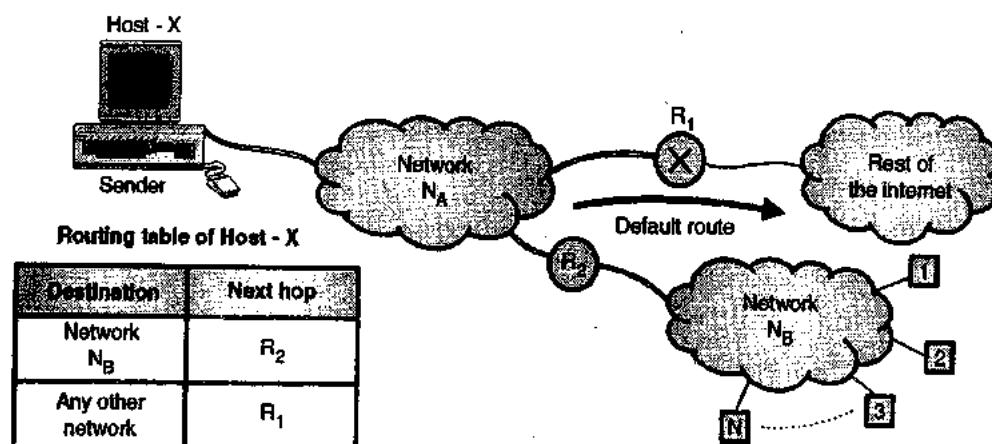
Host specific method

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. 4.4.1(b) : Host specific method versus network specific method



(G-444) Fig. 4.4.1(c) : Default method

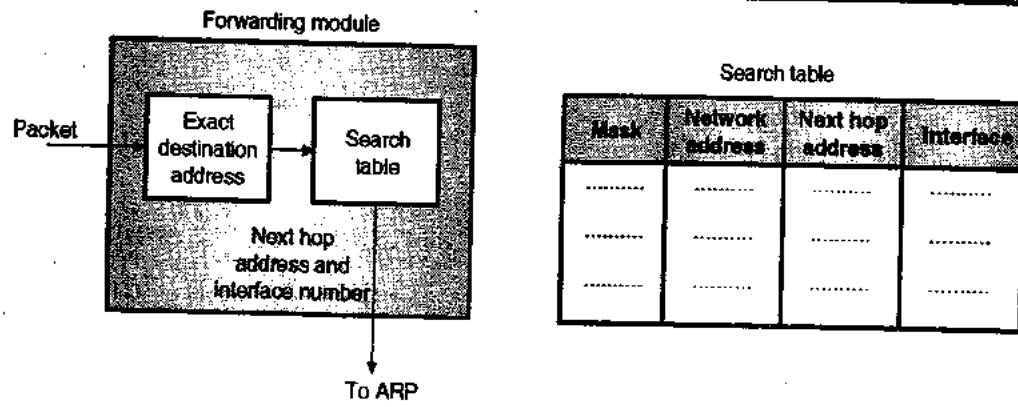
4.4.4 Default Method :

- This is one more method of simplifying the routing tables. Refer Fig. 4.4.1(c) in which the sending host X is connected to a network with two routers R₁ and R₂.
- Router R₂ routes the packets to the hosts connected to network N_B. However router R₁ 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).

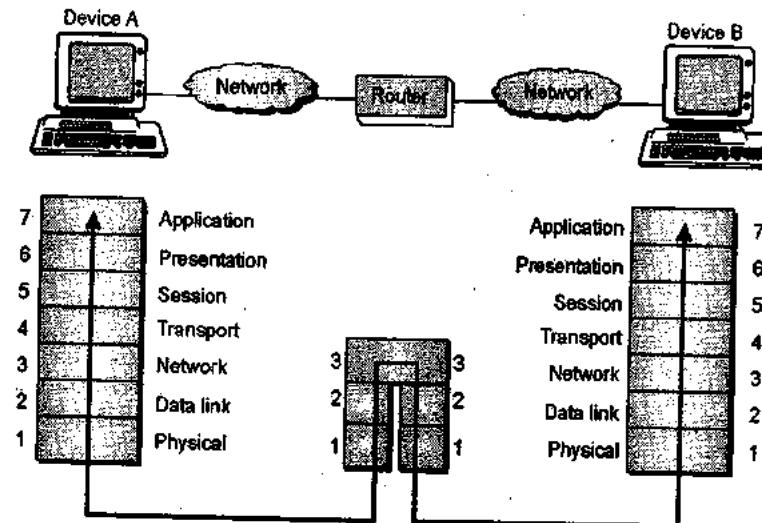
4.4.5 Forwarding Process :

- In order to explain the forwarding process let us assume that hosts as well as routers use classless addressing.

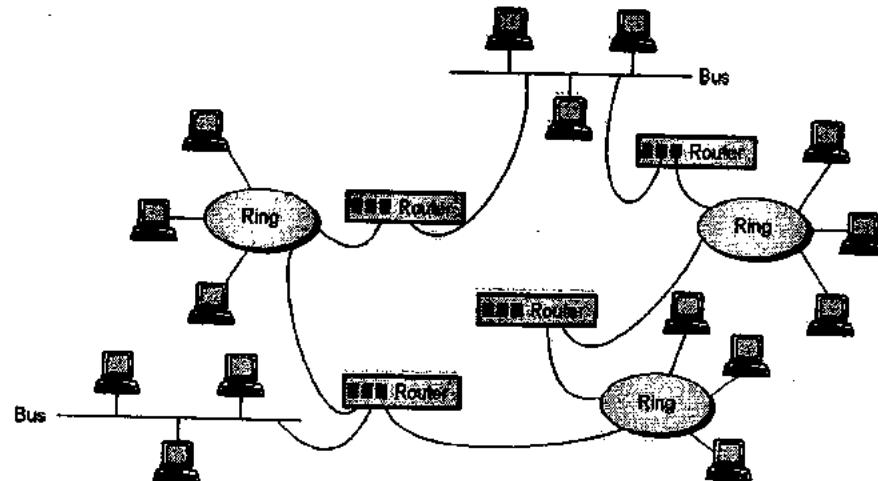
- For classless addressing, in the routing table we should have one row of information for each block.
- This table should be searched on the basis of the network address (first address in the block).
- But the problem here is that the destination address does not tell anything about the network address. 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.
- The forwarding module for the classless addressing is shown in Fig. 4.4.2.



(G-445) Fig. 4.4.2 : Forwarding module in classless address



(G-446) Fig. 4.5.1(a) : A router in the OSI model



(G-447) Fig. 4.5.1(b) : Routers in an internet

4.5 Routers :

- Routers are devices that connect two or more networks as shown in Figs. 4.5.1(a) and (b). They consist of a combination of hardware and software.
- Routers are devices that connect two or more networks as shown in Figs. 4.5.1(a) and (b). They consist of a combination of hardware and software.
- The hardware can be in the form of a network server, a separate computer or a special device, as

well as the physical interfaces to the various networks in the internetwork.

- Various types of networks can be interconnected through routers as shown in Fig. 4.5.1(b).
- The software in a router are the operating system and the routing protocol. Management software can also be used.
- Routers use logical and physical addressing to connect two or more logically separate networks.

- The large network is organized into small network segments called as subnets and these subnets are interconnected via routers.
- Each of the subnet is given a logical address. This allows the networks to be separate but still access each other and exchange data.
- Data is grouped into packets, or blocks of data. Each packet has a physical device address as well as logical network address.
- The network address allows routers to calculate the optimal path to a workstation or computer.
- Route discovery is the process of finding the possible routes through the internetwork and then building routing tables to store that information. The two methods of route discovery are :
 - Distance vector routing
 - Link state routing.

Note:

- Router's work at the network layer of the OSI model.
- With static route selection, packets always follow a pre-determined path.

- In distance vector routing, each router advertises its presence periodically to other routers on the network.
- Link state routers broadcast their complete routing tables only at startup and at certain intervals.
- Dynamic route selection permits routers to constantly adjust to changing network conditions.
- With static route selection, packets always follow a pre-determined path.

4.5.1 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 :

- Static routing tables
- 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 :

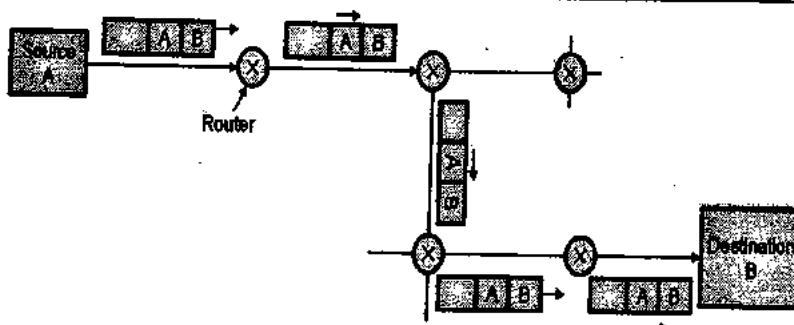
- The dynamic routing tables can get automatically updated by using a dynamic routing protocol such as RIP, OSPF or BGP.
- The structure of a dynamic routing table is shown in Table 4.5.1.

Table 4.5.1 : Format of dynamic routing table

Mask	Network Address	Next Hop IP Address	Interface	Flags	Reference count	Time

4.6 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. 4.6.1.



(G-44) Fig. 4.6.1 : 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.

4.6.1 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.

4.6.2 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 :

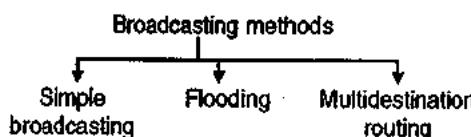
The routing that takes place inside an AS is called as interior routing.

Exterior routing :

The routing that takes place among various autonomous systems is called as exterior routing.

4.7 Broadcast Routing :

- In certain applications, the host has to send packets to many or all other hosts.
- If the sender send a packet to all destinations simultaneously then it is called as broadcasting.



(G-44) Fig. 4.7.1 : Various methods of broadcasting

- Various methods of broadcasting are as follows :

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 :

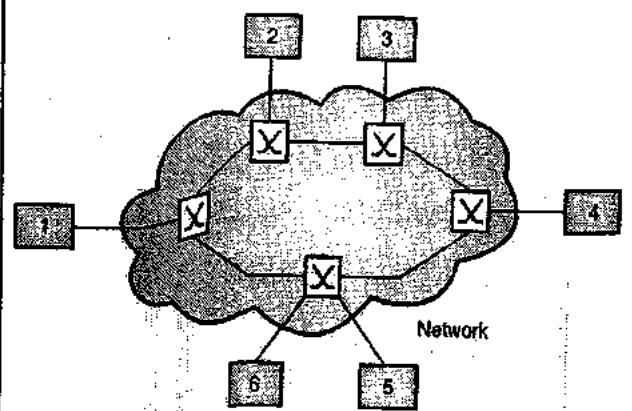
- Flooding is another method used for broadcasting. The problem with flooding is that it has a point to point routing algorithm.
- So it consumes a lot of bandwidth and generates too many packets.

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.

4.8 Introduction to Switching :

- A network consists of many switching devices. In order to connect multiple devices, one solution could be to have a point to point connection between each pair of devices. But this increases the number of connections.
- The other solution could be to have a central device and connect every device to each other via the central device (Star topology).
- Both these methods are wasteful and impractical for very large networks. The other topologies also can not be used.



(G-61) Fig. 4.8.1 : Switched network

Hence a better solution is switching. A switched network is made of a series of interconnected nodes called switches.

Switch is a device that creates temporary connections between two or more devices. Fig. 4.8.1 shows a switched network.

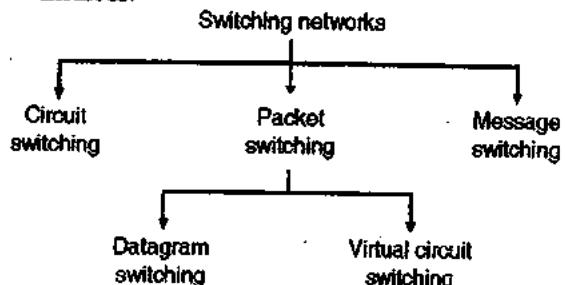
4.9 Switching Methods :

SPPU : Dec. 05, Dec. 11, Dec. 13

University Questions

- 1 Explain the switching techniques used in computer data communication. (Dec. 05, 8 Marks)
- 2 Explain different switching techniques. (Dec. 11, 6 Marks)
- 3 Explain the switching techniques used in computer data communication. (Dec. 13, 8 Marks)

- The three basic methods of switching are :
 1. Circuit switching
 2. Packet switching
 3. Message switching
- Out of these, the circuit and packet switching are commonly used today but the message switching has been phased out in general communication but is still used in the networking applications.
- Fig. 4.9.1 shows the classification of switching methods.



(L-617) Fig. 4.9.1 : Classification of switching methods

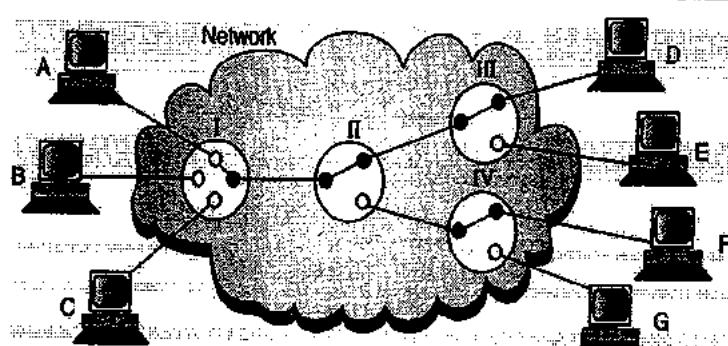
4.10 Circuit Switching Networks :

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

University Questions

- Q. 1 Explain the switching techniques used in computer data communication. (May 11, 8 Marks)
- Q. 2 Explain different switching techniques. (Dec. 11, 6 Marks)
- Q. 3 Explain the switching techniques used in computer data communication. (Dec. 13, 8 Marks)

- Circuit switching is used in public telephone networks. It was developed to handle voice traffic but it can also handle digital data.
- However circuit switching can not handle digital data efficiently.
- Using the circuit switching, a dedicated path is established between two stations for communication.
- The telephone network provide telephone service which involves the two way, real-time transmission of voice signals across a network.
- The network connection allows electrical current and the associated voice signal to flow between the two users. The end to end connection is maintained for the duration of the call.



(L-618) Fig. 4.10.1 : Circuit-switched network

- The telephone networks are connection oriented because they require the setting up of a connection before the actual transfer of information can take place.
- The transfer mode of a network that involves setting up a dedicated end to end connection is called circuit switching.
- In circuit switching the routing decision is made when the path is set up across the network. After the link has been set between the sender and receiver, the information is forwarded continuously over the link. After the link has been set up no additional address information about the receiver or destination machine is required.
- In circuit switching a dedicated path is established between the sender and the receiver which is maintained for the entire duration of conversation, as shown in Fig. 4.10.1.
- In telephone systems circuit switching is used. If circuit switching is used in computer networks the sending machine has to first establishes a link with the receiving machine.
- After the link is established the data is transmitted from the sender to the receiver. After the data flow stops, the link is released.
- In Fig. 4.10.1, I, II, III and IV are called as the switching nodes. They are used to connect one user to the other.
- The circuit switched networks operate in three phases :
 1. Set up phase
 2. Data transfer phase
 3. Tear down phase
- The circuit switching corresponds to the physical layer.
- Before starting communication in the setup phase the resources are reserved during communication. Some of these resources are channels, switch buffers, input/output ports etc.
- Data transferred between two stations is not in the packet form instead the data gets transferred continuously.
- No addressing is involved during the data transfer as the dedicated connection is established between the sender and receiver.

- The switches route the data on the basis of the allotted frequency band (FDM) or allotted time slot (TDM).

4.10.1 Three Phases :

- Communication via circuit switching takes place over three phases of operation as follows :
 1. Circuit establishment
 2. Data transfer
 3. Circuit disconnect. (tear down)

1. Circuit establishment :

- In a circuit switching network, before any signal is transmitted, it is necessary to establish an end-to-end (station to station) link.
- For example, in Fig. 4.10.1, if the communication is to be between A and D, then the path from A to node I to node II to node III and D has to be established first.
- The node to node links are usually multiplexed. They either use FDM or TDM.

2. Data transfer :

- The information can now be transferred from A to D through the network.
- The data can be analog or digital depending on the nature of network.
- Generally all the internal connections are duplex.

3. Circuit disconnect (tear down phase):

- After some time the connection between two users is terminated usually by the action of one or two stations.
- Circuit switching is inefficient in most of the applications.
- The entire channel capacity is dedicated for the duration of connection, even if the data is not being transferred.
- Once the circuit is established, the network is effectively transparent to the users with no delays involved.

4.10.2 Efficiency :

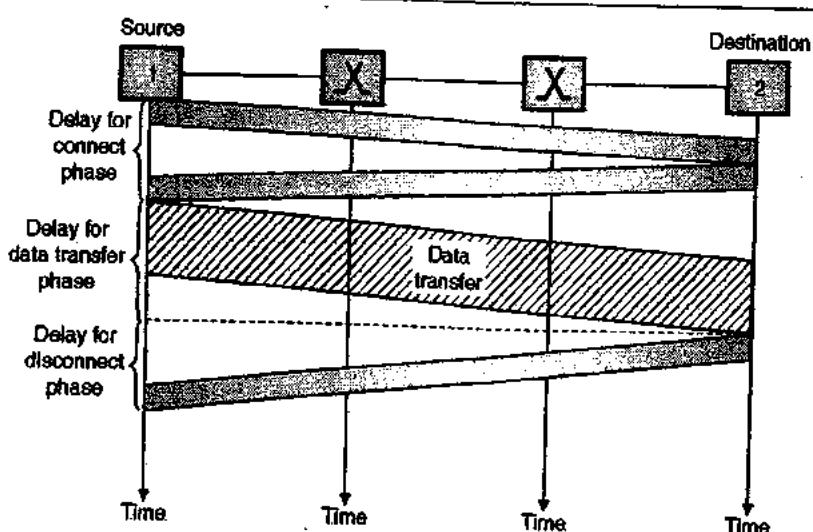
- In circuit switching the resources remain dedicated as long as a connection is alive.

Due to the allocation of resources during the entire duration of the connection, the efficiency of circuit switched networks is lower than the other two types of switching.

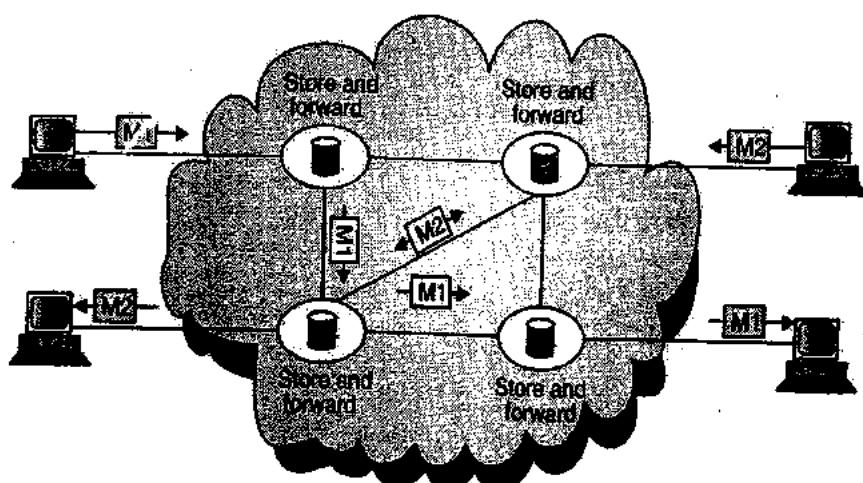
4.10.3 Delay :

- Eventhough the efficiency is low, the delay in this type of networks is very small.
- Fig. 4.10.2 explains the idea of delay in the circuit switched networks, when only two switches are used.
- During the data transfer the data is not delayed at any switch because there is no waiting time involved.
- The total delay is due to the time required for creating the connection, transfer data, and disconnect the connection.

- The delay at the time of set up is the sum of the following four parts :
 - The propagation time related to the request message of the source computer (slope of the first gray box in Fig. 4.10.2).
 - The time required for the transfer of request signal (height of the first gray box in Fig. 4.10.2).
 - The time taken by the acknowledgement from the destination computer to propagate back to source (slope of the second gray box in Fig. 4.10.2).
 - The propagation time required to transfer the acknowledgement from destination computer (height of second gray box.).



(L-619) Fig. 4.10.2 : Delay in circuit switching



(L-620) Fig. 4.11.1 : Message switching



- The delay corresponding to the data transfer phase is equal to the sum of the following two components :
 1. The propagation delay (slope of hatched portion) for data transfer.
 2. Time required to transfer data (height of hatched portion) which can be very long.
- The third component of delay is the delay corresponding to the disconnect or tear down phase. In Fig. 4.10.2 we have considered the situation in which the destination computer requests disconnection because this creates the maximum delay.

Application :

The circuit switching is used in the telephone networks.

4.10.4 Advantages :

1. The major advantage of circuit switching is that the dedicated transmission channel the computers establish provides a guaranteed data rate.
2. In circuit switching because of the dedicated path there is no delay in data flow.

4.10.5 Disadvantages :

1. The disadvantage of circuit switching is that, since the connection is dedicated it cannot be used to transmit any other data even if the channel is free.
2. Dedicated channels require more bandwidth.
3. It takes long time to establish connection.

4.10.6 Circuit Switched Technology in Telephone Networks :

- The telephone companies previously used the circuit switching technology for switching and routing a call. This was a physical layer technology.
- However, today the tendency is to use other switching techniques. For example the telephone number is used as the global address and a signalling system (called SS7) is used for creating and disconnecting the connections.

4.11 Telegraph Networks and Message Switching :

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

University Questions

- Q. 1 Explain the switching technologies used in computer data communication. (May 11, 8 Marks)**
- Q. 2 Explain different switching techniques. (Dec. 11, 6 Marks)**
- Q. 3 Explain the switching techniques used in computer data communication. (Dec. 13, 8 Marks)**

- In telegraphy the text message is encoded using the Morse code into sequences of dots and dashes. Each

dot or dash is communicated by transmitting short and long pulses of electrical current over a copper wire.

- In telegraph networks the text message is transmitted from the source telegraph office to the telegraph switching station. At this switching station an operator takes the decision of routing the message based on the destination address information. The operator will either forward the message if a communication line to the destination is free or store the message till the communication line becomes free.
- Message switching does not establish a dedicated path between two communicating devices. In message switching, each message is treated as an independent unit and includes its own destination and source address.
- Each complete message is then transmitted from device to device through the internetwork as shown in Fig. 4.11.1.
- Each intermediate device receives the message, stores it, until the next device is ready to receive it and then forwards it to the next device. For this reason, a message switching network is sometimes called as a store and forward network.
- Message switches can be programmed with information about the most efficient routes as well as information regarding neighbouring switches that can be used to forward messages to their ultimate destination.

4.11.1 Advantages :

1. It provides efficient traffic management by assigning priorities to the messages to be switched.
2. It reduces network traffic congestion because it is able to store message until a communication channel becomes available.
3. With message switching, the network devices share the data channels.
4. It provides asynchronous communication across time zones.

4.11.2 Disadvantages :

1. The storing and forwarding introduces delay hence cannot be used for real time applications like voice and video.
2. The intermediate devices require a large storing capacity since it has to store the message unless a free path is available.

4.12 Packet Switching :

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

University Questions

Explain the switching techniques used in computer data communication. (May 11, 8 Marks)

Explain different switching techniques. (Dec. 11, 6 Marks)

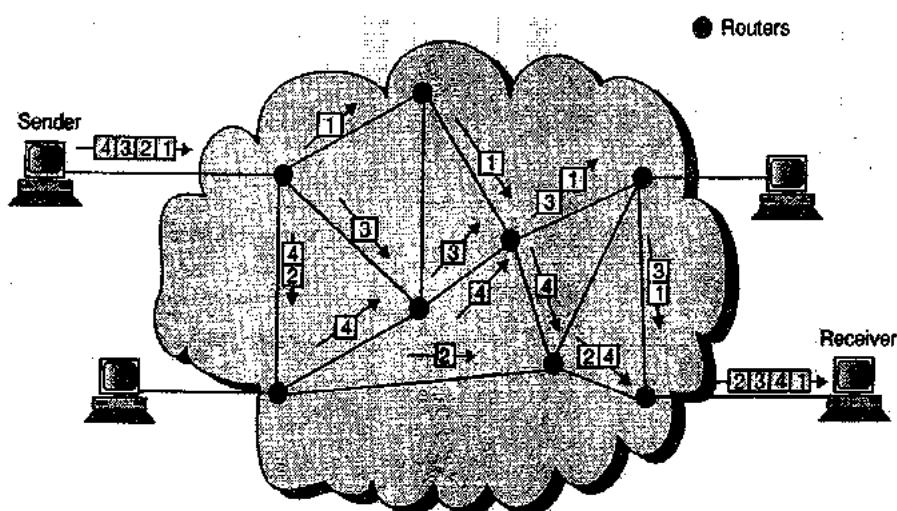
Explain the switching techniques used in computer data communication. (Dec. 13, 8 Marks)

- In packet switching, messages are broken up into packets. Each packet has a header with source, destination and intermediate node address information. The other part of the packet includes data load.
- Individual packets can take different routes to reach the destination. Independent routing of packets gives two advantages :
 - Bandwidth is reduced due to splitting data onto different routes in a busy circuit.
 - If a certain link in the network goes down during the transmission, the remaining packets can be sent through another route.
- The packets can arrive out of order at the receiver and have to be reassembled in proper sequence.
- In packet switching, the packet length is restricted to a certain maximum length. This length is short enough to allow the switching devices to store the packet data in memory.
- There are two methods of packet switching :
 - Datagram packet switching

- Virtual circuit packet switching.

4.12.1 Datagram Packet Switching :

- In this method a message is divided into a stream of packets. Each packet has its individually included address and treated as an independent unit with its own control instructions.
- The switching devices would route each packet independently through the network. Each intermediate node will determine the packet's next route segment.
- Before transmission starts, the sequence of packets and their destinations are communicated by exchanging control information between the sending terminal, the network and the receiving terminal.
- In packet switching, the resources are not allocated for any packet so there is no reserved bandwidth and no scheduled processing time allotted for each packet.
- No dedicated connection is established between the sender and receiver. The resource allocation is on demand and on the first come first serve basis.
- When a switch receives a packet, it has to wait if there are any other packets being processed. This will increase the delay.
- The datagram packet switching generally corresponds to the network layer. The packets are called as datagrams.
- Datagram packet switching is shown in Fig. 4.12.1.



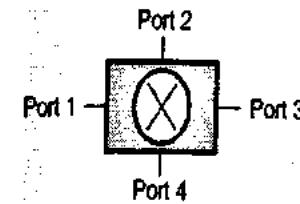
(L-623) Fig. 4.12.1 : Datagram packet switching



- In this circuit, four packets are to be delivered from the sender to receiver. The switches in the datagram network are called as routers.
- All the four packets (datagrams) belong to the same message in this circuit however actually they can get originated from any computer.
- The four datagrams, as shown in Fig. 4.12.1 may travel different paths to reach the destination. Due to this the packets may arrive out of order at the destination.
- The delay associated with each packet will be different as a result of the different paths followed by them. The datagrams may get lost or dropped out due to lack of resources.
- The upper layer protocols are supposed to reorder the received datagrams or ask for the lost ones before passing them on the application.
- The datagram networks, are called as the connectionless networks. This is because the switch (packet switch) does not keep any information about the connection state. There are no connection set up or tear down processes in the packet switching networks.

4.12.2 Routing Table :

- In packet switched networks, each packet switch has a routing table. This table contains the destination address.
- The routing tables are dynamic and their information is updated on periodic basis. The routing table consists of destination address and the corresponding output port over which the packet is to be forwarded as shown in Fig. 4.12.2:



(L-624) Fig. 4.12.2 : Router and Routing table

Destination address	Output port
1323	1
4360	2
9140	3
6436	4

Destination Address :

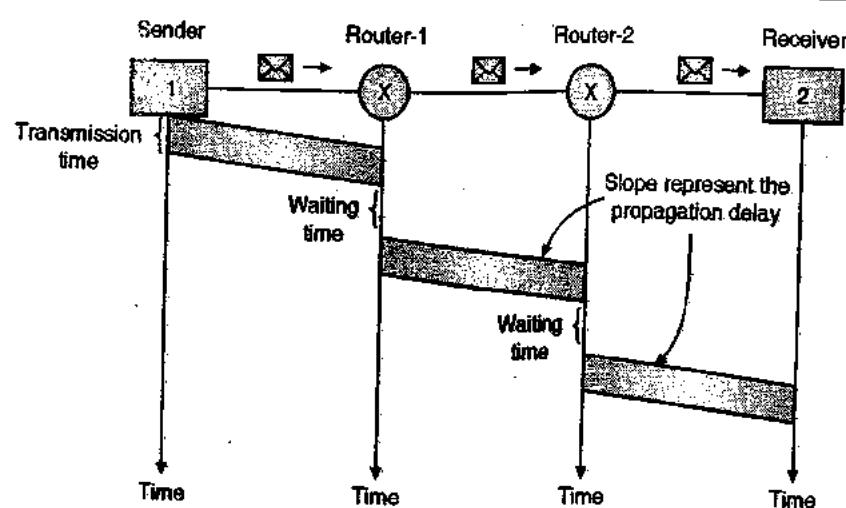
- Every packet in the datagram network consists of a header that contains the destination address where the packet is to be delivered and some additional information.
- When the router receives a packet, it examines the destination address of the packet and refers to its routing table to decide the port through which the packet is to be forwarded.
- For example in the routing table of Fig. 4.12.2, if the destination address on the received packet is 4360 then it will be forwarded through port 2.

4.12.3 Efficiency :

- As the resources are allocated only when the packets are to be transferred, the efficiency of datagram network is higher than that of the circuit switched network.

4.12.4 Delay :

- There are no set up or tear down phases in datagram circuit switching but each packet may have to wait at a switch before getting forwarded.



(L-625) Fig. 4.12.3 : Delay in datagram network

- All the packets in a message take different paths. Hence the delay associated with each packet is different.
- Fig. 4.12.3 illustrates the delays in a datagram network for one single packet.
- In Fig. 4.12.3, the packet travels through two switches while travelling from sender to receiver. The packet needs some transmission time (T) to travel from source to router 1. Then it has to wait for some time (w_1) before being forwarded.
- The total delay is made up of three transmission times ($3T$) and three propagation delays (3τ). The propagation delays correspond to the slopes of the lines as shown in Fig. 4.12.3 and the two waiting times w_1 and w_2 .
- ∴ Total delay = $3T + 3\tau + w_1 + w_2$... (4.12.1)
- The datagram switching is used in Internet.

4.12.5 Advantages of Packet Switching :

1. Greater line utilization efficiency, as a single node-to-node link can be dynamically shared by many packets over time.
2. A packet switching network can perform data-rate conversion.
3. When traffic becomes heavy on circuit switching network, some calls are blocked. On a packet switching network, packets are still accepted, but delivery delay increases.
4. Priorities can be used.
5. Each terminal in a group sharing the same physical circuit may be connected to a totally different destination. This versatility is one of the major strengths of packet switching.
6. No single user or large data block can tie up circuit or node resources indefinitely, making it well suited for interactive traffic.
7. Data protection against corruption or loss, errors are corrected by retransmission.
8. Users can select different destinations for each virtual call, overcoming the inflexibility of point to point dedicated networks.
9. Simultaneous calls allow PC users to access multiple windows to different remote applications.
10. Since many users can share transmission resources efficiently, the cost of intermittent data communication is reduced.

11. New calls can be added and old ones disconnected without affecting other users.

4.12.6 Disadvantages of Packet Switching :

1. Increased delay due to following reasons :
 - (a) Transmission delay = Length of packet divided by incoming channel rate.
 - (b) Variable delay due to processing and queuing.
2. The amount of overall packet delay can vary substantially (jitter) due to the following reasons :
 - (a) Packets may vary in length.
 - (b) Packets may take different routes.
 - (c) Packets are subject to varying delays in switches.
 - (d) This is not good for real time applications.
3. Header overhead reduces capacity to carry user data.
4. More processing required at node.

4.12.7 Datagram Networks in Internet :

The internet uses the datagram approach to switching at the Network layer. The routing of packets in Internet takes place on the basis of the universal addresses defined in the network layer.

4.13 Virtual Circuit Packet Switching :

SPPU : Dec. 13

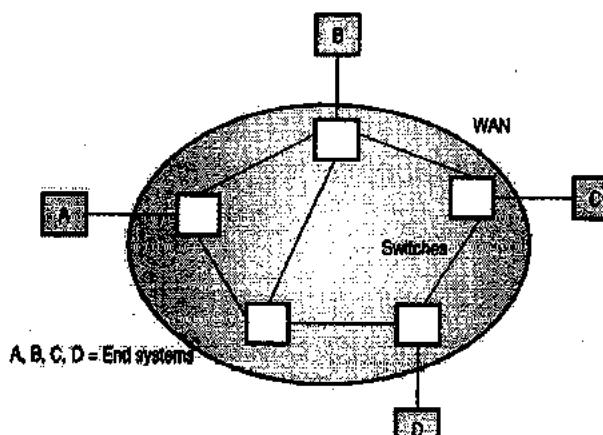
University Questions

Q.1 Explain the switching techniques used in computer data communication. (Dec. 13, 8 Marks)

- It establishes a logical connection between the sending and receiving devices called virtual circuit.
- The sending device and receiving device agree upon some important communication parameters, such as maximum message size and the network path to be taken. Once this virtual circuit is established the two devices use it for the rest of the conversation.
- In virtual circuit packet switching, all the packets travel through the virtual circuit established between the sending device and the receiving device.
- Virtual circuit switching has some characteristics of both circuit switched network and a datagram network.
- Similar to circuit switched network, there are setup and tear down phases alongwith the data transfer phase.



- It is possible to allocate the resources either in the set up phase similar to the circuit switched networks or as per requirement similar to the datagram networks.
- Similar to datagram networks, the data is sent in the form of packets. Each packet carries the address of the next switch and not the final destination address.
- Similar to circuit switching networks all the packets follow the same path established during the set up phase. That means packets don't take different paths to arrive at the destination.
- Virtual circuit corresponds to the data link layer.
- Fig. 4.13.1 shows the virtual circuit network. The network consists of switches which route the traffic from source to destination.



(L-62) Fig. 4.13.1 : Virtual circuit network

4.13.1 Addressing :

The virtual circuit networks use two types of addressing :

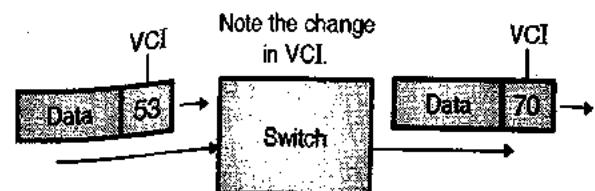
1. Global addressing
2. Local addressing (Virtual circuit Identifiers).

Global addressing :

- A source or destination can be a computer, router, bridge or any device which connects other networks such as LANs to the switched WAN.
- The source or destination must have a global address. This is a unique address.
- The global addressing in virtual circuit networks is used only for the creation of a virtual circuit identifier as explained below.

Virtual Circuit Identifier (VCI) :

- It is the identifier which is used for the actual data transfer and denoted by VCI.
- VCI is small number which is used by a frame between two switches.
- When a frame arrives at a switch, it contains one VCI (say 53) as shown in Fig. 4.13.2 but when the frame leaves that switch it contains another VCI (70) as shown.



(L-62) Fig. 4.13.2 : VCI

4.13.2 Three Phases of Communication :

- A source and destination have to undergo three phases to communicate between each other.
- The three phases are :
 1. Set up
 2. Data transfer
 3. Teardown

Set up phase :

In this phase the source and destination use their global addresses. This will help switches to make table entries for the connection.

Data transfer :

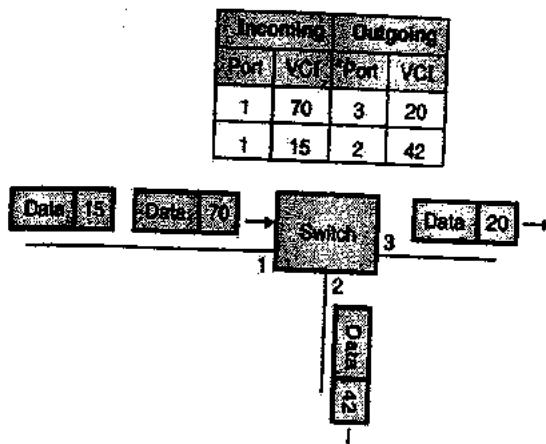
The data transfer is the second phase in which the frames are transferred from source to destination.

Teardown :

- In the teardown phase both source and destination will communicate the switches to erase the corresponding entry.
- Let us discuss these phases one by one.

Data transfer phase :

- For this phase all the switches need to have a table entry for this particular virtual circuit. Such a table has four columns.
- Fig. 4.13.3 shows such a switch and its table. The switch has three ports with port 1 acting as the incoming port while ports 2 and 3 as outgoing ports.
- A frame with VCI of 70 arrives at port 1. The switch scans its table to find port 1 and VCI 70.



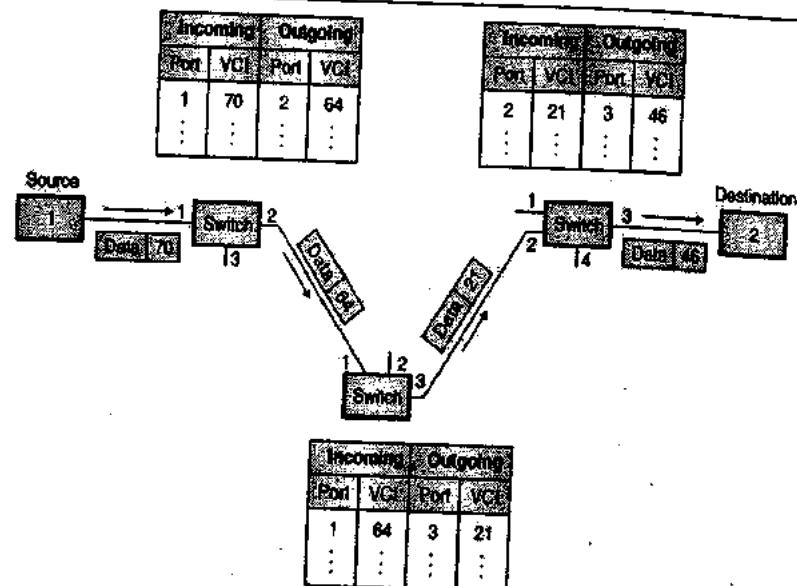
(L-628) Fig. 4.13.3 : Switch and its table

- After finding them, the switch knows that the VCI should be changed to 20 and send out the frame from port 3.

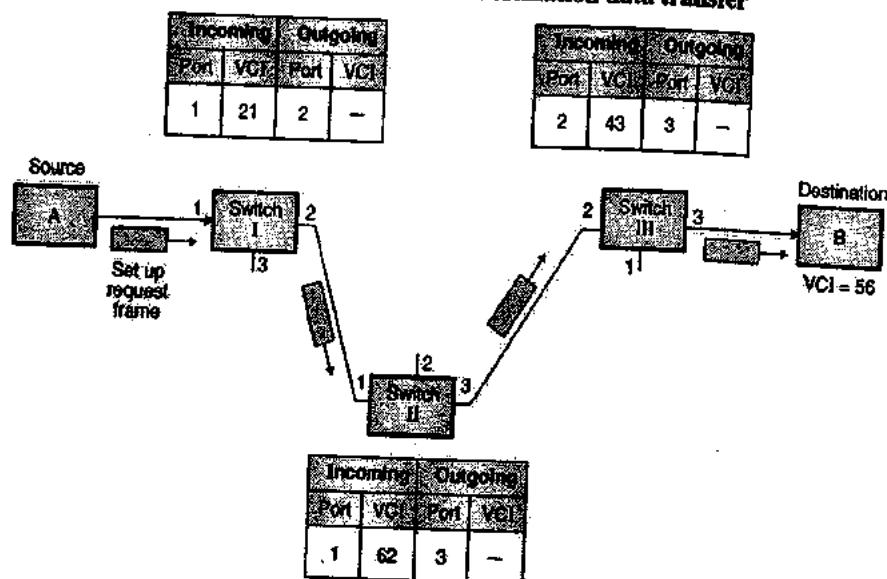
- Similarly the incoming frame with VCI 15 is sent out on port 2 with a new VCI 42 as shown in Fig. 4.13.3.

Source to destination data transfer :

- Fig. 4.13.4 shows the actual data transfer taking place between source 1 and destination 2.
- It shows how the VCI of a frame is changed by each switch for routing it from source to destination.
- The data transfer phase is active as long as the source is sending its frames to destination.
- The procedure followed by each switch is same for each frame of the message being communicated.
- This process creates a virtual circuit which is not real to connect a source to destination.



(L-629) Fig. 4.13.4 : Source to destination data transfer



(L-630) Fig. 4.13.5 : SVC set up request

Set up phase :

- In the set up phase a switch creates an entry for a virtual circuit by following one of the two approaches given below :
 - Permanent Virtual Circuit (PVC) approach
 - Switched Virtual Circuit (SVC) approach.

Permanent Virtual Circuit (PVC) :

- The PVC is like a leased telephone line between two parties. One party can pick up the phone and talk to the other one without dialling.
- A source and destination should choose to have a PVC between them.
- Then the corresponding table entries are recorded for all the switches by the administrator remotely and electronically.
- An outgoing VCI number is allotted to the source and incoming VCI number is allotted to the destination.
- This VCI number will always be used by this source to send frames to a particular destination.

Disadvantages of PVC :

- Following are the disadvantages of PVC :
 - PVC is costly because the connection always remains established between two parties whether it is required or not.
 - We need to create many PVCs from a source to different destinations.
- To overcome these disadvantages, the other approach (SVC) is tried.

Switched Virtual Circuit (SVC) :

- In SVC a temporary connection is established between the source and destination.
- This connection exists only when the data is to be transferred.
- When source A wants to establish a virtual circuit with destination B then the following two steps are to be followed :
 - Set up request

2. Acknowledgement.

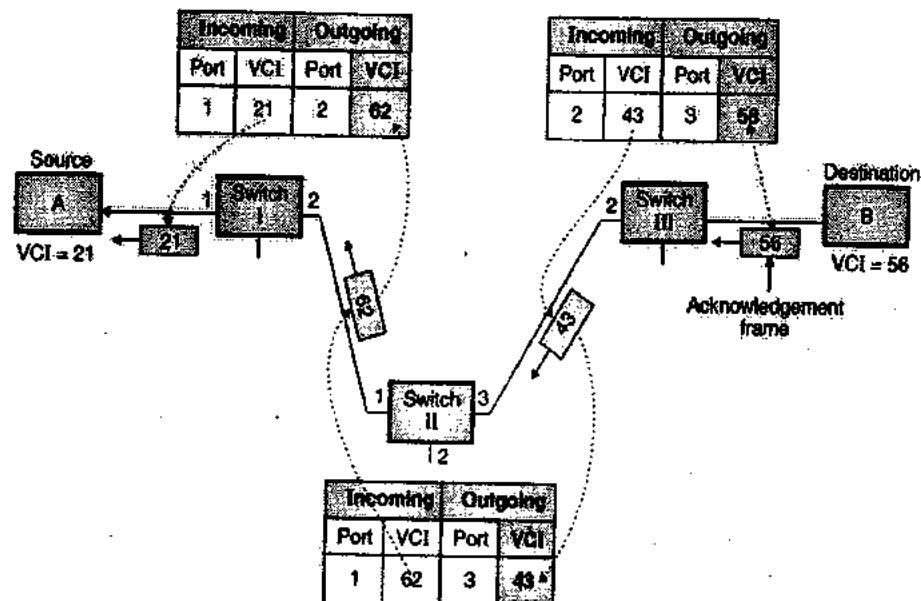
- Let us discuss the sequence of events taking place in these steps.

Set up request :

- The source A sends a set up request frame to the destination via various switches as shown in Fig. 4.13.5.
- The events take place in the following sequence after that :
 - Source A sends a set up frame to switch - I.
 - Each switch acts as a router. Switch I has a routing table which is different from the switching table. The switch creates an entry in its table for this virtual circuit but it can fill up only 3 columns out of 4, namely incoming port 1, VCI 21 and outgoing port 2. It does not know the outgoing VCI because it is found in the acknowledgement step. The set up frame is forwarded to switch II.
 - Switch II receives the set up request frame and same events will take place as those happened at switch I. Three columns are filled : incoming port 1, VCI 62 and outgoing port 3.
 - Switch III receives the set up request frame from switch II. Here also the three columns are filled as : incoming port 2, VCI 43 and outgoing port 3.
 - Destination B receives the set up request frame. If it is ready to receive frames from source A, then a VCI is assigned to the frames coming from A. In this case the VCI is 56. This VCI is an indication that frames come from A and not from any other source.

Acknowledgement :

- The acknowledgement frame is sent from the destination B to source A via the three switches. This completes the entries in the switching tables.
- The acknowledgement process is illustrated in Fig. 4.13.6.



(a-63) Fig. 4.13.6 : SVC acknowledgement

- The sequence of events is as follows :
 - Destination B sends an acknowledgement frame to switch III. This frame contains the global source and destination address and VCI 56. Switch III fills this number into the fourth column of its routing table.
 - Switch III sends the acknowledgement to switch II that contains its incoming VCI = 43. Switch II fills this into its table as outgoing VCI as shown in Fig. 4.13.6.
 - Switch II sends an acknowledgement to switch I which contains its incoming VCI = 62. Switch I fills this into its switching table as outgoing VCI.
 - Switch I sends the acknowledgement which contains its incoming VCI = 21.
 - Source A uses it as the outgoing VCI for all the data frames directed to destination B.

Teardown phase :

- When source A sends all the frames to destination B, the data transfer phase is over.
- Then A sends a special frame called teardown request to B.
- B will respond to it with a teardown confirmation frame, after which all the switches erase the corresponding entry from their tables and the connection will be destroyed.

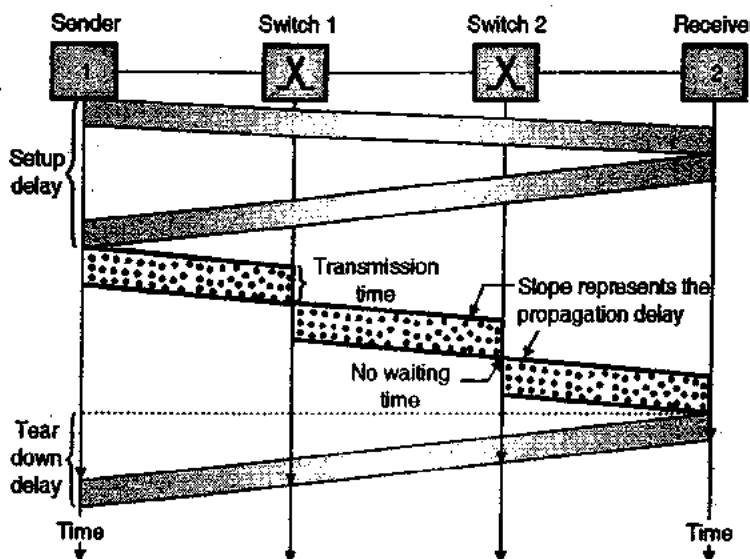
4.13.3 Efficiency :

- In the virtual circuit networks, the resources can be either allocated during the set up phase or they can be allocated on demand during the data transfer phase.
- Even though resources are allocated on demand, it is possible for the source to check the availability of resources, without actually reserving them. This is a big advantage as it saves a lot of time and effort. This increases the efficiency of the virtual circuit network.

4.13.4 Delay :

- Different delays in virtual circuit networks are illustrated in Fig. 4.13.7.
- One component of delay is the time delay for set up phase. The other component is the time delay corresponding to the tear down phase.
- If the resources are allocated during the set up phase, then there is no waiting delays for individual packets.
- In Fig. 4.13.7, as there are two routers, there are three transmission times ($3T$), three propagation times (3τ) as signal will be transmitted thrice, corresponding to the three different segments of networks, data transfer delay, a set up delay and finally the delay corresponding to the tear down phase.

$$\begin{aligned} \therefore \text{Total delay} &= 3T + 3\tau + \text{Set up phase delay} \\ &\quad + \text{Tear down delay} \end{aligned}$$



(L-632) Fig. 4.13.7 : Delays in virtual circuits

4.13.5 Circuit Switched Technology in WANs :

The virtual circuit networks are used in switched WANs such as Frame Relay and ATM networks.

4.13.6 Advantages of Virtual Circuit Packet Switching :

- Virtual circuit packet switching uses abbreviated headers and hardware based table lookup, which allows fast processing and forwarding of packets.
- In the virtual circuit packet switching, resources can be allocated during connection setup.
- The number of bit required in the header is much smaller than the number required to provide full destination network addresses. This reduces the wastage of transmission bandwidth.
- Virtual circuit packet switching uses Virtual-Circuit Identifier (VCI) which uses to identify connection and to specify the type of priority given to the packet by scheduler that controls the transmissions in next output port.
- The efficiency of virtual circuit packet switching is high.

4.13.7 Disadvantages of Virtual Circuit Packet Switching :

- The switches in the network need to maintain information about the flows they are handling. The amount of required 'state' information grows very quickly with number of flows.
- In the case of fault occurs in the network, all affected connections must be set up again.

- Connection setup is not possible, if the switch is unable to handle the volume of traffic allowed or link utilization exceeds certain thresholds.

4.13.8 Comparison of Datagram and Virtual Circuits :

Circuit switching	Datagram packet switching	Virtual-circuit packet switching
Dedicated transmission path	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of packets	Transmission of packets
Fast enough for interactive	Fast enough for interactive	Fast enough for interactive
Messages are not stored	Packets may be stored until delivered	Packets stored until delivered
The path is established for entire conversation	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Packet transmission delay	Call setup delay; packet transmission delay

Circuit switching	Datagram packet switching	Virtual circuit packet switching
Busy signal if called party busy	Sender may be notified if packet not delivered	Sender notified of connection denial
Overload may block call setup; no delay for established calls	Overload increases packet delay	Overload may block call setup; increases packet delay
Electromechanical or computerized switching nodes	Small switching nodes	Small switching nodes
User responsible for message loss protection	Network may be responsible for individual packets	Network may be responsible for packet sequences
Usually no speed or code conversion	Speed and code conversion	Speed and code conversion
Fixed bandwidth transmission	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each message	Overhead bits in each packet

4.14 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.

4.15 Routing Algorithms :

SPPU : Dec. 09

University Questions

- Q. 1 Write short notes on : Routing algorithm.

(Dec. 09, 8 Marks)

- One of the important functions of the network layer is to route the packets from the source machine to the destination machine.
- Routing algorithm** is a part of network layer software. It is responsible for deciding the output line (port) over which a given packet is to be sent.
- Such a decision is dependent on whether the subnet is a virtual circuit or it is datagram switching.

4.15.1 Desired Properties of a Routing Algorithm :

SPPU : Dec. 13

University Questions

- Q. 1 What are design principles of good routing algorithm ?

(Dec. 13, 8 Marks)

- A routing algorithm is supposed to have the following properties :
 - Optimality.
 - Fairness
 - Robustness
 - Stability
 - Correctness

4.15.2 Types of Routing Algorithms :

SPPU : Dec. 11

University Questions

- Q. 1 Classify routing algorithms

(Dec. 11, 4 Marks)

- Routing algorithms can be divided into two groups :
 - Non-adaptive (static) algorithms.
 - Adaptive (dynamic) algorithms.

1. Non-adaptive (static) 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. So the choice of routing cannot be changed in this event of congestion or link failure.
- This is called as static routing or non-adaptive routing.

2. Adaptive (dynamic) algorithms :

- For these algorithms the routing decision can be changed dynamically if there are any changes in topology or traffic etc.

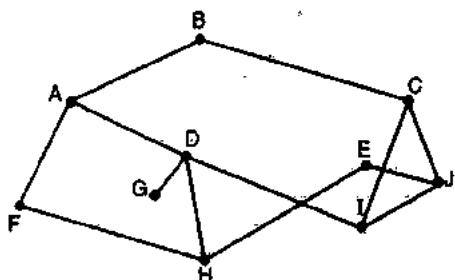
- This is called as dynamic routing.
- In the following sections we are going to discuss various static and dynamic algorithms.

4.15.3 Optimality Principle :

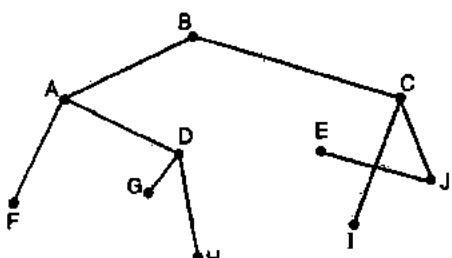
- A general statement about optimality is called as optimality principle.
- It states that if router J is on the optimal path from router I to router K, then the optimal path from J to K will also be along the same route.

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. 4.15.1. 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. 4.15.1, the distance metric is the number of hops. In Fig. 4.15.1(b) a sink tree for router B has been shown. The paths from B to every router with minimum number of hops.



(a) A subnet

(b) A sink tree for router B
(G-450) Fig. 4.15.1

4.16 Static (Non adaptive) Algorithms :

SPPU : Dec. 06

University Questions

- Q.1** Mention the different routing algorithms. Give difference between static and dynamic routing algorithm with suitable example.

Dec. 06 - 8 Marks

The examples of static algorithms are :

1. Shortest path routing.
2. Flooding.
3. Flow based routing.

4.16.1 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 queueing 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.

4.16.2 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.

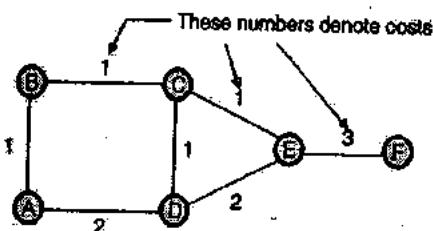
As stated earlier we define two sets P (permanent) and T (temporary) of the nodes. In set P we have nodes to which the shortest path has already been found and in set T we have nodes to which we are considering the shortest paths.

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 :
 1. 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.
 2. 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.
3. 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.
4. Stop when T is empty.

This algorithm will be clear after solving the following example.

Ex. 4.16.1 : For the network shown in Fig. P. 4.16.1(a), show the computations at node A using the Dijkshtra's algorithm.



(G-451) Fig. P. 4.16.1(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. 4.16.1(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. 4.16.1(a).

(G-451(a)) Table P. 4.16.1(a)

Permanent (P)	Temporary (T)
A	B(A,1),D(A,2)

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. 4.16.1(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. 4.16.1(b).

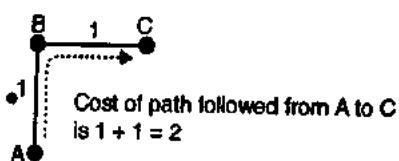
(G-452) Table P. 4.16.1(b)

Permanent (P)	Temporary (T)
A	B(A,1),D(A,2)
A,B(A,1)	D(A,2),C(B,2)

A

A — 1 — B

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. 4.16.1(b).



(G-453) Fig. P. 4.16.1(b)

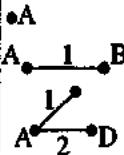
Step 3 :

- Now pick up the neighbour in T set with the smallest cost in Table P. 4.16.1(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. 4.16.1(c). Note that C(B,2) goes as it is, and E(D,4) is a new entry to Table P. 4.16.1(c). But C(D,3) can not be entered because its cost is 3.



(G-454) Table P. 4.16.1(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)

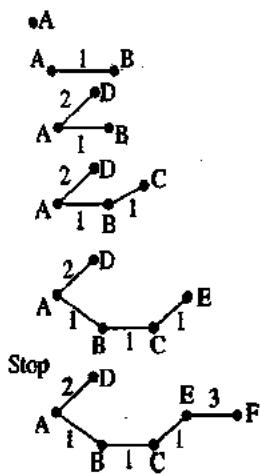


Where E(D,4) means E is reached by A via D and the cost is 4.

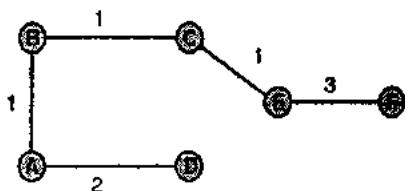
- Similarly we can proceed further. The final table is as shown in Table P. 4.16.1(d).

(G-455) Table P. 4.16.1(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),C(B,2)	E(C,3) E(D,4) can not be included
A,B(A,1), D(A,2),C(B,2), E(C,3)	F(E,6) 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)

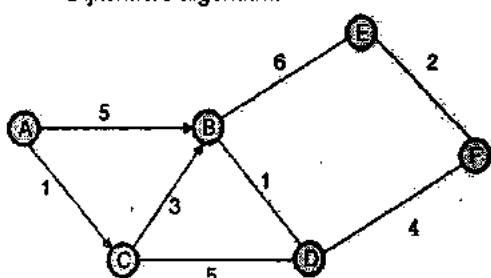


- The shortest paths from A to all other nodes are as shown in Fig. P. 4.16.1(c).



(G-456) Fig. P. 4.16.1(c) : Shortest paths from A to all other nodes

Ex. 4.16.2 : For the network shown in Fig. P. 4.16.2(a) show the computations at node A using the Dijkshtra's algorithm.



(G-457) Fig. P. 4.16.2(a) : Given network

Soln. :

Step 1 :

- The starting node is A. Enter it in to group P as shown in Table P. 4.16.2(a).
- Add the neighbours B and C to the temporary group T.

(G-457(a)) Table P. 4.16.2(a)

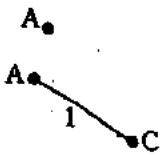
Permanent (P)	Temporary (T)
A	B(A,5),C(A,1)

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. 4.16.2(b).

(G-458) Table P. 4.16.2(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)



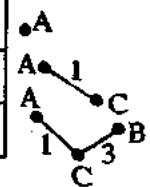
- B(C, 4) is another entry in T group which shows that B is approached by A via C and the cost is 4.

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. 4.16.2(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. 4.16.2(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)

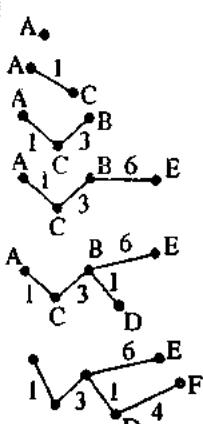


Step 4 :

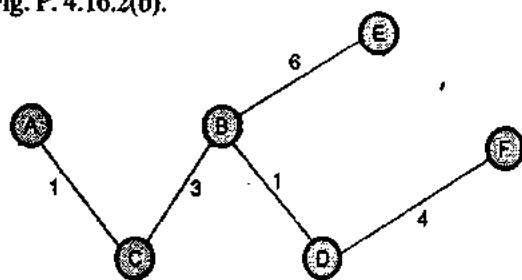
- Now continue in the same manner to get the final table as shown in Table P. 4.16.2(d).

(G-46) Table P. 4.16.2(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)



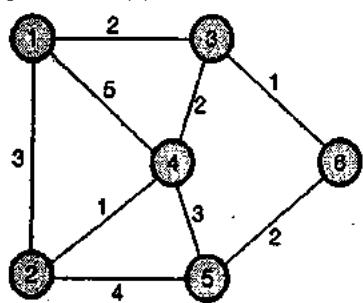
- The shortest path from A to other nodes is shown in Fig. P. 4.16.2(b).



(G-46) Fig. P. 4.16.2(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. 4.16.3 : Write Dijkstra's algorithm. Find shortest path Fig. P. 4.16.3(a) to destination node 6.



(G-183) Fig. P. 4.16.3(a)

Soln. : For Dijkstra's algorithm refer section 4.16.2.

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. 4.16.3(a).
- Add neighbours B, C and D to the temporary group T.

Table P. 4.16.3(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. 4.16.3(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.

Table P. 4.16.3(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. 4.16.3(c).

Table P. 4.16.3(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. 4.16.3(d).

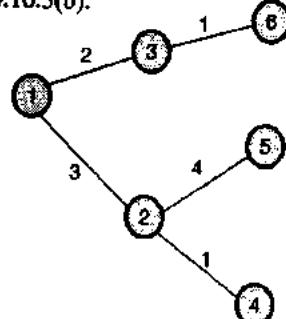
Table P. 4.16.3(d) : Final table

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)



Permanent (P)	Temporary (T)
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. 4.16.3(b).



(G-1384) Fig. P. 4.16.3(b) : Shortest path from 1 to all other nodes

4.16.3 Flooding :

SPPU : May 10

University Questions

- Q. 1 Explain the following routing algorithm with example
Flooding routing algorithm.

(May 10, 8 Marks)

- 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.

4.17 Dynamic Routing Algorithms :

SPPU : Dec. 06

University Questions

- Q. 1 Mention the different routing algorithms. Give difference between static and dynamic routing algorithm with suitable example. (Dec. 06, 8 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.

4.17.1 Distance Vector Routing Algorithm :

SPPU : May 08, May 12, Dec. 12, May 13

University Questions

- Q. 1 Explain the distance vector routing algorithm.

(May 08, 9 Marks)

- Q. 2 Explain in detail working principle behind Distance Vector and link State routing.

(May 12, 10 Marks)

What is the difference between forwarding and routing? Describe link state routing algorithm.

(Dec. 12, 8 Marks)

What are the drawbacks of Distance Vector Routing (DVR) and the solutions to recover them?

(May 13, 8 Marks)

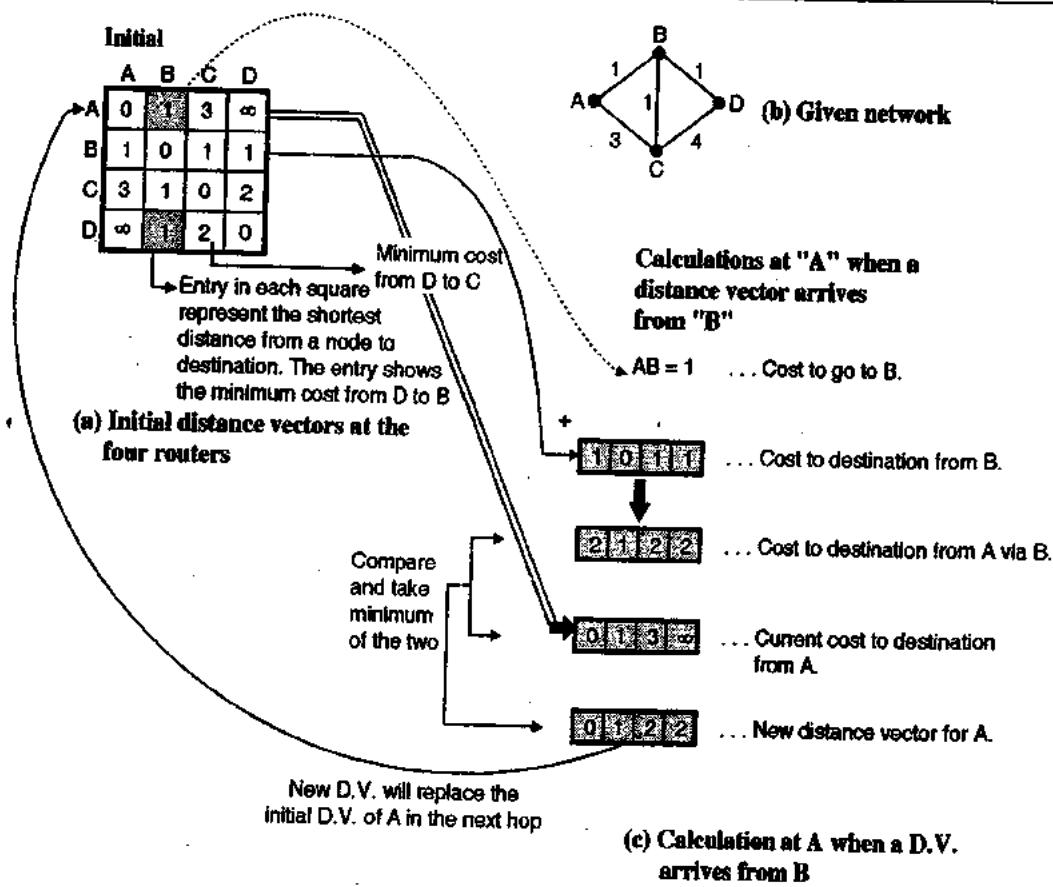
- In this algorithm, each router maintains a table called vector, such a table gives the best known distance to each destination and the information about which line to be used to reach there.
- This algorithm is sometimes called by other names such as,
 - Distributed Bellman-Ford routing algorithm.
 - 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 :
 - The first part shows the preferred outgoing line to be used to reach the specific destination.
 - 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. 4.17.1.

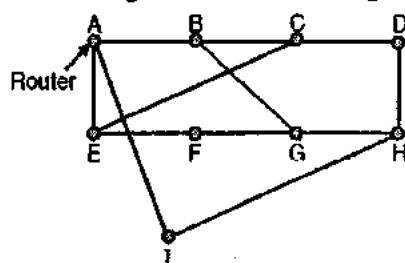


(G-43) Fig. 4.17.1 : Distance vector algorithm at router A

- Fig. 4.17.1 shows how the D.V. at A is automatically modified when a D.V. is received from B.
- A similar calculation takes place at the other routers as well. So the entries at every router can change. In Fig. 4.17.1(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.

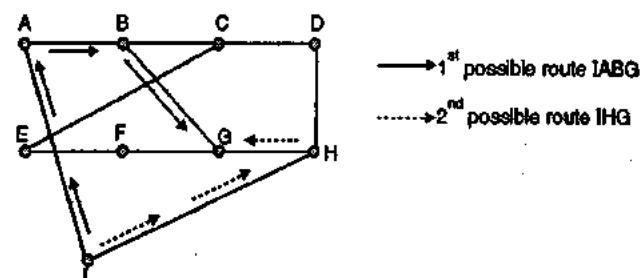
Routing procedure in distance vector routing :

- The example of a subnet is shown in Fig. 4.17.2(a) and the routing tables are shown in Fig. 4.17.2(b).



(G-46) Fig. 4.17.2(a) : A subnet

- The entries in router tables of Fig. 4.17.2(b) are the delay vectors. For example consider the shaded boxes of Fig. 4.17.2(b).
- 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. 4.17.2(c) shows the two possible routes between I and G.



(G-46) Fig. 4.17.2(c)

This shows that the delay from A to B is 10 mS

This shows that the delay from A to D is 38 mS

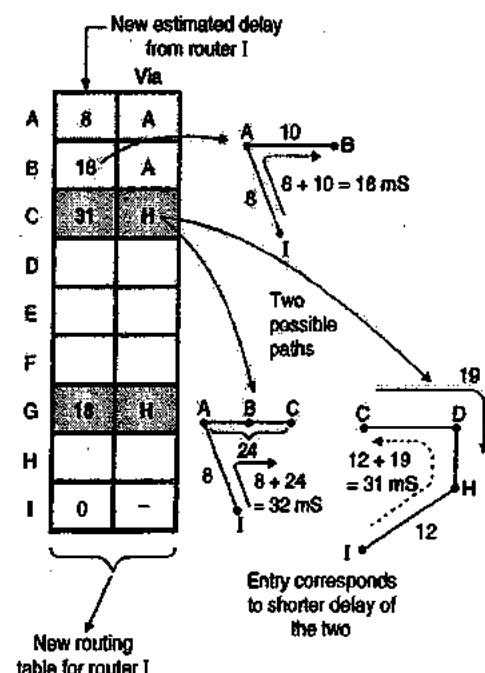
To	A	H
A	0	20
B	10	31
C	24	19
D	38	8
E	12	30
F	24	19
G	16	6
H	19	0
I	9	7

Delay vectors

Delay is 8

Delay is 12

Vectors received from I's two neighbours



(G-46) Fig. 4.17.2(b) : Routing tables

- I know that the reach G via A, the delay required is :

$$\begin{array}{ll} I \text{ to } A & \text{Delay} = 8 \text{ mS} \\ A \text{ to } G & \text{Delay} = 16 \text{ mS} \end{array} \left. \begin{array}{l} \therefore I \text{ to } G \\ \text{Delay} = 8 + 16 \\ = 24 \text{ msec} \end{array} \right\}$$

- Whereas the delay between I and G via H (route IHG) is :

$$\begin{array}{ll} I \text{ to } H & \text{Delay} = 12 \text{ mS} \\ H \text{ to } G & \text{Delay} = 6 \text{ mS} \end{array} \left. \begin{array}{l} \therefore I \text{ to } G \\ \text{Delay} = 12 + 6 \\ = 18 \text{ msec} \end{array} \right\}$$

- 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. 4.17.2(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.

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.

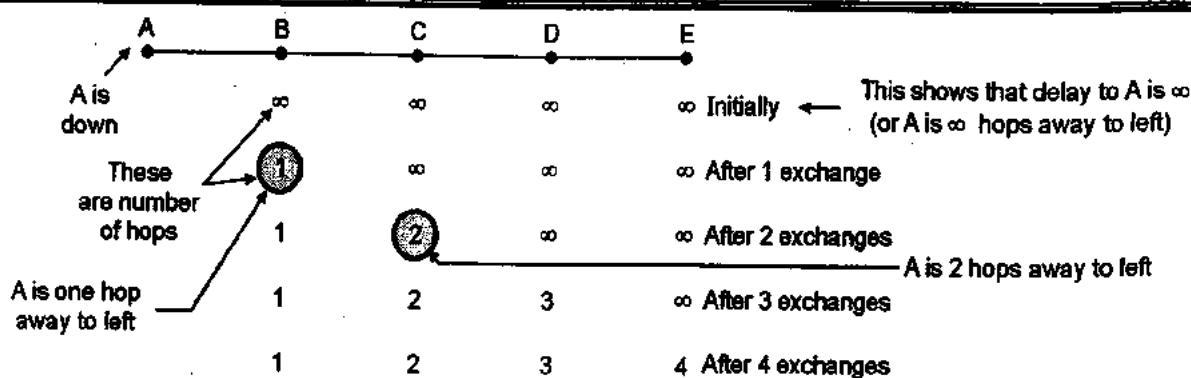
4.17.2 Count to Infinity Problem :

SPPU : Dec. 06

University Questions

- Q. 1** What is count to infinity problem ? Explain with suitable example. (Dec. 06, 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. 4.17.3 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. 4.17.3(a), B makes an entry in its routing table that A is one hop away to the left.
- All the other routers still think that A is down. So in the second row of Fig. 4.17.3(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.



(G-467) Fig. 4.17.3(a)

A	B	C	D	E	
	1	2	3	4	Initially ∞ 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	8	7	6	After 5 exchanges
	7	8	7	8	After 6 exchanges
	∞	8	∞	∞	

(G-468) Fig. 4.17.3(b)

- So after the second vector exchange the entries in the third row of Fig. 4.17.3(a) are :

A	B	C	D	E	
	1	2	∞	∞	After 2 exchanges

(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. 4.17.3(b) :

- Now refer Fig. 4.17.3(b). Here initially all routers are OK. The routers B, C, D and E have distances of 1, 2, 3 and 4 respectively to A. So the first row of Fig. 4.17.3(b) is as follows :

A	B	C	D	E	
	1	2	3	4	Initially First row of Fig. 4.17.3(b)

These are distances of B,C,D,E to A

(G-468(b))

- 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.

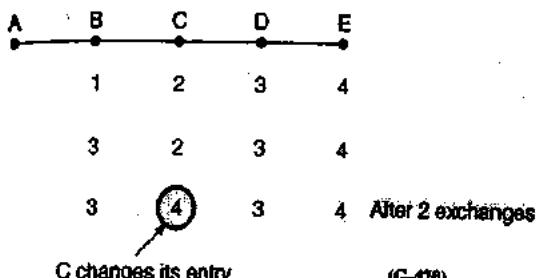
- So B thinks that it can reach A via C with a path length 3. (B to C 1 hop and C to A 2 hops) so it accordingly updates its routing table. But D and E do not update their entries. So the second row of Fig. 4.17.3(b) looks as follows :

A	B	C	D	E	
	1	2	3	4	Initially
	3	2	3	4	After 1 exchange

Updated entry

No change

- 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. 4.17.3(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. 4.17.3(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.

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.

4.17.3 Link State Routing :

SPPU : Dec. 06, May 12

University Questions

- Q.1** Discuss the link state routing algorithm with example. (Dec. 06, 8 Marks)
- Q.2** Explain in detail working principle behind distance vector and link state routing. (May 12, 10 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 :

- Each router should discover its neighbours and obtain their network addresses.
- Then it should measure the delay or cost to each of these neighbours.
- It should construct a packet containing the network addresses and the delays of all the neighbours.
- Send this packet to all other routers.
- 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.

4.17.4 Comparison of Link State Routing and Distance Vector Routing :

SPPU : Dec. 11, Dec. 15

University Questions

- Q.1** Compare link state and distance vector routing algorithm. (Dec. 11, 4 Marks, Dec. 15, 8 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.



4.18 Hierarchical Routing :

SPPU : May 10, Dec. 11, Dec. 12, May 13

University Questions

- Q. 1 Explain the following routing algorithm with example
Hierarchical routing algorithm.** (May 10, 8 Marks)
- Q. 2 Explain hierarchical routing. How is it implemented in internet ?** (Dec. 11, 8 Marks)
- Q. 3 Explain in brief hierarchical routing and discuss its advantages.** (Dec. 12, 8 Marks)
- Q. 4 Explain hierarchical routing in detail.** (May 13, 8 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

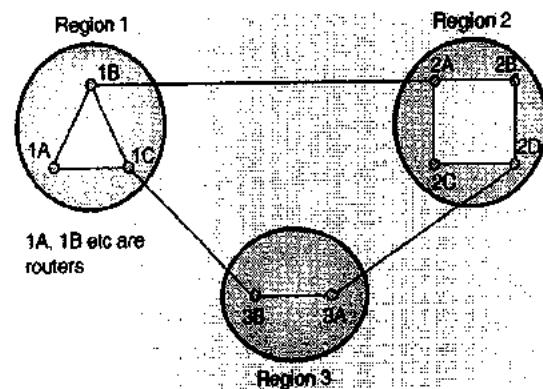
Level 2 : Clusters : it is a group of regions.

Level 3 : Zones : zone is a group of clusters.

Level 4 : Groups : group contains many zones.

Two level hierarchical routing :

- For networks of smaller size, a two level hierarchical routing is sufficient.
- Fig. 4.18.1(a) shows network containing 3 regions. Fig. 4.18.1(b) shows the full routing table of router 1A which has 9 entries because in all there are 9 routers.



(G-47) Fig. 4.18.1(a) : A network

Now with a two level hierarchical routing, the routing table of the same router reduces to a much smaller size as shown in Fig. 4.18.1(c). This table has only 5 entries.

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

(b) Full routing table for router 1A

Hierarchical routing table

For 1 A

Destination	Line	Hops
Region 1	1 A	-
	1 B	1
	1 C	1
Region 2	→	2
Region 3	→	3

(c) Hierarchical routing table for router 1A

Fig. 4.18.1

- In the hierarchical table of Fig. 4.18.1(c), there are entries for all local routers (1A, 1B and 1C) belonging to the region of 1A 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 1B-2A line as shown by the shaded entry in Fig. 4.18.1(c). Similarly all the traffic from 1A to region 3 is routed through the line 1C-3B.
- Comparison of Figs. 4.18.1(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.

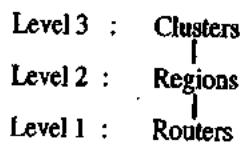
How many levels a hierarchy should have ?

Karnoun 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. 4.18.1: 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 ?

Soln. :

- The three level hierarchy has got the three levels as shown in the following diagram.



- 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.

\therefore Total number of entries in the router table

$$= (x - 1) + (y - 1) + z$$

$$= x + y + z - 2$$

- As an example, the 4800 routers mentioned in this example may be divided into 10 clusters ($x = 10$), 20 regions in each cluster ($y = 20$) and 24 routers in each region ($z = 24$). So that,

$$x \times y \times z = 10 \times 20 \times 24 = 4800$$

For this arrangement the number of entries in a router table would be,

$$\text{Entries} = x + y + z - 2$$

$$= 10 + 20 + 24 - 2 = 52$$

- It is possible to find the values of x , y and z by trial and error to minimize the number of entries.

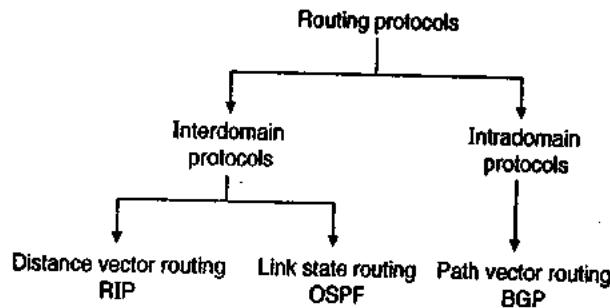
4.19 Intra and Interdomain Routing :

SPPU : May 12

University Questions

Q.1 What is AS ? What are Intra Domain routing protocols ? Explain one Inter Domain routing protocol. (May 12, 6 Marks)

- The size of the Internet is so big that for one routing protocol it is impossible to handle the task of updating the routing tables of all the routers.
- Hence Internet is divided into a number of autonomous systems (AS). An autonomous system (AS) is a group of networks and routers and each one is controlled by a single administrator. An AS is shown in Fig. 4.19.1.
- The **Intradomain routing** is defined as the routing that takes place inside an autonomous system whereas the routing that takes place among various autonomous system is known as the **interdomain routing**.
- Several intradomain and interdomain protocols are used. They are as shown in Fig. 4.19.1.

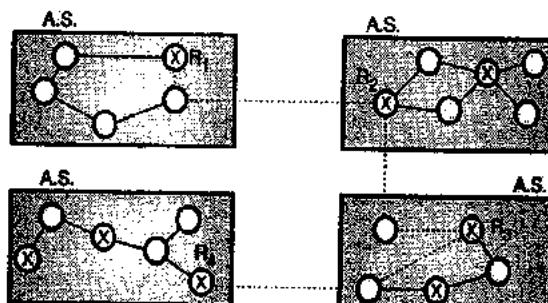


(G-129) Fig. 4.19.1 : Classification of routing protocols

- The examples of interdomain routing protocols are :
 - Distance vector routing
 - 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.



(G-129) Fig. 4.19.2 : Autonomous systems

4.20 Internetworking :

- We have discussed the basic concepts in computer networking. An another very important concept is **Internetworking** which deals with connecting many computer networks together.
- A network of computer networks is known as **internetwork** or simply an Internet (note that i is small). The best example of an internetwork is Internet (note that I is capital).
- The difference between Networking and Internetworking may be states as follows : In networking all the devices (hosts) involved are compatible with each other. But in internetworking this may not be true.
- The networks that are being connected to each other through internetworking may or may not be compatible with each other, in many respects.
- For example the networks which are to be connected to form an internetwork can be an Ethernet, a token ring LAN and a WAN. All these networks are entirely different from each other, in terms of their topologies, signaling, transmission mechanism, wiring etc.
- Therefore in internetworking it is a challenge to handle these incompatibilities and bring all these networks together.

- The Internet is the biggest network of computer networks. The TCP/IP protocol is the backbone of Internet. We will discuss some of these and related topics in this chapter.

4.20.1 Why Internetworking ?

- Different networks such as LANs, MANs and WANs are designed with a specific task or application. So these networks won't have the same technology (hardware and protocols used).
- So the computers connected in the same network only can communicate to each others. It is not possible for a computer to communicate with some other computer outside its own network.
- For example an employee would be unable to communicate with the other computer connected to a printer or it would not possible to access a file on a computer which is on some other network and so on.
- This affected the productivity to a large extent in 1970's. So the concept of **universal service** came into existence.
- The simple meaning of universal service was that there was no dependence on the underlying physical technology or existence of separate physical networks.
- People wanted a single computer network to exist the way a telephone network exists. People should be able to use resources such as a printer or a file on any other computer without any hurdles.
- For this to become a reality it was necessary to connect all the computer networks together. This is why internetworking is essential.

4.20.2 The Problems in Internetworking :

- When internetworking is to be done, it must be remembered that the organizations involved have invested a lot of money on the infrastructure, cabling etc. of their existing network that they would like to reuse it when becoming the member of the internetwork.
- But it is not that simple to form a network merely by interconnecting wires from two networks. The problems are due to the incompatibilities in the electrical as well as the software aspects.

The packet sizes used by different networks will be different, the methods of acknowledgement or error detection etc. can also be totally different. There could be many more differences between them other than these.

Hence any two networks cannot be connected to each other just by connecting a wire between them to form an internetwork.

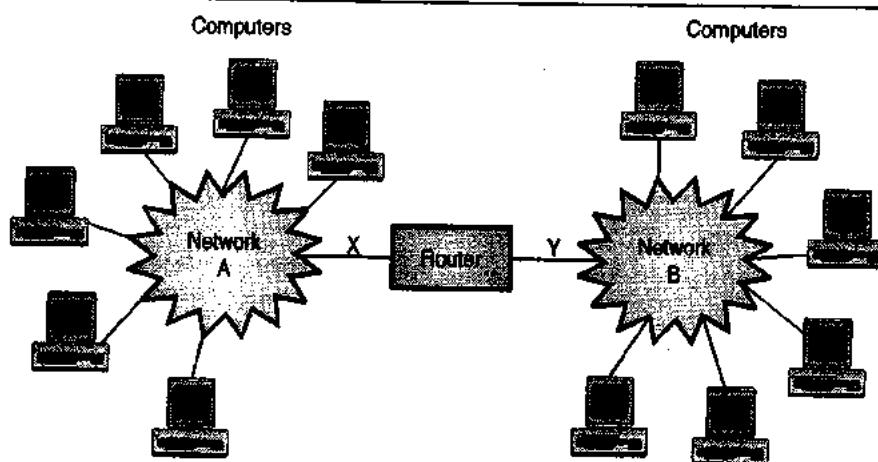
4.20.3 Dealing with Incompatibility Issue :

- Despite all the problems present with the internetworking, computer scientists and engineers have found a mechanism in order to connect computer networks together.
- The two important incompatibility issues which need to be sorted out are as follows :

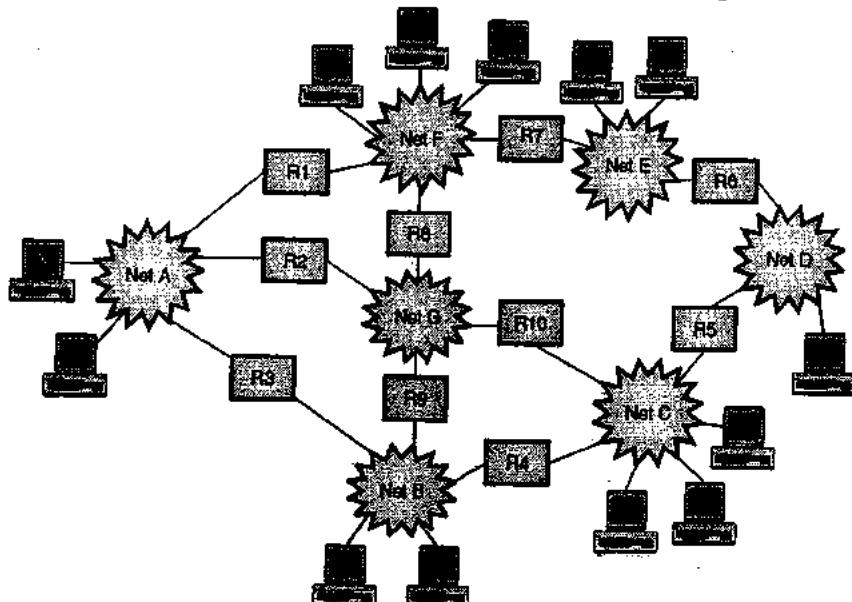
1. Hardware issues and 2. Software issues.

Hardware issues :

- We have to add some hardware for physically connecting computer networks which are far away to each other. Generally a router is used for this purpose as shown in Fig. 4.20.1(a).
- A router has its own CPU and memory. It has multiple input/output (I/O) interfaces which allows connections to many computer networks.
- For a network to get connected to a router is not a big deal. It is same as getting connected to a computer. So any network can get connected to a router very easily. The use of router for interconnecting two networks is as shown in Fig. 4.20.1(a).



(G-1445) Fig. 4.20.1(a) : Use of a router to connect two or more computer networks



(G-1446) Fig. 4.20.1(b) : Use of routers for interconnection



- A router will have two different physical addresses. One address corresponding to network-1 at point X and the other one corresponding to network 2 at point Y.
- The router in Fig. 4.20.1(a) will have two NICs which connect to these two networks. These two NICs will have two physical addresses.
- Thus it should be noted that a router can connect two incompatible networks with each other. In Fig. 4.20.1(a), the networks A and B can be two LANs or a LAN and a WAN etc.
- The router has necessary hardware and software to deal with the incompatibilities of the two networks A and B.
- We can extend this concept to interconnect more networks as shown in Fig. 4.20.1(b). The structure of an Internet is also like this.
- The routers in Fig. 4.20.1(b) will route the packets from source to destination. The software used in the routers computes the path from source to destination using a routing algorithm. Every router has its own routing table stored in its memory.

Software issues :

- The routers on the software level must agree with the manner in which information from the source computer be transmitted to the destination computer.
- All routers must conform to a pre-specified standard for the same. But this is not easy practically because the addressing mechanisms and packet formats of the underlying networks could be entirely different.
- Hence a standard packet format is decided. The sender breaks down its original message into this standard packet format.
- Therefore we need some protocols for standardizing the communication between incompatible networks.
- In case of the Internet the communication is made possible using TCP/IP protocol suite.
- The TCP/IP defines the packet size, routing algorithms, error control methods etc.

4.21 Fragmentation :

SPPU : May 07, May 11

University Questions

- Q.1** What is fragmentation ? What are different strategies for fragmentation ? (May 07, 8 Marks)
- Q.2** Describe a way to do reassembly of IP fragments at the destination. (May 11, 6 Marks)

- The network designers are not free to choose any size of the packet. The maximum packet size varies network to network and the factors which decide the maximum packet size are as follows :
 1. Width of the TDM transmission slot.
 2. Protocols used.
 3. Type of operating system.
 4. International standards.
 5. Efforts to reduce retransmission.
 6. Desire to prevent one packet from occupying the channel too long.
- All these factors put a limit on the maximum packet size.
- The maximum payload size ranges from 48 bytes for an ATM cell to 65, 515 bytes for an IP packet.
- When a large packet wants to travel over a network whose maximum packet size is very small, we face a problem.
- The solution to this problem is to avoid this situation in the first place by using a routing algorithm which will avoid sending packets through the networks that cannot handle them. But this solution cannot be exercised every time.
- The real solution to this problem is **Fragmentation**.

Fragmentation :

- In this technique, the gateways break up large packets into smaller ones called as fragments.
- Then each fragment is sent as a separate internet packet.
- But the reverse process of putting the fragments together is considerably difficult.

Recombination of fragments :

The recombination of fragments can be done by using one of the following two strategies.



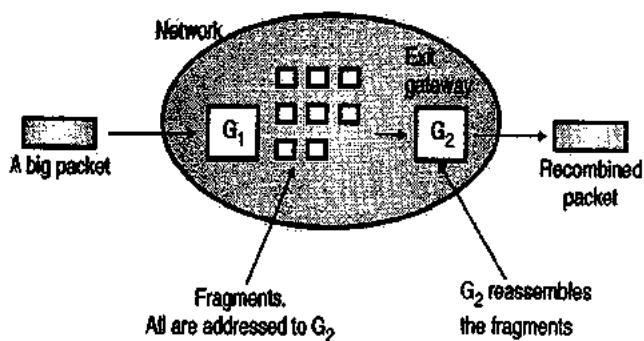
4.21.1 Strategy - 1 for Fragmentation (Transparent Strategy) :

SPPU : May 07, May 11

University Questions

- Q.1** What is fragmentation ? What are different strategies for fragmentation ? (May 07, 8 Marks)
Q.2 Describe a way to do reassembly of IP fragments at the destination. (May 11, 6 Marks)

- In this strategy, the fragmentation caused by a "small packet" network is made transparent to any subsequent network through which the packets will pass.
- When a large packet arrives at a gateway, G_1 in Fig. 4.21.1(a) it breaks the packet into fragments.
- Each fragment is then addressed to the same exit gateway. The exit gateway (G_2) recombines all these fragments. This strategy is illustrated in Fig. 4.21.1(a). In this way the small packet network has been made transparent i.e. the rest of the network can't see what happened.
- The subsequent networks are not even aware that fragmentation has taken place.
- Fragmentation in ATM networks is called segmentation, but the concept is same.



(G-494) Fig. 4.21.1(a) : Strategy - 1 for fragmentation

Disadvantages :

The disadvantages of transparent fragmentation are :

- The first problem with transparent fragmentation is that the exit gateway G_2 has to know that it has received all the pieces. For this a count field or an end of packet bit has to be included in each packet.
- Another important factor is that all the packets should exit via the same gateway.
- The last problem is the overhead required to repeatedly fragment and reassemble a large packet.

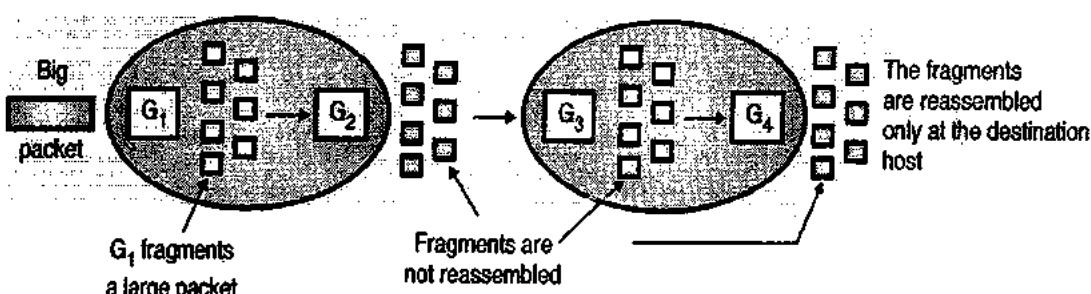
4.21.2 Strategy - 2 for Fragmentation (Non-transparent Strategy) :

SPPU : May 07, May 11

University Questions

- Q.1** What is fragmentation ? What are different strategies for fragmentation ? (May 07, 8 Marks)
Q.2 Describe a way to do reassembly of IP fragments at the destination. (May 11, 6 Marks)

- In this strategy, the fragmented packets are not reassembled at any intermediate stage. That means the exit gateways will not reassemble the fragments.
- Instead each fragment is treated as a separate original packet. All these packets are passed through the exit gateway or gateways and their recombination is carried out at the destination host as shown in Fig. 4.21.1(b).



(G-495) Fig. 4.21.1(b) : Strategy - 2 for fragmentation



- This is called as a non-transparent fragmentation.

Disadvantages :

The disadvantages of non-transparent fragmentation are :

- Every host must be capable of reassembling the fragments.
- The total overhead increases due to fragmentation since each fragment has to have a header.
- When a packet is fragmented, the fragments will have to be numbered in such a way that the original data stream can be reconstructed at the destination.

Advantage :

The advantage of non-transparent strategy is that now we can use multiple exit gateways and improve the network performance.

4.22 The Network Layer in the Internet :

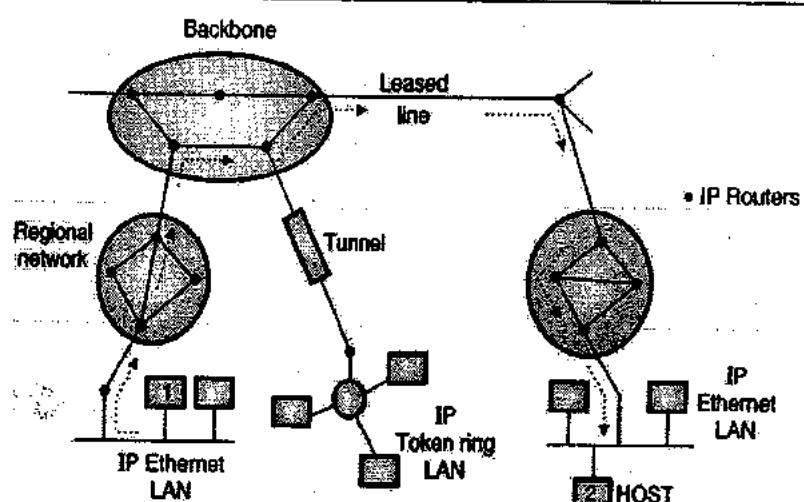
- The important principles used for the network layer design in the internet are as follows :
 - Make sure that the design works.
 - Keep the design simple.
 - Choose a correct design alternative from many possible designs.
 - Use modular design.
 - Let the design be suitable for heterogeneity.
 - Avoid static options and parameters.
 - Make the design perfect.

- Be strict as a sender and tolerant as a receiver.

- Scalability of the design is important.

- High performance and low cost.

- The most important binding factor which holds the whole Internet together is the network layer protocol IP (Internet Protocol).
- This protocol right from beginning was designed by keeping the internetworking in mind.
- The job of the network layer is to provide the best effort (not guaranteed) way to transport datagram, from the source to destination, irrespective of whether these machines are on the same network or on different networks.
- Communication in the Internet works as follows. The transport layer breaks the data stream into datagrams.
- Theoretically, datagrams can be upto 64 kbytes each, but practically they are not more than 1500 bytes so that they fit in one Ethernet frame.
- Each datagram is transmitted through the Internet after fragmenting it into smaller units.
- At the destination machine, all these pieces are reassembled by the network to form the original datagram.
- This datagram is then given to the transport layer which inserts it into the receiving process input stream.
- Fig. 4.22.1 explains this process.



(G-496) Fig. 4.22.1 : Communication in Internet

4.23 Congestion :

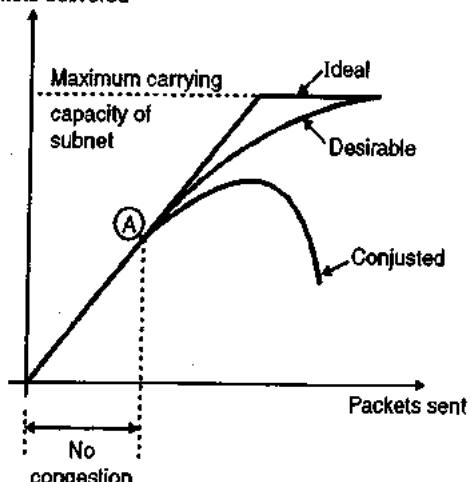
SPPU : May 09, May 12, Dec. 12, May 13, Dec. 13

University Questions

- Q. 1** Explain congestion. How do we control the same ? Which packets are used practically for this purpose ? At what layer this is done ?
 (May 09, 9 Marks)
- Q. 2** What is congestion ? List various network parameters affected due to congestion.
 (May 12, Dec. 12, May 13, Dec. 13, 8 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. 4.23.1 explains the concept of congestion graphically.
- Up to point A in Fig. 4.23.1, 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 the 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.

Packets delivered



(G-473) Fig. 4.23.1 : Concept of congestion

4.23.1 Need of Congestion Control :

SPPU : May 09

University Questions

- Q. 1** Explain congestion. How do we control the same ? Which packets are used practically for this purpose ? At what layer this is done ?
 (May 09, 9 Marks)

- 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).

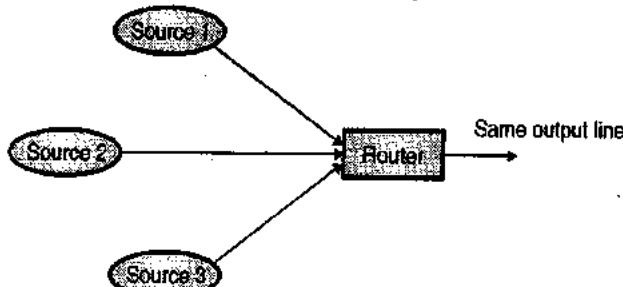
4.23.2 Causes of Congestion :

SPPU : May 09, May 12, Dec. 12, Dec. 13

University Questions

- Q. 1** What are the problems that the TCP may face with the emergence of high speed networks and how can these be addressed ?
 (May 09, 8 Marks)
- Q. 2** What is congestion ? List various network parameters affected due to congestion.
 (May 12, Dec. 12, Dec. 13, 8 Marks)

- Some of the causes of congestion are as follows :
 - If suddenly a flow of packets start coming on three or four senders which all needs 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. 4.23.2(a). This leads to congestion.

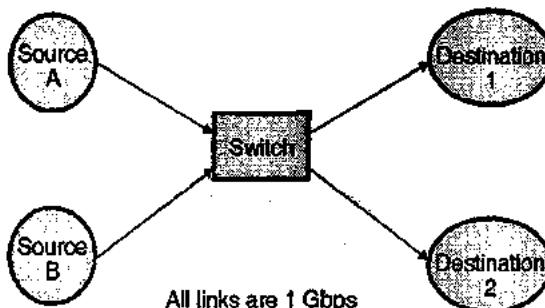


(G-474) Fig. 4.23.2(a)

- Note that increasing the memory to infinity also does not solve the problem, in fact it worsens.
- 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. 4.23.2(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. 4.23.2(b) : Network with high speed links

- 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.

- 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.

4.23.3 Difference between Congestion Control and Flow Control :

SPPU : May 06

University Questions

- Q.1 How congestion control is different from flow control ? Explain the load-shading Algorithm.

(May 06, 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.

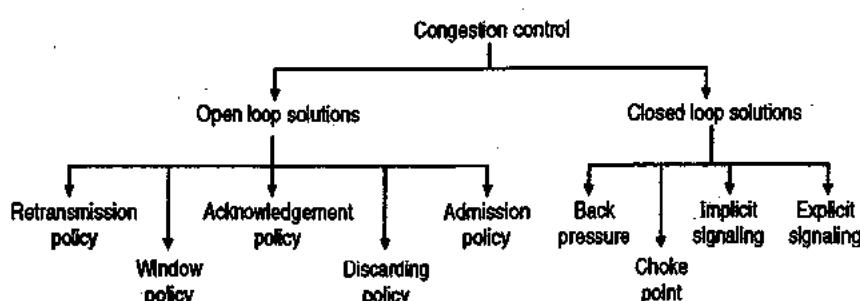
4.23.4 Principle of Congestion Control :

SPPU : May 16

University Questions

- Q.1 What is the difference between open-loop congestion control and closed loop congestion control ? Name the policies that can prevent congestion. (May 16, 4 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. 4.23.3 shows the classification of congestion control schemes and various policies used in open loop and closed loop groups.



(G-476) Fig. 4.23.3 : 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 Vs 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 today's 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.

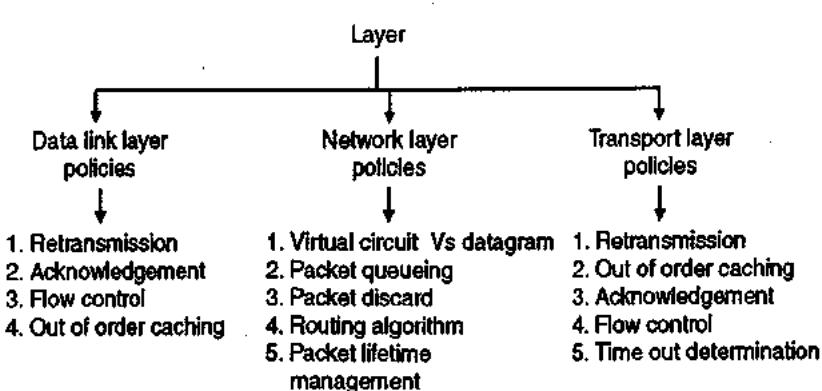
4.23.5 Congestion Prevention Policies :

SPPU : Dec. 06, Dec. 08, Dec. 09,
Dec. 11, May 16

University Questions

- Q. 1** Explain the congestion prevention policy of the data link layer, network layer, transport layer.
(Dec. 06, Dec. 09, 8 Marks)
- Q. 2** List the six ways for preventing congestion control. Explain any two of them. **(Dec. 06, 6 Marks)**
- Q. 3** Explain various congestion prevention policies for maintaining the QoS in the networks.
(Dec. 11, 5 Marks)
- Q. 4** What is the difference between open-loop congestion control and closed-loop congestion control ? Name the policies that can prevent congestion. **(May, 16, 4 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. 4.23.4 lists various policies corresponding to different layers for avoiding congestion.



(G-47) Fig. 4.23.4 : 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 queueing 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.

4.23.6 Congestion Control in Virtual Circuit Subnets :

- 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.

Review Questions

- | | |
|--|---|
| <p>Q. 1 Explain the connection oriented and connectionless services.</p> <p>Q. 2 What are the network design issues involved in designing a typical network and what are the supporting design tools available to make this design as a good design ? Explain how these design tools help to address design issues.</p> <p>Q. 3 Why modern computer use dynamic routing ? Explain with example how distance vector routing is used to route the packet and why count-to-infinity problem arises and how does it get solved.</p> | <p>Q. 4 Why leaky bucket algorithm should allow only 1 packet tick independent of how large the packet is ?</p> <p>Q. 5 A computer on 6 Mbps network is regulated by token bucket. The token bucket is filled at a rate of 1 Mbps. It is initially filled to capacity with 8 megabits. How long can the computer transmit at the full 6 Mbps.</p> <p>Q. 6 What is firewall ? What is difference between packet filtering firewall and proxy server gateways ?</p> <p>Q. 7 What is fragmentation ?</p> <p>Q. 8 Write a short note on leaky bucket algorithm.</p> <p>Q. 9 Write a short note on Congestion control.</p> <p>Q. 10 Enlist and discuss various design layer issues.</p> <p>Q. 11 A message is broken up into three pieces. Discuss the transmission of packets using : <ol style="list-style-type: none"> 1. The datagram approach to packet switching. 2. Permanent virtual circuit. 3. Switched virtual circuit. </p> <p>Q. 12 What is fragmentation ?</p> <p>Q. 13 What is fragmentation ? Is fragmentation needed in concatenated virtual circuit internets, or only in datagram system ?</p> <p>Q. 14 Write short notes on : Hierarchical routing.</p> <p>Q. 15 Give an efficient algorithm for finding the shortest paths between all pairs of nodes in a tree. What is the complexity of the algorithm ?</p> <p>Q. 16 Write short notes on : Tunneling.</p> <p>Q. 17 What is the difference between flow control and congestion control ?</p> <p>Q. 18 What is the difference between end to end delay and packet jitter ? What are the causes of packet jitter ?</p> <p>Q. 19 Tunneling through a concatenated virtual circuit subnet is straight forward. The multi protocol router at one end just sets up a virtual circuit to the other end passes packets through it. Can tunneling also be used in datagram subnets ? If so, how ?</p> <p>Q. 20 What is transparent and non transparent fragmentation ? Is fragmentation needed in concatenated virtual circuit internets or only in datagram systems ?</p> <p>Q. 21 Write short notes on : Congestion prevention policies.</p> |
|--|---|



- Q. 22 Write short notes on : Multicast routing.
- Q. 23 What is fragmentation ?
- Q. 24 What is firewall ? Explain proxy server gateway.
- Q. 25 Discuss the various causes of congestion in subnet.
- Q. 26 Write a short note on leaky bucket algorithm.
- Q. 27 Give an argument why the leaky bucket algorithm should allow just one packet per tick, independent of how large the packet is.
- Q. 28 Write short notes on : Jitter control.
- Q. 29 Whether the network layer should provide a connection oriented service or connectionless service ? Explain with suitable example.
- Q. 30 Write short notes on : Network design issues.
- Q. 31 What is the difference between congestion control and flow control ?
- Q. 32 Explain the term circuit switching. How is it different from the packet switching ?
- Q. 33 Explain the three phases related to the communication via circuit switching.
- Q. 34 Write a short note on Space-Division switches.
- Q. 35 Explain the time-division switches.
- Q. 36 Write a short note on Time-space-Time switches.
- Q. 37 Explain the routing system in circuit switching networks.
- Q. 38 State the three switching methods.
- Q. 39 Name different types of switches used in circuit switching.
- Q. 40 How is space division switching better than time division switching ?
- Q. 41 Explain the concept of datagram packet switching.
- Q. 42 State the advantages and drawbacks of datagram packet switching.
- Q. 43 Explain the delays in datagram switching.
- Q. 44 Write a short note on message switching.
- Q. 45 What is virtual circuit packet switching ?
- Q. 46 Explain the three phases of virtual circuit switching.
- Q. 47 Compare virtual switch and datagram switching.

- Q. 48 Compare the three switching types.

4.24 Solved University Examples :

Ex 4.24.1: Suppose a router has built up the routing table shown below. The router can deliver packets directly over interfaces 0 and 1 or it can forward packets to routers R2, R3 or R4. Describe what the router does with a packet addressed to each of the following destinations ?

1. 128.96.39.10
2. 128.96.40.12
3. 128.96.40.151
4. 192.4.153.17
5. 192.4.153.90

May 16. 8 Marks

Routing table

SubnetNumber	SubnetMask	NextHop
128.96.39.0	255.255.255.128	Interface 0
128.96.39.128	255.255.255.128	Interface 1
128.96.40.0	255.255.255.128	R2
192.4.153.0	255.255.255.192	R3
(Default)		R4

Soln. :

The router masks the destination address of packet with Subnet Mask and matches with Subnet Number and accordingly sends the packet corresponding to the matching entry in routing table. For no match, the packet is sent to the default router.

1. 128.96.39.10 and 255.255.255.128 = 128.96.39.0. So next hop is port0
2. 128.96.40.151 and 255.255.255.128 = 128.96.40.0. So next hop is R2
3. To default router R4
4. To default router R4
5. To default router R4

4.25 University Questions and Answers :

- Q. 1 What is fragmentation in IPv4 ? Explain with example. An IPv4 datagram arrives with fragmentation offset of 0 and an Mbit (More fragment bit) of 0. Is this a first fragment, middle fragment or last fragment ? (May 2016, 4 Marks)

Ans. :

Refer section 4.21 for fragmentation and 5.3.2 for structure of IP frame header.

Offset = 0 and M = 0 shows that it is the last or the only fragment.



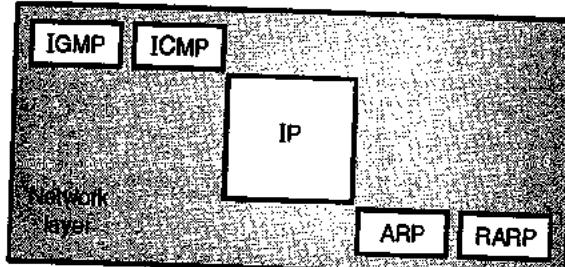
Network Layer Protocols

Syllabus :

IP Protocol, IPv4 and IPv6 addressing schemes, Subnetting, NAT, CIDR, ICMP, Routing in Internet : RIP, OSPF, BGP, MPLS, Mobile IP, Routing in MANET : AODV, DSR.

5.1 Introduction :

- 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. 5.1.1.



(G-524)Fig. 5.1.1 : Protocols at network layer

- Out of these protocols IP is the most important protocol. It is responsible for host to host delivery of datagram's 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.

5.1.1 Why IP Address ?

- How does the Internet Protocol (IP) know about the source of a datagram and its destination ?

- For a common user the Internet should appear as a single network and all the incompatibilities of the physical networks that make the Internet should remain hidden from the common user. Also the people connected to these physical networks should be able use any technology of their choice.
- So we need to have a common interface which binds the end users of Internet and the people dealing with their own networks.
- To identify each computer connected to the Internet uniquely is a great challenge.
- Different networking technologies have different physical addressing mechanisms. A physical address is also known as the hardware address and there are three methods to assign the hardware address to a computer as follows :

1. Static addresses
2. Configurable addresses
3. Dynamic addresses.

Static addresses :

- The static address is a physical address which is hard coded in the Network Interface Card (NIC) of the computer.
- This address is provided by the network hardware manufacturer and it does not change ever.

Configurable addresses :

- In this method, the physical address is configured inside a computer at the time of its first installation at its site. The configurable address allows the user to set up a physical address.

Dynamic addresses :

- In this method, a server computer dynamically assigns a physical address to a computer every time it boots. Thus the physical address of a computer changes everytime it is switch off and on.

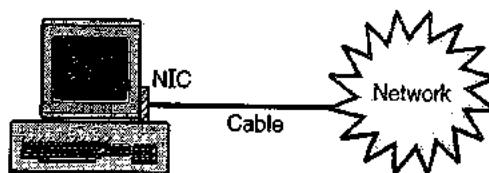


Note : The method of static addresses is the simplest of all the three methods discussed so far.

- It is important to understand that every computer has a unique hardware or physical address and it is stored in the NIC of the computer.

Role of NIC :

- As discussed earlier, the NIC is an input/output interface on each computer. It allows the computer to communicate with all other computers on the network. This is as shown in Fig. 5.1.2.



(G-1439) **Fig. 5.1.2 : Role of NIC**

- The NIC acts as an interface between a computer and its network.

5.1.2 Logical Addresses (IP Addresses) :

- 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.

5.2 ARP (Address Resolution Protocol) :

SPPU : May 08, May 12, Dec. 13

University Questions

- Q. 1 Illustrate ARP in detail with example.**

(May 08, 9 Marks)

Q. 2 Describe working of ARP with suitable example. What is Inverse ARP ? (May 12, 8 Marks)

Q. 3 Describe in short the importance and working of ARP and RARP protocol ? (Dec. 13, 8 Marks)

- ARP as defined in RFC 826 is Ethernet Address Resolution Protocol.
- ARP provides service to IP, which make us think that it is in the link layer TCP/IP model (or DLL of OSI model). But its messages are carried by DLL protocol and are not encapsulated within IP datagrams. That is why it can be called as a network layer protocol as well. Thus ARP occupies an unusual place in TCP/IP suite.
- But the most important point is that ARP provides an essential service when TCP/IP is running on a LAN.
- An internet consists of various types of networks and the connecting devices like routers.
- 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.

IP address :

- An IP address is an internetwork address. It is a universally unique address.
- Every protocol involved in internetworking requires IP addresses.

MAC address :

- 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 addressed 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 operating at the network layer at the same time.
- Similarly a packet may travel through different physical networks.
- So to deliver a packet to a host or a router, we require addressing to take place at two levels namely IP addressing and MAC addressing.
- Most importantly we should be able to map the IP address into a corresponding MAC address.

5.2.1 Mapping of IP Address into a MAC Address :

SPPU : May 09, May 11-

University Questions

- Q.1 How do IP addresses get mapped onto data link layer addresses, such as Ethernet?
 (May 09, 8 Marks)
- Q.2 Explain with suitable examples, how do IP addresses get mapped onto data link layer address?
 (May 11, 8 Marks)

- We have seen the need of mapping an IP address into a MAC address.
- Such a mapping can be of two types :
 - Static mapping and
 - Dynamic mapping

1. Static mapping :

- In static mapping a table is created and stored in each machine. This table associates an IP address with a MAC address.
- If a machine knows the IP address of another machine then it can search for the corresponding MAC address in its table.
- The limitation of static mapping is that the MAC addresses can change. These changed MAC addresses must be updated periodically in the static mapping table.

2. Dynamic mapping :

- In dynamic mapping technique a protocol is used for finding the other address when one type of address is known.
- There are two protocols used for carrying out the dynamic mapping. They are :
 - Address Resolution Protocol (ARP).
 - Reverse Address Resolution Protocol (RARP)

- The ARP is used for mapping an IP address to a MAC address whereas the RARP is used for mapping a MAC address to an IP address.

5.2.2 ARP Operation :

SPPU : Dec. 07, Dec. 12

University Questions

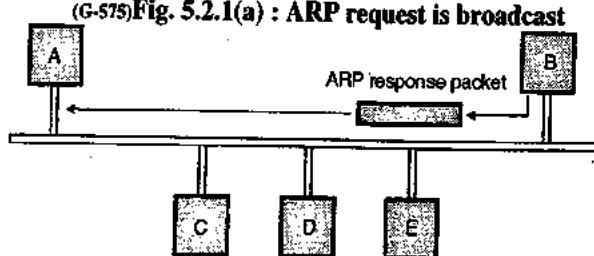
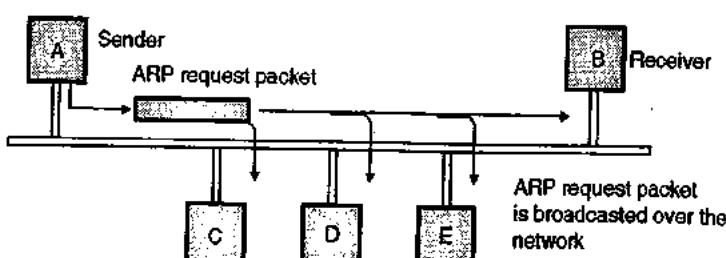
- Q.1 Describe in short the importance and working of ARP protocol. What is ARP cache?
 (Dec. 07, Dec. 12, 8 Marks)

- ARP is used for mapping an IP address to its MAC address. For a LAN, each device has its own physical or station address as its identification. This address is stored on the NIC (Network Interface Card) of that machine.

How to find the MAC address ?

When a router or a host (A) needs to find the MAC address of another host (B) the sequence of events taking place is as follows :

- The router or host A who wants to find the MAC address of some other router, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender A and the IP address of the receiver (B).
- This request packet is broadcasted over the network as shown in Fig. 5.2.1(a).
- Every host and router on the network will receive the ARP request packet and process it. But only the intended receiver (B) will recognize its IP address in the request packet and will send an ARP response packet back to A.
- The ARP response packet has the IP and physical addresses of the receiver (B) in it. This packet is delivered only to A (unicast) using A's physical address in the ARP request packet. This is shown in Fig. 5.2.1(b). Thus host A has obtained the MAC address of B using ARP.





5.2.3 ARP Cache Memory :

SPPU : Dec. 07, Dec. 12

University Questions

- Q.1** Describe in short the importance and working of ARP protocol. What is ARP cache?

(Dec. 07, Dec. 12, 8 Marks)

- The use of ARP would be inefficient if A needs to broadcast an ARP request for each IP packet that is to be sent to B, because instead of broadcasting the request it could have broadcast the IP packet itself.
- So ARP is efficient only if the ARP reply is stored in cache memory (cached) for a while. This is due to the fact that a system generally sends hundreds of packets to the same destination.
- Thus the system that receives an ARP reply stores the mapping in the cache memory and keeps it for 20 to 30 minutes. So if packets are again sent to the same destination then it could use this mapping instead of broadcasting an ARP request.
- Before sending an ARP request, the system checks its cache to see if the mapping could be found.

5.2.4 ARP Packet Format :

The ARP message format is as shown in Fig. 5.2.2.

The various fields in it are as follows :

- HTYPE (Hardware Type)** : This 16 bit field defines the type of network on which ARP is being run. ARP is capable of running on any physical network.
- PTYPE (Protocol Type)** : This 16 bit field is used to define the protocol using ARP. Note that we can use ARP with any higher-level protocol such as IPv4.
- HLEN (Hardware length)** : It is an 8 bit field which is used for defining the length of the physical address in bytes. For example, this value is 6 for Ethernet.

Hardware Type (16 bits)		Protocol type (16 bits)
Hardware length	Protocol length	Operation request 1, Reply 2
Sender hardware address		
Sender protocol address		
Target hardware address		
Target protocol address		

Fig. 5.2.2 : ARP message format

- PLEN (Protocol Length)** : This field is 8 bit long and it defines the length of the IP address in bytes. For IPv4 this value is 4.
- OPER (Operation)** : It is a 16 bit field which defines the type of packet. The two possible types of packets are : ARP request (1) and ARP reply (2).
- SHA (Sender Hardware Address)** : This field is used for defining the physical address of the sender. The length of this field is variable.
- SPA (Sender Protocol Address)** : This field defines the logical address of the sender. The length of this field is variable.
- THA (Target Hardware Address)** : It defines the physical address of the target. It is a variable length field. This field contains all zeros for the ARP request packet, because the receiver's physical address is not known to the sender.
- TPA (Target Protocol Address)** : This field defines the logical address of the target. It is a variable length field.

5.2.5 Encapsulation :

SPPU : Dec. 08

University Questions

- Q.1** Explain how ARP protocol makes the use of distance vector routing to discover the route.

(Dec. 08, 8 Marks)

- An ARP packet (request or reply) is inserted directly into the data link frame. Such an insertion is known as encapsulation.
- Fig. 5.2.3 shows an example of encapsulation in which an ARP packet is being encapsulated in an Ethernet frame. The type field shows that the data carried by the frame is an ARP request or reply packet.

The type field indicates that
the data carried by the frame is -
ARP packet



Data field contains
the ARP request or reply
packet

(G-578)Fig. 5.2.3 : Encapsulation of ARP packet

5.2.6 Operation of ARP on Internet :

- The services of ARP can be used under the following working conditions when it is being operated on internet :

- 1. The sender is a host and wants to communicate with another host which is on the same network.
- 2. The sender is a host and wants to communicate with a host on another network.
- 3. The sender is a router. It has received a datagram with a destination address of a host on another network.
- 4. The sender is a router. It has received a datagram which is meant for a host in the same network.
- Now let us see how ARP works on the internet.

Operation :

1. The sender (host or router) knows the IP address of the target.
2. IP orders ARP to create an ARP request message. The request packet consists of senders physical and IP addresses plus the IP address of the target but the physical address of the target is not known.
3. This ARP request packet is sent to the data link layer. Here the ARP request packet is inserted in a frame.
4. Every router or host receives this frame because it is broadcast. All the machines except the target drop this packet as discussed earlier.
5. The target machine sends back a reply packet which contains the target's physical address. This reply is unicast and addressed only to the sender.
6. The sender receives the reply packet. Hence the physical address of the target has been obtained.
7. The IP datagram carrying data for the target machine is inserted in a frame and the frame is unicast to the target machine.

5.2.7 Four Different Cases :

The four different cases in which the services of ARP can be used are as follows :

Case 1 :

- The host sender wants to send a packet to another host on the same network.
- In this case, the destination IP address in the datagram header acts as the logical address which should be mapped to a physical address.

Case 2 :

- This case corresponds to a situation where a host wants to send a packet to another host on another network.
- Here the host refers its routing table and finds the IP address of the next hop (router) for the destination host.

- If it does not have the routing table, then it will search for the IP address of the default router.
- The IP address of the router will be considered as the logical address which is to be mapped to the corresponding physical address.

Case 3 :

- In this case a router has received a datagram which is to be sent to a host on another network.
- To do this the router checks its routing table and finds the IP address of the next router.
- The IP address of the next router should be mapped to a physical address by the ARP.

Case 4 :

- The sender is a router. It has received a datagram which is to be sent to a host on the same network.
- In this case the IP address of the destination host should be mapped into a physical address.

5.2.8 Proxy ARP :

- Proxy ARP is a technique that is used for creating the subnetting effect.
- The proxy ARP is basically an ARP that acts on behalf of a group of hosts.
- If a router running a proxy ARP receives an ARP request to look for the IP address of one of these hosts, the router will send back an ARP reply in which the physical address of the router is sent.
- If the router receives an actual IP packet then it sends that packet to the corresponding correct host.

5.3 Internet Protocol (IP) :

SPPU : Dec. 11

University Questions

- | | | |
|-------------|---|--------------------|
| Q. 1 | Compare IP and ICMP. Explain header format of ICMP v6 protocol. | (Dec. 11, 8 Marks) |
| Q. 2 | State which transport layer protocol is used by the following protocols-HTTP, FTP, DHCP, DNS, ICMP, TFTP, IP, SMTP. | (Dec. 11, 4 Marks) |

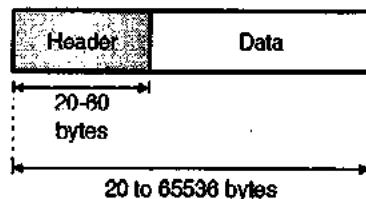
- This is the host to host delivery protocol which belongs to the network layer and is designed for the Internet.
- IP is a connectionless datagram protocol with no guarantee of reliability.
- It is an unreliable protocol because it does not provide any error control or flow control.
- IP can only detect 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.

5.3.1 Datagram :

- Packets in IP layer are called datagrams. Fig. 5.3.1 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. 5.3.1 : IPv4 datagram format

5.3.2 Structure of IP Frame Header :

- The IP frame header contains routing information and control information associated with datagram delivery. The IP header structure is as shown in Fig. 5.3.2.

			32 bits
4	8	16	
VER	HLEN	D.S. type of service	Total length 16 bits
Identification 16 bits	Flags 3 bits	Fragmentation offset (13 bits)	
Time to live	Protocol	Header checksum (16 bits)	
Source IP address			
Destination IP address			
Option + Padding			

Fig. 5.3.2 : IPv4 header structure

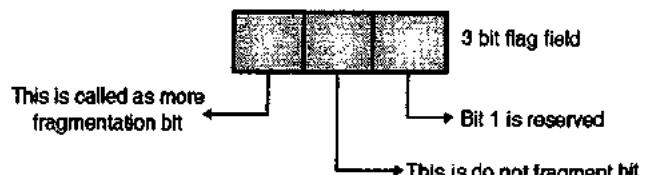
Various fields in the IP header are as follows :

- VER (Version) :** This 4 bit long field defines the version of IP. Current version of IP is IPv4 and the latest version of IP is IPv6.
- HLEN (Header Length) :** This field is 4 bit long and defines the length of the datagram header in 4-byte word. The value of this field multiplied by 4 to give the length in bytes.
- Differential services (DS) :** This is an 8 bit field. Its job is to define the class of the datagram for quality of service (QoS) purpose.
- 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.

5. Identification, flag and offset :

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.

Flags : This is a three bit field. The 3 bits are as shown in Fig. 5.3.3.



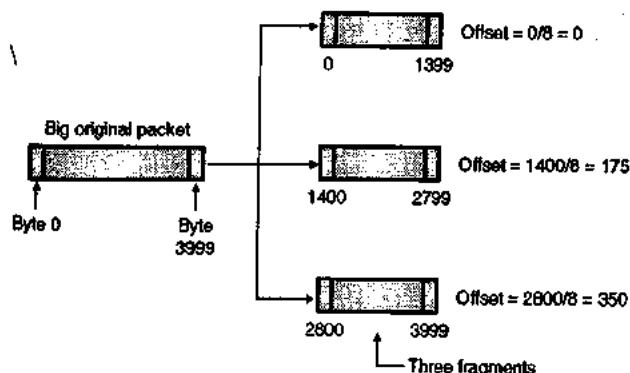
(G-527) Fig. 5.3.3 : Flag bits

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.

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. 5.3.4.
- 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. 5.3.4.
- 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.



(G-528)Fig. 5.3.4 : Example of fragmentation

6. Time to live :

This is an 8 bit long field which controls the maximum number of routers visited by the datagram.

7. Protocol :

- This field defines the higher-level protocol which uses the services of the IP layer. An IP datagram can encapsulate data from various higher level protocols such as TCP, UDP, ICMP and IGMP.

- The protocol field specifies the final destination protocol to which the IP datagram should be delivered.
- Since IP multiplexes and demultiplexes data from different higher level protocols, the value of protocol field helps in demultiplexing at the final destination.

8. 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.

9. Source address :

This field is used for defining the IP address of the source.

10. Destination address :

This field is used for defining the IP address of the destination.

11. Options :

- Options are not required for every datagram. They are used for network testing and debugging.
- IP provides several optional features, allowing a packet's sender to set requirements on the path it takes through the network (source routing), trace the route a packet takes (record route), and label packets with security features.

5.3.3 Services Provided :

IP provides following services :

- Addressing :** IP headers contain 32-bit addresses which identify the sending and receiving hosts. These addresses are used by intermediate routers to select a path through the network for the packet.
- Fragmentation :** IP packets may be split, or fragmented, into smaller packets. This permits a large packet to travel across a network which can only handle smaller packets. IP fragments and reassembles packets transparently.
- Packet timeout :** Each IP packet contains a Time To Live (TTL) field, which is decremented every time a router handles the packet. If TTL reaches zero, the packet is discarded, preventing packets from running in circles forever and flooding a network.
- Type of service :** IP supports traffic prioritization by allowing packets to be labeled with an abstract type of service.

5.3.4 IPv4 Addresses :

SPPU : May 06, Dec. 08

University Questions

Q. 1 Illustrate with a diagram the five address formats used in Internet.

(May 06, 8 Marks)



Q-2 What is the difference between classful and classless IP addressing? Which addressing is currently used in the internet? Explain with suitable example. (Dec. 08, 8 Marks)

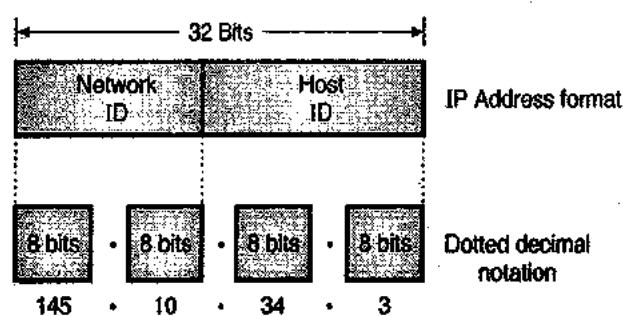
- As already stated every host and router on the internet has a unique IP address.
- All the IP addresses are 32 bit long and they are used in the source address and destination address fields of the IP header.
- Fig. 5.3.5 shows the IP address format. It consists of two fields called Network ID and Host ID.
- The IP numbers (addresses) for the hosts are assigned by the network administrator. For a public network on the internet, we have to obtain a network number assigned by the network information center.
- An IP address consists of two parts. The first part of the address, called the network number, identifies a network on the internet; the remainder, called the host ID, identifies an individual host on that network.

Address Space :

- The IPv4 protocol has an address space. It is defined as the total number of addresses used by the protocol.
- If N number 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.

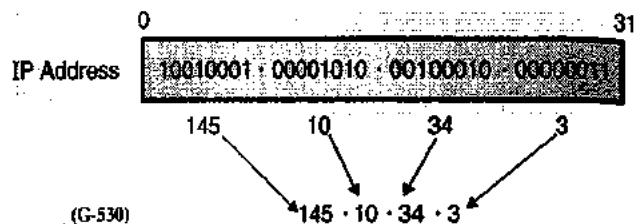
IPv4 Address Format and Notations :

- The 32 bit IPv4 address is grouped into groups of eight bits, separated by dots. Each 8 bit group is then converted into its equivalent binary number as shown in Fig. 5.3.5.
- Thus each octet (8 bit) can take value from 0 to 255. The IPv4 in the dotted decimal notation can range from 0.0.0.0 to 255.255.255.255.



(G-529) Fig. 5.3.5 : IPv4 address format and dotted decimal format

- For example the IPv4 address of 1001 0001.00001010 00100010 00000011 is denoted in the dotted decimal form as 145.10.34.3.



IPv4 Address classes : (Classful Addressing)

- The IPv4 addresses are classified into 5 types as follows :

 1. Class A
 2. Class B
 3. Class C
 4. Class D
 5. Class E



(G-531) Fig. 5.3.5(a) : Class A IPv4 address formats

- The formats used for IPV4 address are as shown in Fig. 5.3.5. The IPV4 address for class A networks is shown in Fig. 5.3.5(a).
- The network field is 7 bit long as shown in Fig. 5.3.5(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. 5.3.5(b).
- The first two fields identify the network, and the number in the first field must be in the range 128 - 191.

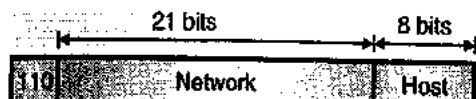


(G-532) Fig. 5.3.5(b) : Class B format

- 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. 5.3.5(c).



(G-533) Fig. 5.3.5(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. 5.3.5(d).



Fig. 5.3.5(d) : Class D format

- The class D 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. 5.3.5(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.

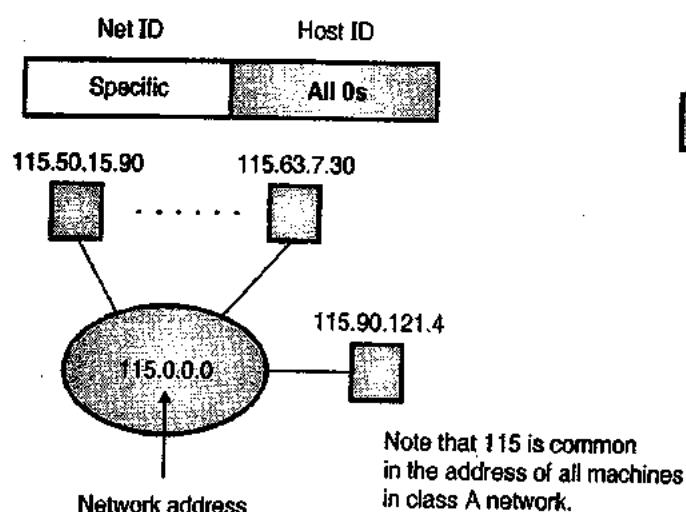


Fig. 5.3.5(e) : IPv4 address for class E network

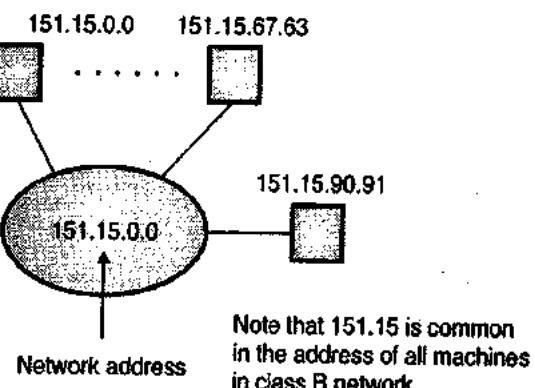
- The 32 bit (4 byte) network addresses are usually written in dotted decimal notation. In this notation each of the 4-bytes is written in decimal from 0 to 255.
- So the lowest IP address is 0.0.0.0 i.e. all the 32 bits are zero and the highest IPv4 address is 255.255.255.255.

5.3.5 Network Address :

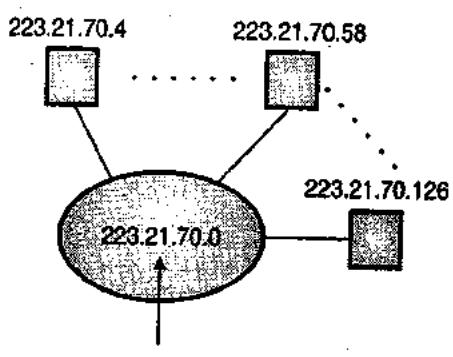
- The network address is an address that defines the network itself. It cannot be assigned to a host. Fig. 5.3.6 shows the examples of network addresses for different classes.



(a) Class A network address



(b) Class B network address



(c) Class C network address

(G-536) Fig. 5.3.6

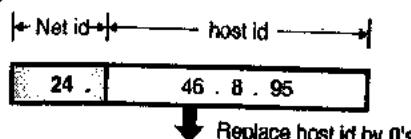


- The following examples will enable you to find the network address.

Ex. 5.3.1 : 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. 5.3.1.



Network address → 24 . 0 . 0 . 0

(G-537) Fig. P. 5.3.1

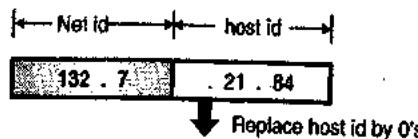
So the network address is 24.0.0.0.

Ex. 5.3.2 : For the address 132.7.21.84 find the type of network and the network address.

May 09, 4 Marks

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. 5.3.2.



Network address → 132 . 7 . 0 . 0

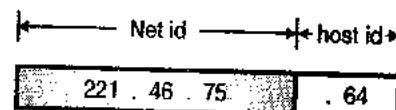
(G-538) Fig. P. 5.3.2

So the network address is 132.7.0.0.

Ex. 5.3.3 : 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. 5.3.3.



(G-539) Fig. P. 5.3.3

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.

5.3.6 Special IP Addresses :

SPPU : Dec. 08

University Questions

Q. 1 What is the difference between classful and classless IP addressing ? Which addressing is currently used in the internet ? Explain with suitable example.
(Dec. 08, 8 Marks)

- Fig. 5.3.7 shows some 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.

(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 All 1s means broadcast on the local network

(d) Network 1 . 1 . 1 1 Broadcast on a distant network

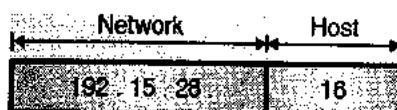
(e) 127 . Anything Loop back

(G-540) Fig. 5.3.7 : Special IP addresses

- The IP addresses with 0 as the network number refer to their own network without knowing its number as shown in Fig. 5.3.7(b).
- The address having all ones is used for broadcasting on the local network such as a LAN as shown in Fig. 5.3.7(c).
- Refer Fig. 5.3.7(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. 5.3.7(e) then it is a reserved address **loopback testing**. This feature is also used for debugging network software.

5.3.7 Address Masks (Default Masks) :

- An address mask determines which portion of an IP address identifies the network and which portion identifies the host.
- Like the IP address, the mask is represented by four octets. (An octet is an 8-bit binary number equivalent to a decimal number in the range 0 - 255).
- If a given bit of the mask is 1, the corresponding bit of the IP address is in the network portion of the address, and if a given bit of the mask is 0, the corresponding bit of the IP address is in the host portion.
- For example consider a class C address 192.15.28.16. This is shown in Fig. 5.3.8. Note that 192.15.28 corresponds to the network part and 16 correspond to the host part.



(G-54) Fig. 5.3.8

- So as to differentiate the network and host parts. We have to use a mask 255.255.255.0.

- Table 5.3.1 shows the mask 255.255.255.0 in both decimal and binary form, aligned with the class C address 192.15.28.16, also in both decimal and binary form :
- If a field of the network address is entirely used for the network number, the corresponding field of the mask has the decimal value 255 (binary 11111111), and if an address field is entirely used for the host ID, the corresponding field of the mask has the decimal Value 0

Table 5.3.2

Decimal Value in Field of Mask	Binary Value in Field of Mask	Function
255	11111111	Identify network number
0	00000000	Identify host ID

- Accordingly, the address masks for the three network classes described above are as shown in Table 5.3.3. These masks are also called as default masks.

Table 5.3.3

Address Class	Address Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Which IP protocol version is being used currently ?

- The network protocol in the Internet is currently IPv4. It was first introduced in 1970's.
- After that the world of data communication has grown beyond imaginations. Even though IPv4 is a well designed protocol, it has some limitations.

5.3.8 Limitations of IPv4 :

- The most obvious limitation of IPv4 is its address field. IP relies on network layer addresses to identify end-points on networks, and each networked device has a unique IP address.

Table 5.3.1 : IP address (In decimal and binary form)

Element	Network			Host
Mask	255	.255	.255	.0
	11111111	11111111	11111111	00000000
Address	192	.15	.28	.16
	11000000	00001111	00011100	00010000



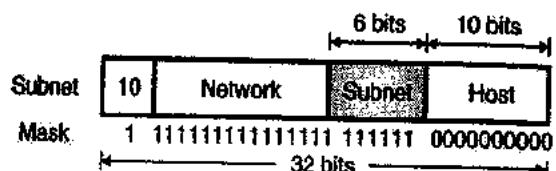
- IPv4 uses a 32-bit addressing scheme, which gives it 4 billion possible addresses. With the proliferation of networked devices including PCs, cell phones, wireless devices, etc., unique IP addresses are becoming scarce, and the world could theoretically run out of IP addresses.
- If a network has slightly 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.

5.3.9 Subnetting in IP :

All the hosts in a network must have the same network number. But this property of IP addressing can be problematic as the network size increases.

- For example a company initially may have only one LAN but as the time passes by it might end up with many LANs each one having its own router and each one with its own class C network number.
- With increase in the number of distinct local networks, their management becomes a problem.
- Everytime a new network gets installed, the system administrator has to contact NIC to get a new network number and then this number is to be announced worldwide.

- Another problem is that if a machine is to be moved from one LAN to the other, then its IP address needs to be changed. This will require modification in its configurational files and its modified IP number needs to be announced to the world.
- The solution to this problem is that, the network is split into several smaller networks internally but it acts like a single network to the outside world.
- The smaller parts of a network are called as subnets.
- Now continue with the same example taken at the beginning of this subsection. The growing company should start up with class B address instead of class C address and it can number the hosts from 1 to 254.
- When a second LAN is to be installed it can split the 16 bit host number into a 6-bit subnet number and 10 bit host number as shown in Fig. 5.3.9.

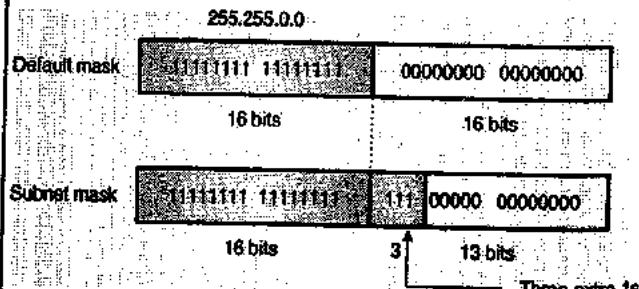


(G-542) Fig. 5.3.9 : One of the ways to subnet class B network

- Due to this split it is possible to connect 62 LANs (0 and -1 are reserved) and each one can contain upto 1022 hosts.
- Outside the network, the subnetting is not visible. So even if a new subnet is created it is not necessary to contact NIC or change any database.

5.3.10 Subnet Mask :

- The number of 1's in the subnet mask is more than the number of 1s in the corresponding default mask.
- In subnet mask we change some of the leftmost 0s in the default mask to make a subnet mask.
- Fig. 5.3.10 shows the difference between a class B default mask and subnet mask for the same block.



(G-543) Fig. 5.3.10 : Subnet mask

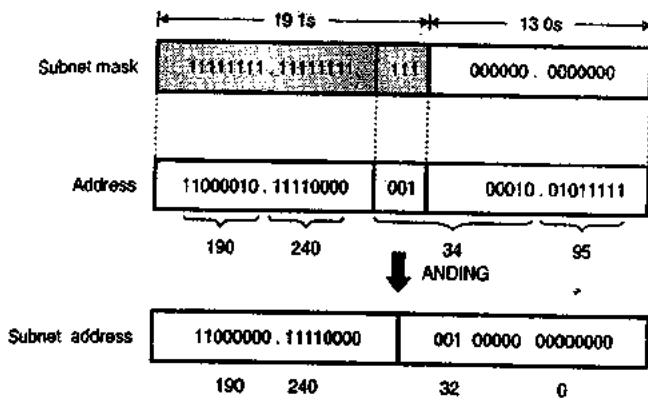
Number of subnets :

The number of subnets is determined by the number of extra 1s. For 3 extra 1s the number of subnets will be $2^3 = 8$. For n extra 1s the number of subnets is 2^n .

Ex. 5.3.4 : 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. 5.3.4.



(G-54) Fig. P. 5.3.4

Thus the subnet address is 190.240.32.0

5.3.11 Classless Addressing :

- Even though 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.

- The addresses in a block should be continuous, i.e. serial in manner.
- 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 ...etc.
- The first address should be evenly divisible by the number of addresses.

5.3.12 Supernetting :

- 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 supernetwork.
- 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 supernetwork as a whole.

Note : The classful addressing is almost obsolete now and it is being replaced with classless addressing.

5.3.13 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.

5.3.14 Registered and Unregistered Addresses :

- 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 5.3.4. 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 5.3.4 : 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

5.4 IPv6 :

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.

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 is compared to IPv4's 32-bit address space. So there is a large increase in the address space.

$$\text{Address space of IPv6} = (2^{128})$$

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 :

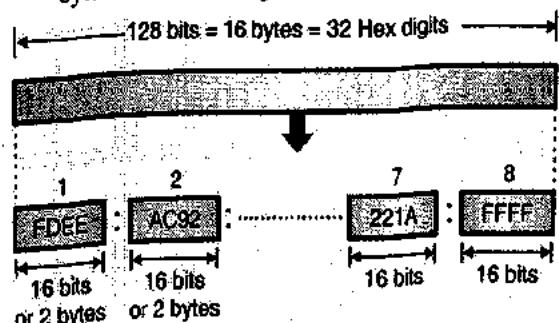
- IPv6 includes plug and play in the standard specification. It therefore must be easier for novice users to connect their machines to the network, it will be done automatically.

8. Clearer specification and optimization :

- IPv6 follows good practices of IPv4, and omits flaws/obsolete items of IPv4.

5.4.1 IPv6 Addresses :

- An IPv6 address is 128 bit long. It consists of 16 bytes as shown in Fig. 5.4.1.



(G-545) Fig. 5.4.1 : IPv6 address

Hexadecimal colon notation :

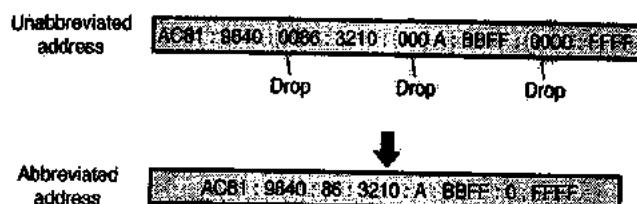
- IPv6 uses a special notation called hexadecimal colon notation. In this, the total 128 bits are divided into 8 sections, each one is 16 bits or 2 bytes long.
- The 16 bits or 2 bytes in binary correspond to four hexadecimal digits of 4-bits each. Hence the 128 bits in hexadecimal form will have $8 \times 4 = 32$ hexadecimal digits. These are in groups of 4 digits as shown and every group is separated by a colon as shown in Fig. 5.4.1.



- 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.

5.4.2 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. 5.4.2.

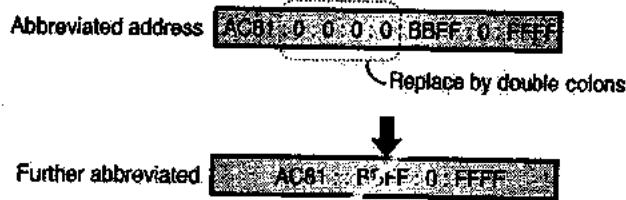


(G-546) Fig. 5.4.2 : Abbreviated address

- Note that only the leading zeros can be dropped but the trailing zeros cannot be dropped. This is illustrated in Fig. 5.4.2. 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.
- We can remove the zeros completely and replace them with double colon as shown in Fig. 5.4.3.



(G-547) Fig. 5.4.3 : Further abbreviation

- 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.

5.4.3 CIDR Notation :

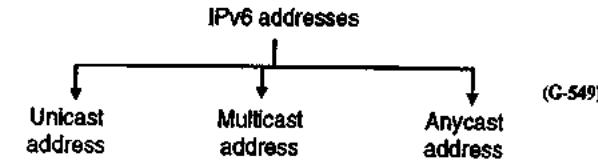
- IPv6 protocol allows classless addressing and CIDR notation. Fig. 5.4.4 shows how to define a prefix of 60 bits using CIDR.

FDEC 0:0:0:0:BBFF:0:FFFF/60

Fig. 5.4.4 : CIDR address

5.4.4 Categories of Address :

- IPv6 defines three different types of addresses.



1. Unicast :

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.

2. Anycast :

- 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 exactly one of the member of the group which is the closest or the most easily accessible.

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.

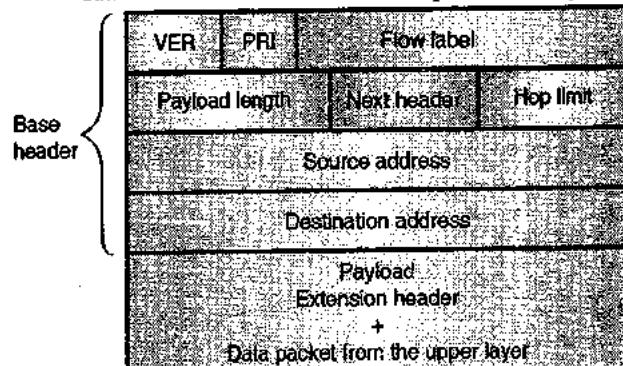
5.4.5 IPv6 Packet Format :

SPPU : Dec. 11, May 13, May 15

University Questions

- Q. 1** Compare IPv6 and IPv4. Draw and explain IPv6 header format. (Dec. 11, 8 Marks)
- Q. 2** What is the significance of priority and flow label fields in IPv6. (May 13, 8 Marks, May 15, 5 Marks)

- Fig. 5.4.5 shows the packet format 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 :
 - An optional extension headers and
 - 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-550) Fig. 5.4.5 : Format of an IPv6 datagram

Base header :

Fig. 5.4.5 shows the base header. It has eight fields. These fields are as follows :

- 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.
- Priority** : This 4 bit field contents defines the priority of the packet which is important in connection with the traffic congestion.
- Flow label** : It is a 24 bit (3 byte) field which is supposed to provide a special handling for a particular flow of data.
- 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.

- Next header** : It is an 8 bit field which defines the header which follows the base header in the datagram.
- Hop limit** : Contents of this 8 bit (1 byte) field have the same function as TTL (time to live) in IPv4.
- Source address** : It is a 16 byte (128 bit) Internet address which corresponds to the originator or source which has produced the datagram.
- 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.

5.4.6 NAT – Network Address Translation :

SPPU : Dec. 07

University Questions

- Q. 1** What is NAT? Explain the operation of NAT with suitable example. (Dec. 07, 6 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	1048576 Hosts
Range 3	192.168.0.0 to 192.168.255.255/16	65536 Hosts

Generally most companies choose the addresses from the first range.

Refer Fig. 5.4.6 which explains the operation of 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. 5.4.6 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.

5.5 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. 5.5.1).

- 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 :

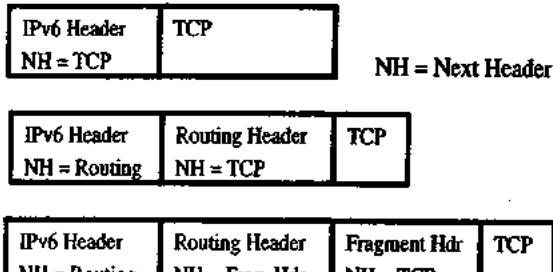
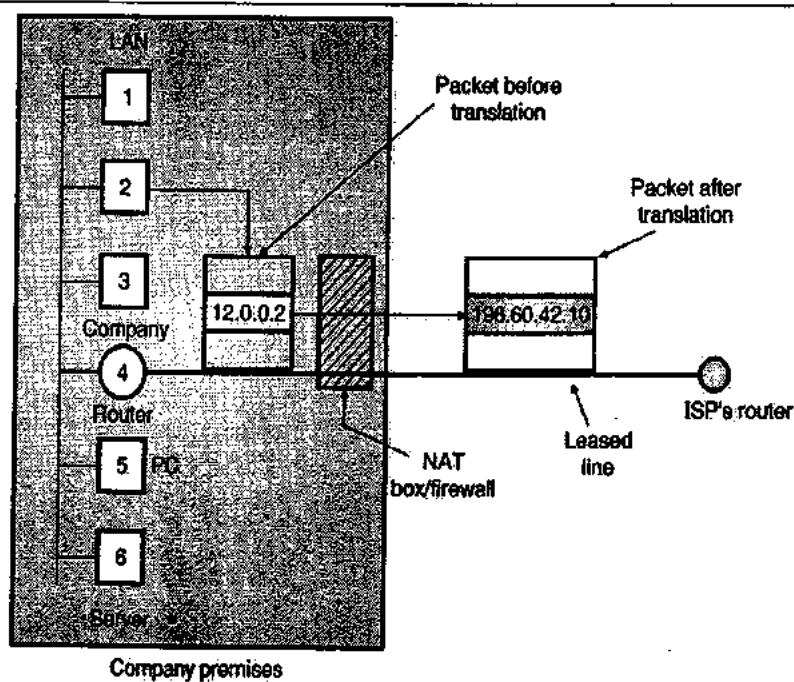


Fig. 5.5.1 : Examples of headers chain

- 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 :



(G-55) Fig. 5.4.6 : NAT

- 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

5.5.1 Fragmentation :

SPPU : Dec. 12

University Questions

- Q.1** Draw and explain IPv6 header. Explain the significance of extension header. (Dec. 12, 8 Marks)

- 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.

5.5.2 Authentication and Privacy :

IPv6 provides authentication and privacy using options in the extension header.

5.5.3 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 6bone, 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 6bone.

4. The transition can be achieved through two approaches: protocol tunneling or IPv4/IPv6 dual stack.

5.5.4 Comparison between IPv4 and IPv6 :

SPPU : Dec. 11, Dec. 13, Feb. 16

University Questions

- Q.1** Compare IPv6 and IPv4. Draw and explain IPv6 header format. (Dec. 11, 8 Marks)
- Q.2** Draw and compare IPv4 and IPv6 header. (Dec. 13, 8 Marks)
- Q.3** Differentiate between IPv4 and IPv6 with header format. (Feb. 16, 6 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.

- A large number of people have portable computers and they want to work on them wherever they are in the world. Such computers are called as mobile hosts.
- To route a packet to a mobile host, the network has to first find the mobile host.
- Refer Fig. 5.6.1 which shows a network model suitable for mobile communication.
- The network of Fig. 5.6.1 consists of a WAN which has routers and hosts. MANs, LANs and wireless cells are connected to this WAN.
- The world is divided into areas. Each area has one or more foreign agent. A foreign agent is supposed to keep track of all the mobile users visiting his area.
- In addition to the foreign agents, each area has a home agent which keeps track of users whose home is in the area but who are currently visiting some other area.
- When a new user enters an area his computer has to register itself to the foreign agent of that area and when the user leaves that area the deregistration should be carried out.
- The routing of packets to a mobile host takes place by following the routing procedure given below :

Routing procedure :

- When a packet is to be sent to a mobile user it is first routed to the user's home LAN.
- This packet is intercepted by the home agent.
- This home agent then looks for the mobile user's current location and finds the address of the corresponding foreign agent.
- The home agent then encapsulates the packet in the payload field of an outer packet and sends it to the foreign agent. This is called tunneling.
- This packet is received by the foreign agent, who removes the original packet from the payload field and sends it to the mobile user as a data link frame.
- The home agent then tells the sender to send the packets directly to the mobile user. The packets are then routed directly to the user via the foreign agent.

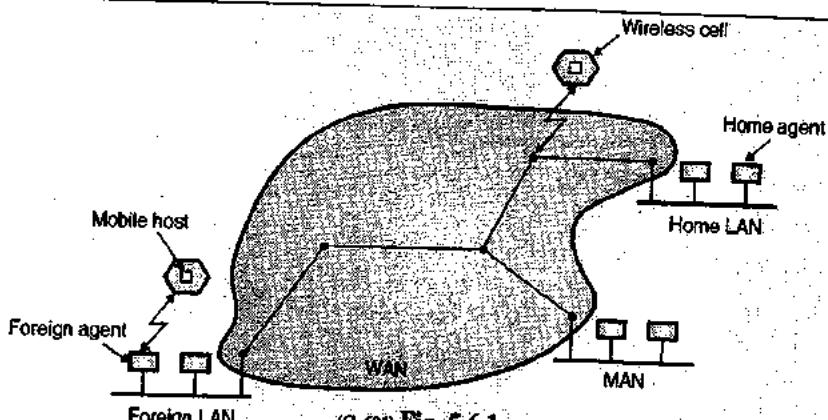
5.6 Mobile IP :

5.6.1 Routing for Mobile Hosts :

SPPU : May 06

University Questions

D.1. Describe the routing method for mobile host ?
(May 06, 8 Marks)



(G-69) Fig. 5.6.1

5.6.2 Mobile IP :

- Many internet users have portable computers and they want to stay connected to the Internet even when they are outside and moving.
- The existing IP addressing system cannot work properly for mobile users.
- The biggest problem is the addressing scheme itself. So IETF set up a working group to get the solution. The group set the following goals for the solution to this problem.
 1. Each mobile host should be able to use its home IP address when he is anywhere.
 2. Software changes to the fixed hosts were not permitted.
 3. Any changes to the router software and tables were not allowed.
 4. Most packets for mobile hosts should not make detours on their way.
 5. No overhead should be incurred when a mobile host is at home.
- The solution chosen was the one discussed earlier i.e. routing for mobile hosts.
- Let us briefly review the principle discussed there.
- Every site which has to allow the users to roam has to create a home agent.
- Every site which has visitors has to create a foreign agent. When a mobile host visits a foreign site it contacts the foreign host there and registers itself.
- The foreign host then contacts the user's home agent and gives it a care-of-address (C/O) which is normally the foreign agent's own IP address.
- When a packet arrives at the user's home LAN it comes in at some router attached to the LAN.
- The router then locates the host by broadcasting an ARP packet asking the Ethernet address.
- The home agent answers this question by giving its own Ethernet address.
- The router then sends the packet to the home agent. It then sends the packet to the care-of-address by encapsulating it in the payload field of an IP packet addressed to the foreign agent.
- The foreign agent decapsulates and delivers them to the data link address of the mobile host.
- The home agent gives the care of address to the sender so future packets can be tunneled directly to the foreign agent.
- This solution satisfies all the requirements (goals) mentioned earlier.

5.7 Mapping Physical Address to Logical Address :

- Sometimes a host knows its physical address but needs to know its logical address.
- This can happen in the following two cases :
 1. If a diskless station has been just booted. This station can find its physical address by checking its interface but it does not know its logical address.
 2. An organization has less number of IP addresses. So it can not assign a separate IP address to each station. Hence it has to assign the IP addresses when a station demands for it.

5.7.1 The Reverse Address Resolution (RARP) Protocol :

SPPU : May 12, Dec. 13

University Questions

- Q. 1** Describe working of ARP with suitable example. What is Inverse ARP ? (May 12, 8 Marks)
- Q. 2** Describe in short the importance and working of ARP and RARP protocol ? (Dec. 13, 8 Marks)

- ARP is used for solving the problem of finding out which Ethernet address corresponds to a given IP address. That means ARP is used for the mapping of IP address to physical or MAC address.
- But sometimes we have to solve a reverse problem. That means we have to obtain the IP address corresponding to the given Ethernet (MAC) address. Such a problem can occur when booting a diskless workstation.
- The problem of obtaining the IP address when an Ethernet address is given, can be solved by using RARP (Reverse Address Resolution Protocol).
- The newly booted workstation is allowed to broadcast its Ethernet address. The RARP server after receiving this request, checks the Ethernet address in its files and finds the corresponding IP address. This IP address is then sent back.
- The disadvantage of RARP is that it uses a destination address of all 1s (limited broadcasting) to reach the RARP server.
- But such broadcasts are not forwarded by routers, so a RARP server is needed on each network.
- In order to get around this problem, another bootstrap protocol called BOOTP has been invented. Unlike RARP, it uses UDP messages which are forwarded over routers. It also provides a diskless workstation with additional information, including the IP address of the file server holding the memory image, the IP address of the default router and the subnet mask to use.

5.7.2 Solved Examples :

Ex. 5.7.1 : Find the sub-network address and the host id for the following.

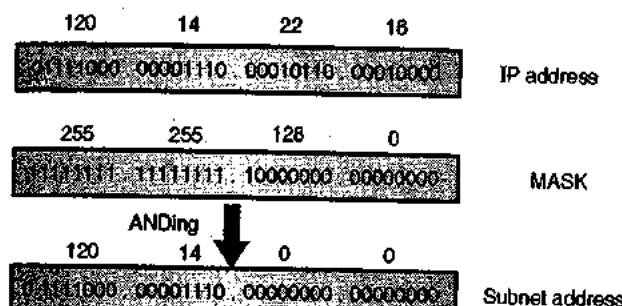
May 07, Dec. 09, 8 Marks

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 :



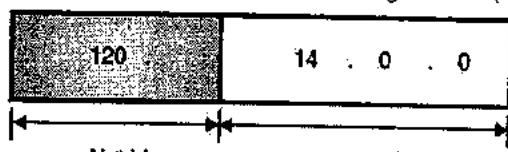
(G-53) Fig. P. 5.7.1(a)

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. 5.7.1(b).



(G-54) Fig. P. 5.7.1(b)

So the host id is 14.0.0.

- Similarly we can find the other host id.

Ex. 5.7.2 : 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?

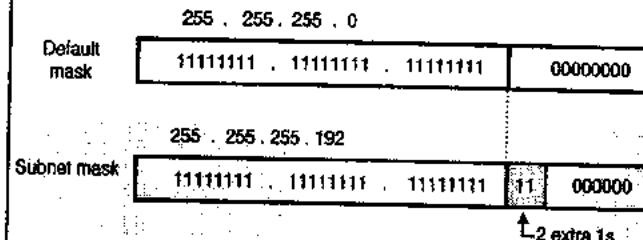
Soln. :

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. 5.7.2.



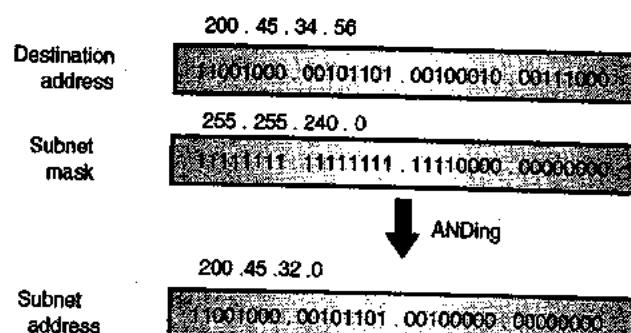
(G-55) Fig. P. 5.7.2

Thus the required subnet mask is 255.255.255.192.

Ex. 5.7.3 : What is the subnet address if the destination address is 200.45.34.56 and subnet mask is 255.255.240.0 ?

Soln. :

To find the subnet address we have to AND the IP address and the subnet mask as shown in Fig. P. 5.7.3.



(G-56) Fig. P. 5.7.3

Thus the required subnet address is 200.45.32.0

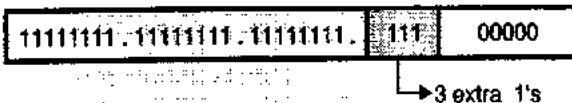
Ex. 5.7.4 : A company is granted a site address 201.70.64.0. The company needs six subnets. Design the subnets.

Feb. 16, 5 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. 5.7.4.



(G-557) Fig. P. 5.7.4

- In order to have six subnets, we can have 6 different combinations of the 3-extra 1s as shown in Table P. 5.7.4(a).

Table P. 5.7.4(a)

Combination n	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. 5.7.4(b).

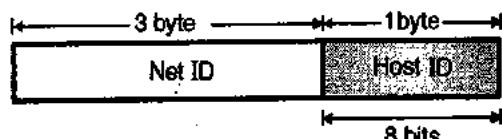
Table P. 5.7.4(b)

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. 5.7.5: For a given class C network 195.188.65.0 design equal subnets in such a way that each subnet has atleast 60 nodes.

Soln. :

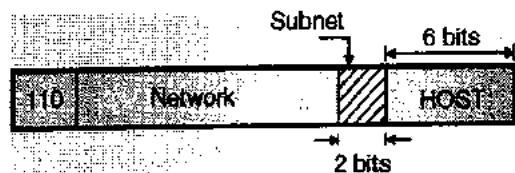
- Fig. P. 5.7.5(a) shows the structure of a class C address in which 3-bytes are reserved for net ID and 1-byte for host ID.



(G-558) Fig. P. 5.7.5(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. 5.7.5(b).



(G-559) Fig. P. 5.7.5(b)

- This shows that there will be four equal subnets each one having at least 60 nodes.

Ex. 5.7.6: Show by calculations how many networks each IP address class can have with one example?

Dec. 06, 4 Marks

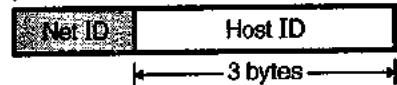
Soln. :

Number of networks in different IP address :

Class A address :

- The format of class A address is shown in Fig. P. 5.7.6(a). Here one byte defines the network ID and three bytes define the host ID.

→ 1 byte →

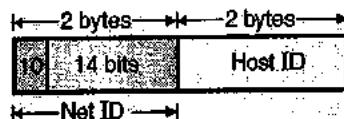


(G-560) Fig. P. 5.7.6(a) : Class A address

- The MSB in the network field is reserved. So actually there are only 7-bits in the network fields.
- So the number of networks in class A address will be 128.

Class B address :

- The format of class B address is shown in Fig. P. 5.7.6(b). Here 2-bytes are reserved for network field and remaining two bytes are for the host field.
- Out of 16-bits in the network field the first two bits (MSBs) are reserved. So actually 14 bits are available in the network field.



(G-561) Fig. P. 5.7.6(b) : Class B address

- So the number of networks in class B address is $2^{14} = 16,384$.

Class C address :

- The format of class C is shown in Fig. P. 5.7.6(c). Here 3-bytes are reserved for network field and only one byte for the host field.



- Out of 24-bits in the network field 3-bits are again reserved. So actually only 21-bits are available.



(G-562) Fig. P. 5.7.6(c) : Class C address

- So the number of networks in class C addresses is $2^{24} - 2 = 16,777,214$.

Ex. 5.7.7 : How many host per network in each IP address class can exist show with example? Dec. 06, 4 Marks

Soln. :

Number of hosts in different IP addresses :

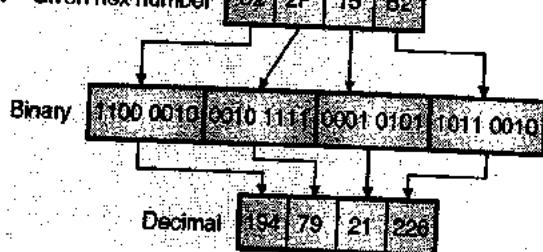
Class A : There are 3-bytes (24-bits) in the host field. Hence the number of hosts in class A address will be $2^{24} = 16,777,216$.

Class B : There are 2-bytes (16-bits) in the host field. So the number of hosts in class B address will be $2^{16} = 65,536$ i.e. 2^{16} per network.

Class C : There is 1-byte (8-bits) in the host field. So number of hosts in class C address will be $2^8 = 256$ per network.

Ex. 5.7.8 : Convert the IP address whose hexadecimal representation is C22F15B2 to dotted decimal notation.

Soln. : Given hex number **C2 2F 15 B2**



(G-563) Fig. P. 5.7.8

∴ The IP address in the dotted decimal notation is as follows :

192.79.21.226

Ex. 5.7.9 : A class B network on Internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts per subnet?

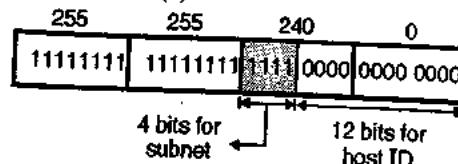
Dec. 07, 6 Marks

Soln. : The structure of class B address is as shown in Fig. P. 5.7.9(a).



(G-564) Fig. P. 5.7.9(a) : Class B address

The given subnet mask is 255.255.240.0. So it is as shown in Fig. P. 5.7.9(b).



(G-565) Fig. P. 5.7.9(b) : Subnet mask

Thus there are 4 extra 1s as shown in Fig. P. 5.7.9(b). So there will be 16 subnets and each subnet can have $2^{12} = 4096$ hosts.

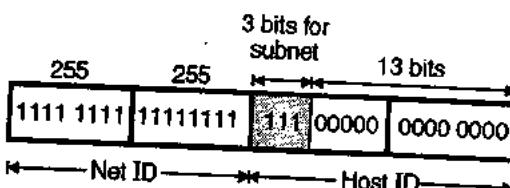
Ex. 5.7.10 : Perform the subnetting of the following IP address 160.111.X.X

Original subnet mask 255.255.0.0

Number of subnets 6 (six)

Soln. :

- The original subnet mask indicates that we are dealing with a class B address.
- In order to have six subnets we need to use 3 extra bits from the bits that are reserved for host ID. So the subnet mask is as shown in Fig. P. 5.7.10(a).



(G-566) Fig. P. 5.7.10(a)

- The 3-bits reserved for subnetting will have 8 combinations from 000 to 111 out of which any six combinations can be used for 6 subnets.
- Let us decide that the combinations 000 to 001 are not to be used. Then the subnet masks for the 6 possible subnets will have the following addresses.

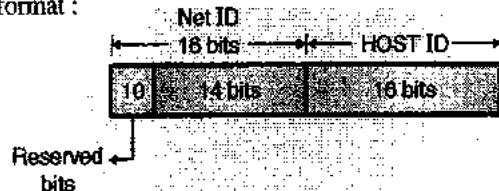
Subnet 1	255.255.64.0
Subnet 2	255.255.96.0
Subnet 3	255.255.128.0
Subnet 4	255.255.160.0
Subnet 5	255.255.192.0
Subnet 6	255.255.224.0

Ex. 5.7.11 : 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.

Dec. 07, 6 Marks

Soln. :

- Fig. P. 5.7.11(a) shows the original class B address format :



(G-567) Fig. P. 5.7.11(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. 5.7.11(b).

$$\therefore \text{Number of class B networks} = 2^{18} = 2,61,888$$



(G-568) Fig. P. 5.7.11(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. 5.7.12 : IPv6 uses 16-byte addresses. If a block of 1 million addresses is allocated every picosecond, how long will the addresses last?

Soln. :

- Total number of address bits $= 16 \times 8 = 128$
- Number of addresses $= 2^{128} = 3.4 \times 10^{38}$
- One picosecond $= 1 \times 10^{-12}$ seconds
- 1 million addresses $= 1 \times 10^6$ address

$$\therefore 1 \text{ picosecond} = 1 \times 10^6 \text{ addresses}$$

$$\therefore x = 3.4 \times 10^{38}$$

$$\therefore x = \frac{3.4 \times 10^{38}}{1 \times 10^6} \times 1 \text{ picoseconds}$$

$$= 3.4 \times 10^{32} \text{ picoseconds}$$

$$= 3.4 \times 10^{20} \text{ seconds}$$

$$= 9.44 \times 10^{16} \text{ hours}$$

$$= 3.9352 \times 10^{15} \text{ days} = 1.0781 \times 10^{13} \text{ years}$$

Ex. 5.7.13 : For a given class-C network, design 4 equal subnets having minimum 50 nodes in each subnetwork.

Soln. :

The default mask for a class C network is

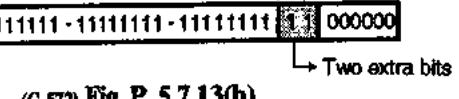
255.255.255.0

This is as shown in Fig. P. 5.7.13(a).

Default mask : 

(G-571) Fig. P. 5.7.13(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. 5.7.13(b).

Subnet mask : 

(G-572) Fig. P. 5.7.13(b)

In order to have four subnets, we can have four different combinations of the two extra bits as shown in Table P. 5.7.13(a).

Table P. 5.7.13(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. 5.7.13(b).

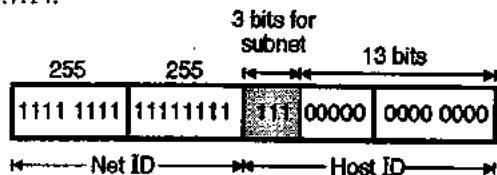
Table P. 5.7.13(b)

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. 5.7.14 : 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?

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. 5.7.14.



(G-56) Fig. P. 5.7.14

- 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.

$$\therefore \text{No. of hosts in each subnet} = 2^{13} = 8192 \dots \text{Ans.}$$

Ex. 5.7.15 : 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 ?

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. 5.7.15.
- In order to have four subnets we can have the 4 combinations of the two extra 1s as shown in Table P. 5.7.15.

Table P. 5.7.15

Combination	Subnet Number
00	Subnet 1
01	Subnet 2
10	Subnet 3
11	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.

$$\therefore \text{No. of hosts/subnet} = 2^6 = 64.$$

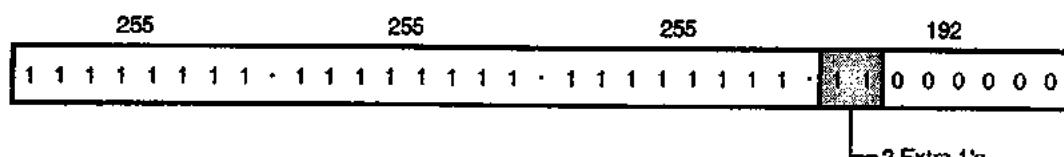
Ex. 5.7.16 : Consider any class - C network with default subnet mask. Design the subnet in such a way that each has 62 nodes. Write the range of IP addresses for all subnets.

Soln. : Refer Ex. 5.7.15.

- 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. 5.7.16(a).

Table P. 5.7.16(a)

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



(G-57) Fig. P. 5.7.15



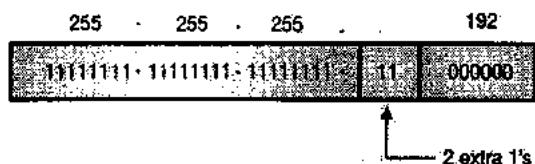
Ex. 5.7.17: For a given C class network 210.50.60.0, how will you divide it into 4 equal subnets? What will be the new subnet mask? Give the network and broadcast address of each subnetwork.

Soln. :

Given : IP address : 210.50.60.0 (class C)

Step 1 : Subnet mask :

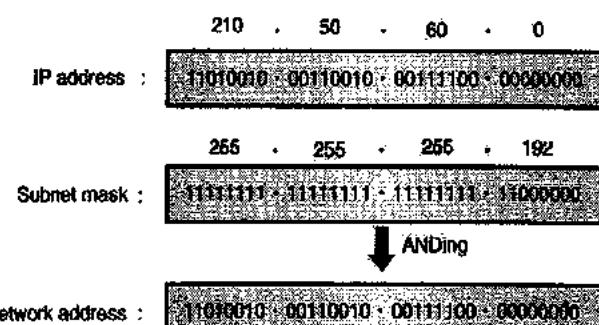
This is class C network. So default mask is given by 255.255.255.0



(G-1483) Fig. P. 5.7.17(a) : Subnet mask

The new subnet mask is 255.255.255.192 ...Ans.

Step 2 : Find network address :

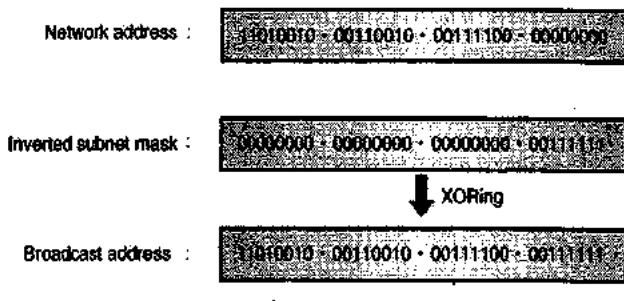


(G-1484) Fig. P. 5.7.17(b)

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.



(G-1485) Fig. P. 5.7.17(c)

The broadcast address is 210.50.60.63 ...Ans.

5.8 ICMP (Internet Control Message Protocol) :

SPPU : Dec. 11, May 12, Dec. 13, Feb. 16

University Questions

Q. 1 Compare IP and ICMP. Explain header format of ICMPv6 protocol. (Dec. 11, 8 Marks)

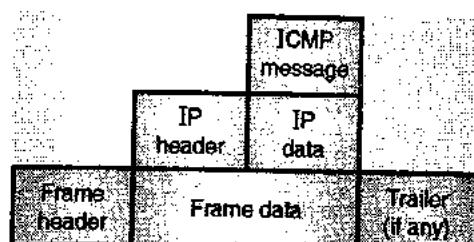
Q. 2 State which transport layer protocol is used by the following protocols - HTTP, FTP, DHCP, DNS, ICMP, TFTP, IP, SMTP. (Dec. 11, 4 Marks)

Q. 3 What is ICMP? Write a note on ICMP messages. (May 12, 8 Marks)

Q. 4 What is ICMP? Explain the functionalities which make this protocol effective. (Dec. 13, 8 Marks)

Q. 5 Explain ICMP in detail. (Feb. 16, 4 Marks)

- The IP provides unreliable and connectionless datagram delivery, and makes an efficient use of network resources.
- IP is a best-effort delivery (which does not provide any guarantee) service that takes a datagram from its original source to its final destination. However, IP has two drawbacks :
 1. It does not have any error control mechanism.
 2. It does not have any assistance mechanism.
- The Internet Control Message Protocol (ICMP) is used to overcome these drawbacks. It is used alongwith IP. It reports presence of errors and sends the control messages on behalf of IP.
- ICMP does not attempt to make IP a reliable protocol. It simply attempts to report errors and provide feedback on specific conditions. ICMP messages are carried as IP packets and are therefore unreliable. ICMP is a network layer protocol.
- IP also lacks a mechanism for host and management queries. A host sometimes wants to know if a router or another host is operating or dead. And sometimes a network manager needs information from another computer on the network (such as host or router).
- ICMP operates in the network layer but its messages are not passed directly to the data link layer. Instead, the messages are first encapsulated inside IP datagrams and then sent to the lower layer.
- This is as shown in Fig. 5.8.1.



(G-583) Fig. 5.8.1 : ICMP encapsulation

- The ping command uses ICMP as a probe to test whether a station is reachable. Ping packages an ICMP echo request message in a datagram and sends it to a selected destination. The user chooses the destination by specifying its IP address or name on the command line in a form such as :

ping 100.50.25.1

- When the destination receives the echo request message, it responds by sending an ICMP echo reply message. If a reply is not returned within a set time, ping resends the echo request several more times. If no reply arrives, ping indicates that the destination is unreachable.
- Another utility that uses ICMP is trace route, which provides a list of all the routers along the path to a specified destination.

5.8.1 Types of Messages :

SPPU : May 12, Dec. 12

University Questions

- Q. 1** What is ICMP ? Write a note on ICMP messages.
(May 12, 8 Marks)
- Q. 2** Describe in brief ICMP error and query messages (at least 2 each).
(Dec. 12, 8 Marks)

- ICMP messages are of two types :
 - Error reporting messages
 - Query messages.

Error reporting messages :

- One of the important responsibilities of ICMP is to report the presence of an error. IP is an unreliable protocol. So error checking and control are not done by IP.
- So ICMP was designed to assist IP. But ICMP does not correct the errors. It simply reports them and leaves the error correction job to the higher level protocols.

- ICMP always sends the error reporting messages back to the original source.
- ICMP has five types of error reporting messages. Fig. 5.8.2 shows different types of error reporting messages.

Destination unreachable :

When a router cannot forward or deliver an IP packet, it sends a destination unreachable ICMP message back to the source which originated the packet.

Source quench message :

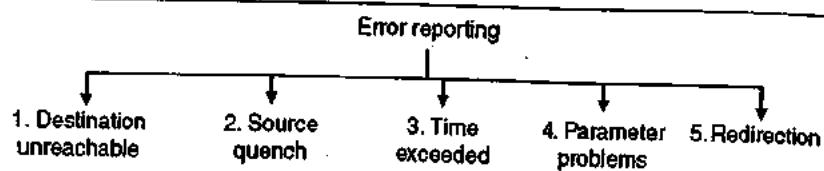
- A host or router uses source quench messages in order to tell the original source that congestion has occurred and to request it to reduce its current rate of packet transmission.
- There is no flow control or congestion control mechanism in IP. So the source quench message in ICMP is designed to add some kind of flow control and congestion control to IP.
- This message serves two purposes :
 - It tells the source that the packet has been discarded and,
 - It gives a warning to the source that the source should slow down (quench) because congestion has taken place somewhere.

Time exceeded message :

- This message is generated in two cases :
 - If a router receives a packet with a 0 in the TTL field then it discards that datagram and send a time exceeded message back to the source originating that packet.
 - If all the fragments which are parts of a message do not arrive at the destination host within a certain time limit then time exceeded message is sent back.

Parameter problem message :

- There should not be any ambiguity in the header part of the packet. If a router or destination host comes across such ambiguity or missing value in any field of the datagram then it simply discards that datagram and sends the parameter problem message back to the source originating that message.



(G-584) Fig. 5.8.2 : Error reporting messages

**Redirection message :**

- If a router or host wants to send a packet to another network then it should know the IP address of the next router.
- The routers and hosts must have a routing table to find the address of the next router and the routing table has to be updated automatically on a continuous basis. The redirection message is used for such updating.
- The ICMP sends a redirection message back to its host to carry out an automatic periodic updating.

5.8.2 Query :

SPPU : Dec. 12

University Questions

- Q.1** Describe in brief ICMP error and query messages (at least 2 each). (Dec. 12, 8 Marks)
- The ICMP can diagnose some of the network problems. This is in addition with the error reporting feature. Such a diagnosis is done through the query messages.
 - The query messages is a group of four different pairs of messages as shown in Fig. 5.8.3.

1. Echo request and reply :

- This is a pair of two messages namely echo request and echo reply messages and they are designed for the purpose of diagnosis.
- This pair of messages determines whether two systems (hosts or routers) can successfully communicate with each other.

2. Time stamp request and reply :

- This pair of messages can be used by the hosts and routers to find out the round trip time that an IP datagram needs to travel between them.
- It can also be used for synchronizing the clock signals used in the two machines (hosts or routers).

3. Address mask request and reply :

- The IP address of a host contains a network address, subnet address and host identifier.
- A host may know its full IP address but may not know it is divided into three parts mentioned above.
- So it can send an address mask request message to the router. The router then sends back the address mask reply message.

4. Router solicitation and advertisement :

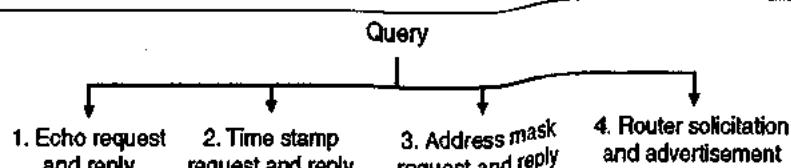
- A host that wants to send data to a host on another network must know the address of routers connected to its own network.
- In such situations the router solicitation and advertisement messages can help.
- A host can broadcast or multicast a router solicitation message. The routers receiving this message can broadcast their routing information using the router advertisement message.

5.8.3 Different Types of Messages in ICMPv6 :

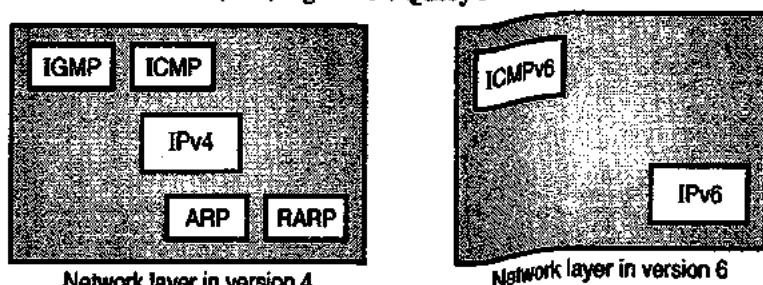
SPPU : May 13

University Questions**Q.1 Explain different types of messages in ICMPv6. (May 13, 8 Marks)**

- We know that IPv4 was modified into IPv6. Similarly ICMPv4 is modified in ICMPv6. This new modified protocol is more suitable to IPv6.
- Fig. 5.8.4 compares the network layers in version 4 and version 6.
- The ARP and IGMP protocols in version 4 are combined in ICMPv6. The RARP protocol has been dropped from the protocol suite as it is not used very frequently.



(G-585) Fig. 5.8.3 : Query messages



(G-1424)Fig. 5.8.4 : Comparison of network layers

- Similar to ICMPv4, the messages in ICMPv6 are divided into two types :
 - Error reporting messages.
 - Query messages.
- However each category has more types of messages in ICMPv6 as compared to those in ICMPv4.

Error reporting :

- ICMPv6 can handle five types of errors. They are :
 - Destination unreachable
 - Packet too big.
 - Time exceeded
 - Parameter problems and
 - Redirection.
- Note that the source quench error message in ICMPv4 has been eliminated in ICMPv6 and packet too big has been newly included.
- The following four messages in ICMPv6 work in a similar or identical manner as those in ICMPv4 :
 - Destination unreachable
 - Time exceeded
 - Parameter problem
 - Redirection.
- The only different error message is packet too big.

Packet too big :

- If a router receives a datagram that is larger than the maximum transmission unit (MTU) size of the network through which the datagram should pass, then two things happen :
 - The router discards the datagram.
 - Then ICMP error packet i.e. a packet too big message is sent to the source originating that message.

Query messages :

- These are the additional messages, that an ICMP can send after diagnosis of some other network problems.
- Here four different groups of messages have been defined :
 - Echo request and reply.
 - Router solicitation and advertisement
 - Neighbour solicitation and advertisement
 - Group membership.
- Two types of query messages present in ICMPv4 have been eliminated in ICMPv6. They are :
 - Time stamp request and reply.
 - Address mask request and reply.
- The first two out of the four groups of messages in ICMPv6 have the similar / identical operation as those in the ICMPv4. The two messages having a different operation are as follows :

Neighbour solicitation and advertisement :

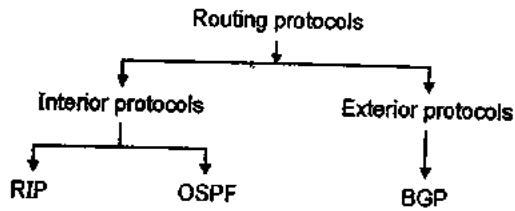
- A network layer in version 4 contains the ARP. But in ICMPv6 ARP has been eliminated and its duties are included in ICMPv6.
- The principle has remained the same, but the format of the message has changed.

Group membership :

- A network layer in version 4 contains an independent protocol called IGMP. But in version 6 this protocol has been eliminated and its duties are included in ICMPv6. The purpose is same.

5.9 Unicast Routing Protocols :

- Various unicast routing protocols are shown in Fig. 5.9.1.
- 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. 5.9.1 : Unicast routing protocols

- RIP and OSPF are used to upgrade the routing tables inside an AS, and BGP is used for upgrading the routing tables for the routers which join multiple AS. together.

5.10 RIP (Routing Information Protocol) :

SPPU Dec. 07, Dec. 12

University Questions

Q. 1 Compare and contrast the advertisement used by RIP and OSPF routing protocols.
(Dec. 07, 6 Marks)

Q. 2 Explain routing protocols RIP and BGP.
(Dec. 12, 8 Marks)

- 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.

Routing table :

- A typical routing table is shown in Table 5.10.1. Every router is supposed to keep such a table with it.

Table 5.10.1 : 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 5.10.1 may include information such as subnet mask or the time this entry was last updated.

5.10.1 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.

5.10.2 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.

5.10.3 Updating the Routing Table :

- When RIP messages are received, each routing table is updated using the RIP updating algorithm as discussed earlier.

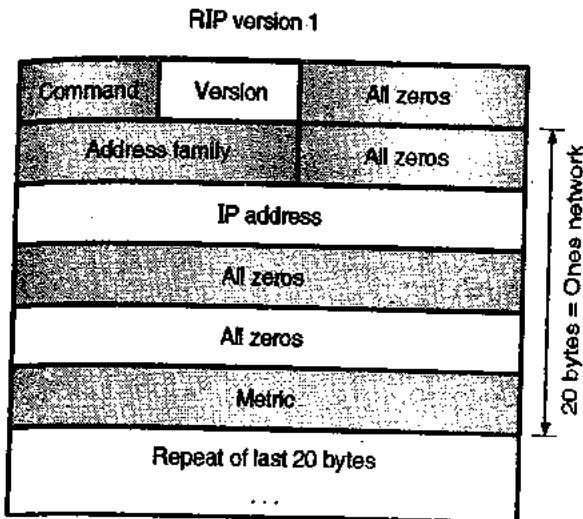
5.10.4 RIP Operation :

- 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.

5.10.5 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.



(G-499) Fig. 5.10.1 : RIP Message Format

- The summary of the RIP packet format fields illustrated in Fig. 5.10.1, is as follows :

(a) 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.

(b) Version number :

This field specifies the RIP version used. This field can signal different potentially incompatible versions.

(c) 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.

(d) Address-family identifier (AFI) :

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.

(e) Address :

This field is used to specify the IP address for the entry.

(f) Metric :

This field indicates the number of hops (routers) 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.

5.10.6 Disadvantages of RIPv1 :

- RIPv1 only understands the shortest route to a destination, based on simple count of number of router hops.
- It depends on other routers for computed routing updates.
- Routing tables can get large and these are broadcasted every 30 seconds.
- Distances are based on hops, not on real costs (such as the speed of link).
- 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.
- If we solve one problem another appears.

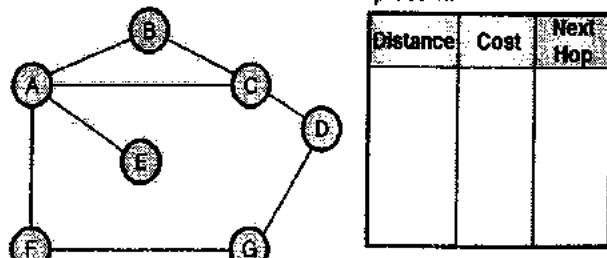
5.10.7 RIP Version 2 :

- 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. 5.10.1: Complete the final routing table at node A using RIP protocol for the following network. Assume the cost of hop count.



(G-50) Fig. P. 5.10.1

Soln. : Table P. 5.10.1 : Routing table at A

Destination n	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

5.11 OSPF Routing Protocol :

SPPU: Dec. 11, May 13

University Questions

- Q.1** Write short note on OSPF protocol. (Dec. 11, 4 Marks)
Q.2 Explain in detail OSPF protocol. (May 13, 8 Marks)

- 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.

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 :

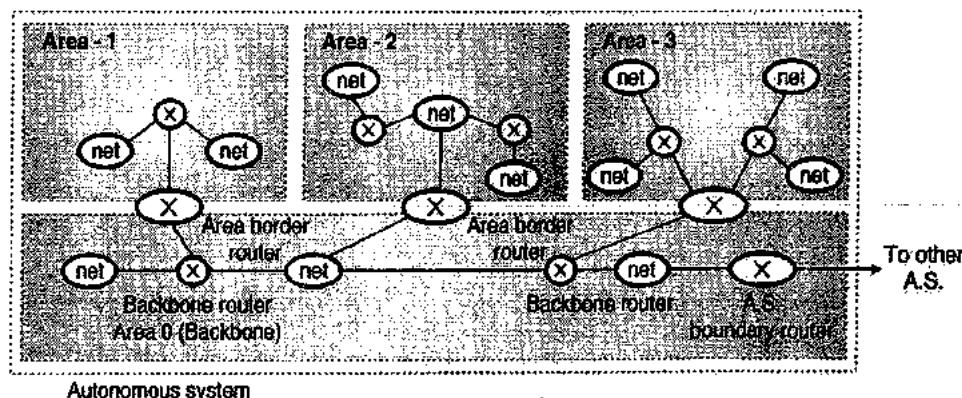
- The routers inside the backbone are called as the backbone routers. But a backbone router can also work as an area border router.

Area identification :

- Each area has an area identification. The area identification of the backbone is zero. An autonomous system is as shown in Fig. 5.11.1(a).

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.



(G-1786) Fig. 5.11.1(a) : Autonomous system



- 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.

5.11.1 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. 5.11.1(a)).

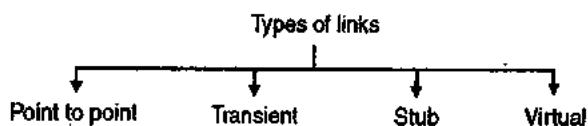
- The protocols used to support OSPF routing include database broadcast packets and link state change broadcasts. A "Hello" protocol is used to detect changes in the availability of adjacent routers.

5.11.2 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.

5.11.3 Types of Links :

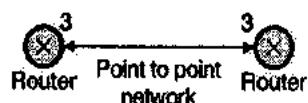
- In the OSPF protocol terminology, a connection is called as a link. OSPF defines four types of links called point to point, transient link, stub link and virtual links as shown in Fig. 5.11.1(b).



(G-501) Fig. 5.11.1(b) : Types of links

1. Point to point :

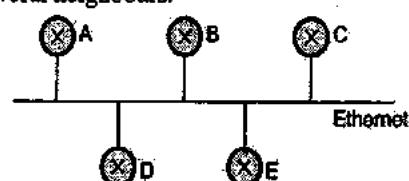
- A point to point link is defined as the link (connection) that directly connects two router without any other host or router present inbetween. An example of such a link is two routers connected by a telephone line.
- Each router has only one neighbour at the other side of the link. This is shown in Fig. 5.11.2. 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.



(G-502(a)) Fig. 5.11.2 : Point to point link

2. Transient link :

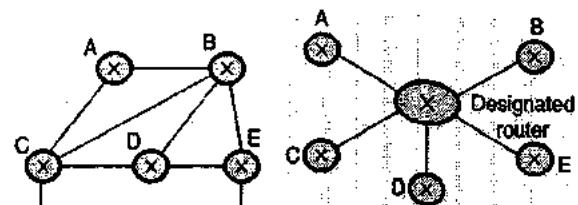
- It is a network having many routers attached to it as shown in Fig. 5.11.3. All LANs and some WANs are of this type.
- A, B, C etc. are the routers. Each router has several neighbours.



(G-503) Fig. 5.11.3 : Transient link

- The relationship between the neighbouring routers is as shown in Fig. 5.11.4(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. 5.11.4(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. 5.11.4(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-178) Fig. 5.11.4

- 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. 5.11.5.

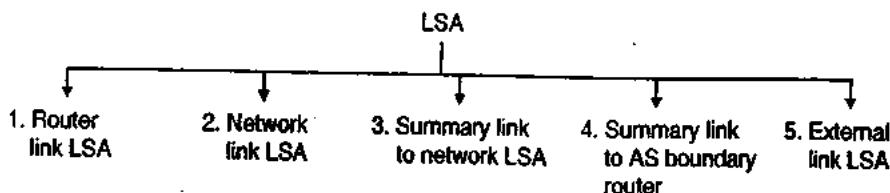


(a) Stub network

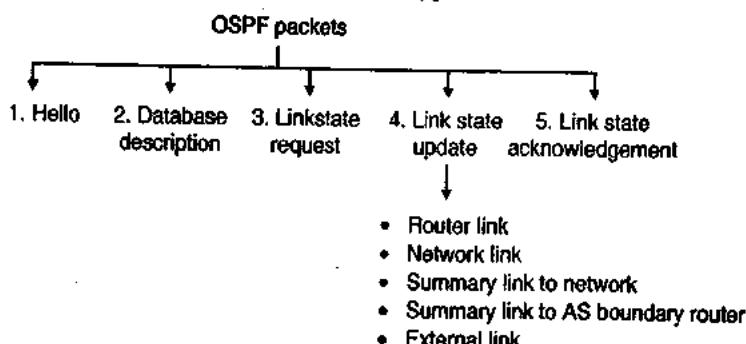
(b) Representation

(G-504) Fig. 5.11.5

- The stub network of Fig. 5.11.5(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. 5.11.5(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.



(G-505) Fig. 5.11.6 : Types of LSAs



(G-506) Fig. 5.11.7 : OSPF packet types

5.11.4 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. 5.11.6.

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.

5.11.5 OSPF Packet Types :

SPPU : Dec. 15

University Questions

- Q. 1** Draw the packet header format of OSPF and explain in detail. (Dec. 15, 6 Marks)

- Different types of OSPF packets are as shown in Fig. 5.11.7.
- 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.

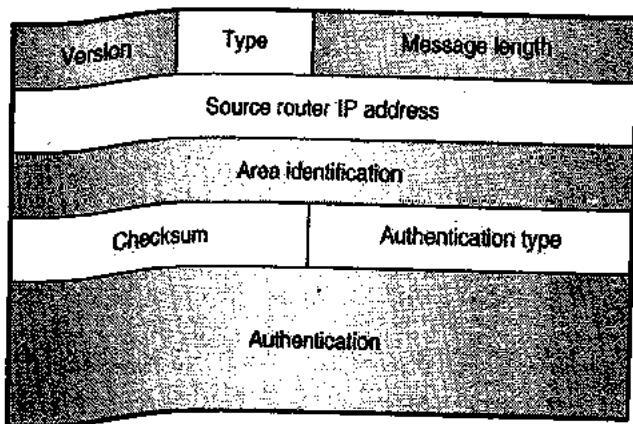
The OSPF makes use of five different packet types.

- Hello :** Used to discover and maintain neighbours.
- 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.

OSPF Packet Format :



(G-507) Fig. 5.11.8 : OSPF packet header

- All OSPF packets have the same common header which is as shown in Fig. 5.11.8. This header is same for all the five packet types of OSPF.
- 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 be 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.

5.11.6 Comparison between RIP and OSPF :

SPPU : Dec. 07

University Questions

Q.1 Compare and contrast the advertisement used by RIP and OSPF routing protocols.

(Dec. 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



Function/Feature	RIPv1	RIPv2	OSPF
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

5.12 Border Gateway Protocol :

SPPU Dec 12

University Questions

Q.1 Explain routing protocols of RIP and BGP.

(Dec. 12, 8 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.

5.12.1 Path Vector Routing :

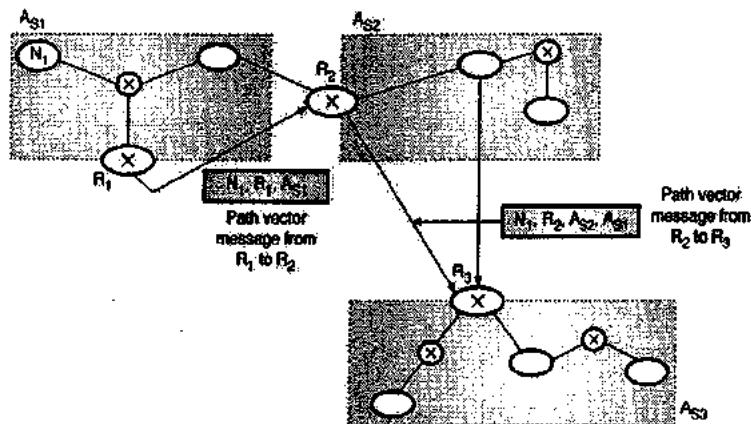
- It is different from both distance vector routing and link state routing.
- Table 5.12.1 shows the example of a path routing table. Each entry in the routing table will have the information about the destination network, the next router and the path to reach the destination.

Table 5.12.1 : Path vector routing table

Network	Next router	Path
N01	R01	AS 12, AS 21, AS 56
N02	R08	AS 20, AS 57, AS 06
•	•	•
•	•	•
•	•	•

5.12.2 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. 5.12.1.
- Fig. 5.12.1 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. 5.12.1.



(G-1788) Fig. 5.12.1 : Path vector messages

5.12.3 Loop Prevention :

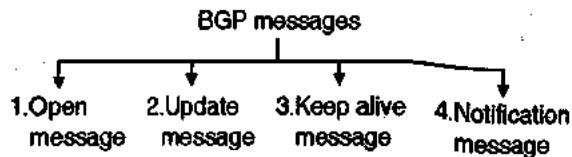
- When a message is received, a router checks it to see if its autonomous system is in the path list to the destination. If it is present it indicates looping is involved which is undesirable and the message is ignored.
- In this way the looping problem and the associated instability which is present in distance vector routing is avoided in path vector routing.

5.12.4 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 :
 - A well known attribute and
 - 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 :
 - Well known mandatory attributes
 - Well known discretionary attributes
- The optional attributes also are classified into two types :
 - An optional transitive attribute
 - An optional nontransitive attribute

5.12.5 Types of Messages :

- BGP uses four different types of messages, as shown in Fig. 5.12.2.



(G-508) Fig. 5.12.2 : BGP message types

1. Open message :

- A BGP router creates a neighbourhood relationship with its neighbour by opening a connection and sending an open message to the intended neighbour.
- If the neighbour is willing to accept the relationship, then it sends back the keep alive message.

2. Update message :

- This is the most important BGP message. It is used by a BGP routers for one or both the tasks mentioned below :
 - In order to withdraw the destinations that were announced earlier.
 - Announcement of a route to new destination.
 - In an update message BGP can withdraw multiple destinations but it can announce only one new destination route.

3. Keep-alive message :

All the BGP routers (also called as peers) exchange these messages among them regularly so as to convey an information that they are alive.

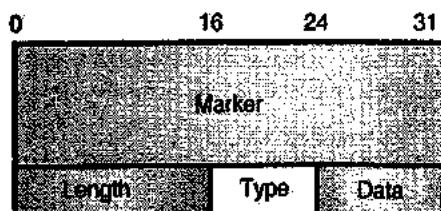
4. Notification message :

A BGP router (peer) would send the notification method under the following circumstances :

- When it detects an error condition
- When it wants to close the connection.

BGP Header Format :

- 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. 5.12.3 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-509) Fig. 5.12.3 : BGP packet header

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

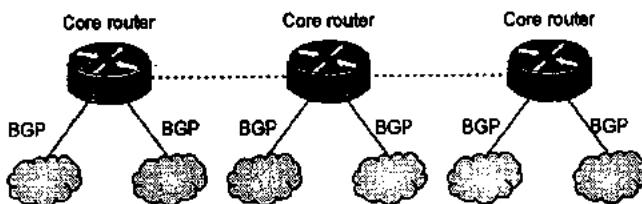
Data :

Contains the upper layer information in this optional field.

5.12.6 BGP Operation :

- Routing involves two basic activities : determination of optimal routing paths and the transport of information groups (i.e. packets) through an internetwork.
- To send and receive packets through an internetwork is relatively straightforward. However deciding the path or route for the packets can be very complex. One protocol that can be used for path determination in today's networks is the Border Gateway Protocol (BGP). The BGP has been designed to perform the interdomain routing in Transmission-Control Protocol/Internet Protocol (TCP/IP) networks.
- BGP is an exterior gateway protocol (EGP), which means that it performs routing between multiple autonomous systems (ASs) or domains and exchanges routing and reachability information with other BGP systems.

- BGP was developed to replace the Exterior Gateway Protocol (EGP), which is now obsolete as the standard exterior gateway-routing protocol used in the global Internet. BGP solves some serious problems associated with EGP to help Internet grow more efficiently.
- Note that EGP is a particular instance of an exterior gateway protocol (also EGP), the two should not be confused. Fig. 5.12.4 illustrates core routers using BGP to route traffic between autonomous systems.



(G-510) Fig. 5.12.4 : Core routers can use BGP to route traffic between autonomous systems

IGPs and EGPs :

- A router in a transit AS may have extremely large routing tables (up to 90,000 networks amounting to over 30Mb) and BGP-4 uses **Classless Inter Domain Routing (CIDR)** to slow the growth of these tables.
- The router maintains routing tables for the IGP (Interior Gateway Protocol) as well as the BGP and information can be exchanged between them.
- There are two types of sessions between a router and its neighbours :
 1. **Exterior Gateway Protocol (EGP)** sessions are designed to take place between routers in different ASs, which are usually next to each other sharing the same media and subnet.
 2. **Interior Gateway Protocol (IGP)** sessions are designed to take place between routers within the same AS and these sessions are used to synchronize the routing policy within an AS. These routers do not have to be next to each other however they should be able to see each other so that a TCP connection can be made between them! You would configure these if you needed to pass BGP information to other ASs.
- Interior Gateway protocols use metric interface costs (OSPF) or hop counts (RIP) to determine the best paths.
- Exterior Gateway Protocols link varying IGPs and use administered routing policies to determine best paths through service providers.
- Originally EGP was used with the old Internet topology, which, due to its small size, was a simple two-tier model with a core AS and the additional ASs around it.



- An AS was given a 16-bit number and every 3 minutes EGP advertised the routes that it knew with other EGP peers via a full class IP address (no subnets) and a metric from 1 to 255, with 255 being unreachable. EGP is considered obsolete except in large private networks.
- The main problem with EGP is that it could not cope with a meshed network of ASs, EGP could not detect loops and had no way of creating policies for routing. EGP was merely a reachability protocol rather than a routing protocol.

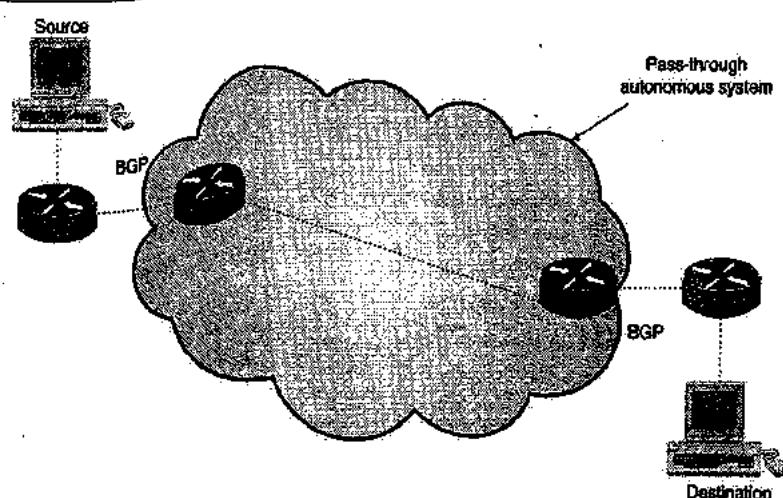
How does BGP operate ?

- BGP performs three types of routing: inter autonomous system routing, intra-autonomous system routing, and pass-through autonomous system routing.
- Inter autonomous system routing would take place between two or more BGP routers in different autonomous systems. Peer routers in these systems use BGP so that they can maintain a consistent view of the internetwork topology.
- BGP neighbours communicating between autonomous systems must be members of the same physical network. The Internet serves as an example of an entity that uses this type of routing because it is made of autonomous systems or administrative domains. Many of these domains correspond to various institutions, corporations, and entities that make up the Internet. BGP is frequently used to determine the path which results in optimal routing within the Internet.
- Intra-autonomous system routing takes place between two or more BGP routers that are located within the same autonomous system. Peer routers within the same autonomous system use BGP so that they can maintain a consistent view of the system topology.

- BGP also is used to determine which router will serve as the connection point for specific external autonomous systems. Once again, the Internet itself is the example of inter autonomous system routing. An organization, such as a university, could make use of BGP to provide optimal routing within its own administrative set up or autonomous system. The BGP protocol can provide both inter- and intra-autonomous system routing services.
- The pass-through autonomous system routing takes place between two or more BGP peer routers that exchange traffic across an autonomous system that does not run BGP. In a pass-through autonomous system environment, the BGP does not deal with the traffic that originates within the autonomous system in question and is not destined for a node in the autonomous system. BGP must interact with whatever intra-autonomous system routing protocol is being used to successfully transport BGP traffic through that autonomous system. Fig. 5.12.5 illustrates a pass-through autonomous system environment: BGP pairs with another intra-autonomous system-routing protocol.

5.12.7 BGP Routing :

- Similar to any routing protocol, BGP maintains routing tables, transmits routing updates, and makes the routing decisions based on routing metrics. The main function of a BGP system is to exchange network-reachability information, which includes the information about the list of autonomous system paths, with other BGP systems. This information can be used to construct a graph of autonomous system connectivity which can be used to determine the routing loops and with which autonomous system-level policy decisions can be enforced.



(G-51) Fig. 5.12.5 : Intra-autonomous system-routing protocol

- Each BGP router maintains a routing table that contains a list of all the feasible paths to a particular network. The router does not refresh the routing table, however. Instead, routing information received from peer routers is retained until an incremental update is received.
- BGP devices exchange routing information when initial data is exchanged and after incremental updates. When a router first connects to the network, BGP routers exchange their entire BGP routing tables. Similarly, when the routing table changes, routers send the portion of their routing table that has changed. BGP routers do not send regularly scheduled routing updates, and BGP routing updates advertise only the optimal path to a network.
- BGP uses a single routing metric to determine the best path to a given network. This metric consists of an arbitrary unit number that specifies the degree of preference of a particular link. The BGP metric is assigned to each link by the network administrator. The value assigned to a link can be based on a number of criteria, including the number of autonomous systems through which the path passes stability, speed, delay or cost.

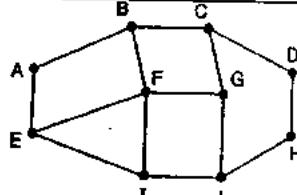
5.12.8 How does BGP Solve the Count to Infinity Problem ?

- 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. 5.12.6 shows a set of BGP routers and Table 5.12.2 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. 5.12.6 crashes, or if the line FG becomes faulty, then router F receives routes from the remaining three neighbours i.e. B, I and E.

- As shown in Table 5.12.2, these routes are BCD, IFGCD and EFGCD.

Table 5.12.2 : 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.



(G-512) Fig. 5.12.6 : A set of BGP router

- 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.

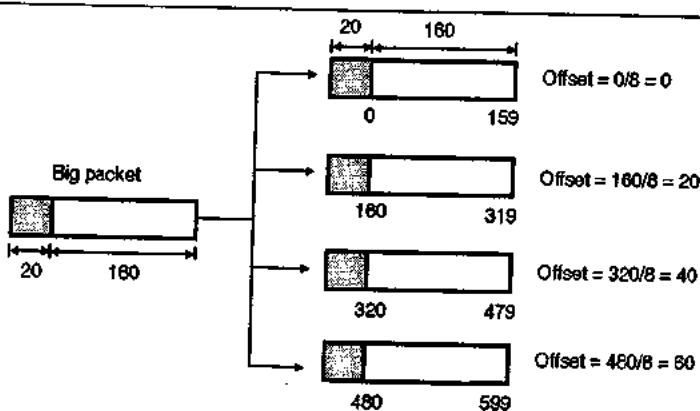
5.13 Solved Examples :

Ex. 5.13.1 :- Suppose a router receives an IP packet containing 600 data bytes and has to forward the packet to a network with maximum transmission unit of 200 bytes. Assume that IP header is 20 bytes long. Show the fragments that the router creates and specify the relevant values in each fragment header.

May 11, 8 Marks

Soln. :

We can divide the 600 data bytes into 4 fragments with first three containing 160 data bytes each and the fourth one contains 120 data bytes. The IP header (20 bytes) will contain the packet number and sequence number. The fragmentation is shown in Fig. P. 5.13.1.



(G-513) Fig. P. 5.13.1 : Fragmentation

Ex. 5.13.2. Divide the network 220.125.5.192/26 into 4 sub networks. How many hosts can be connected in each network ? Show their IP range, network address and broadcast address.

Dec. 11, 8 Marks

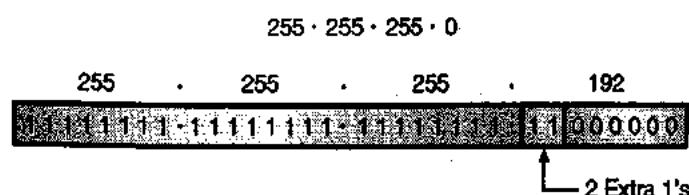
Soln. :

Given : IP address : 220.125.5.192/26

Step 1 : Subnet mask :

- This is class C network. So default mask is given by,
- The subnet mask is given by,
255.255.255.192
- Total number of hosts connected in each network are 64.

Step 2 : Network address :



(G-1504) Fig. P. 5.13.2 : Subnet mask

IP address : 220 . 125 . 5 . 192
01110000111010000000101110000000

Subnet mask : 11111111.11111111.11111111.11000000
11111111.11111111.11111111.11000000

(G-1505)

Network address : 220 . 125 . 5 . 192
01110000111010000000101110000000

- Network address is,

220.125.5.192

Step 3 : Broadcast address :

- To find broadcast address, take the inverted subnet mask and perform XOR with the network address.

Network address : 01110000111010000000101110000000

(G-1506)

00000000.00000000.00000000.00111111
00000000.00000000.00000000.00111111

XORing

01110000111101000000101111111111
01110000111101000000101111111111

- The broadcast address is,

220.125.5.255



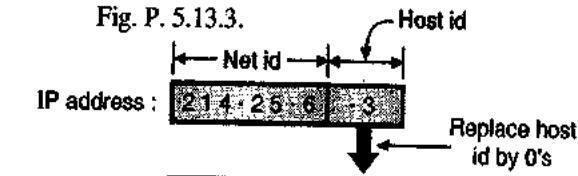
Ex. 5.13.3 : Identify class, subnet mask, network address and broadcast address of following IP addresses

- | | |
|---------------|-----------------|
| 1. 214.25.6.3 | 2. 191.5.8.9 |
| 3. 5.6.45.4 | 4. 230.45.89.63 |

Dec. 11, 8 Marks

Soln. :**1. 214.25.6.3**

- Examine the first byte. Its value is 214 i.e. it is between 192-223. So it is class C network.
- Subnet mask for class C address is 255.255.255.0.
- The net id and host id are as shown in Fig. P. 5.13.3.



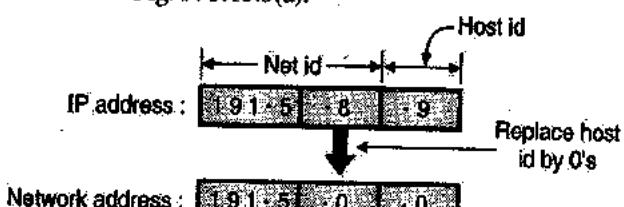
Network address : [214] . [25] . [6] . [0]

Broadcast address : [214] . [25] . [6] . [255]

(G-1507) Fig. P. 5.13.3

2. 191.5.8.9

- Examine the first byte. Its value is 191 i.e. it is between 128-191. So it is class B network.
- Subnet mask for class B address is 255.255.0.0.
- The net id and host id are as shown in Fig. P. 5.13.3(a).



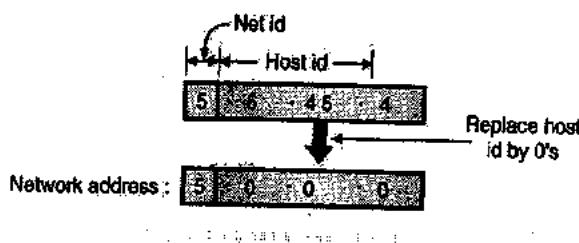
Network address : [191] . [5] . [0] . [0]

Broadcast address : [191] . [5] . [255] . [255]

(G-1508) Fig. P. 5.13.3(a)

3. 5.6.45.4

- Examine the first byte. Its value is 5 i.e. it is between 0 to 127. So it is class A network.
- Subnet mask for class A network is 255.0.0.0.
- The net id and host id are as shown in Fig. P. 5.13.3(b).



(G-1509) Fig. P. 5.13.3(b)

4. 230.45.89.63

- Examine the first byte. Its value is 230 i.e. it is between 224-239. So it is class D network.
- The net id and host id are as shown in Fig. P. 5.13.3(c).



Fig. P. 5.13.3(c)

Ex. 5.13.4 : 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. 195.46.63.10 | 2. 192.53.56.7 |
|-----------------|----------------|

Dec. 11, 8 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 :
 - 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.
 - 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.
 - 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.
 - The network number was then searched in the A, B or C table.
 - 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.

Soln. 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 shown in Fig. A.

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 shown in Fig. B.

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.

Ex. 5.13.5: A router is networking four different networks with network addresses 180.70.65.192/26, 180.70.65.128/25, 201.4.16.0/22 and default router on 180.70.65.200 make a routing table for this router and explain the forwarding process for a 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. 5.13.5.

$$\text{IP} = 135.46.63.10 = 10000111.00101110.00111111.00001010$$

$$22 \text{ bit mask} = 255.255.252.0 = 11111111.11111111.11111100.00000000$$

$$\text{IP AND Mask} = 10000111.00101110.00111100.00000000$$

$$\therefore \text{IP AND Mask} = 135.46.60.0$$

(G-1973) Fig. A

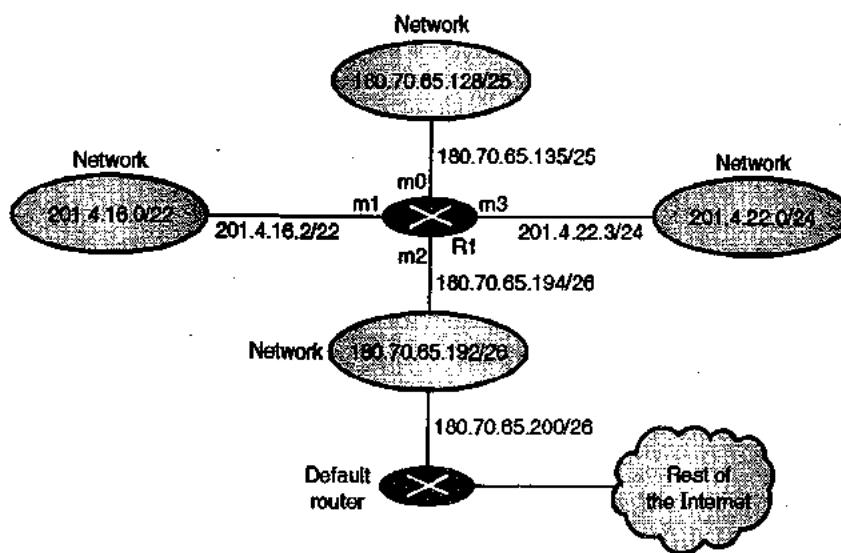
$$\text{IP} = 192.53.56.7 = 11000000.00110101.00111000.00000111$$

$$23 \text{ bit mask} = 255.255.254.0 = 11111111.11111111.11111110.00000000$$

$$\text{IP AND Mask} = 11000000.00110101.00111000.00000000$$

$$= 192.53.56.0$$

(G-1974) Fig. B



(G-151) Fig. P. 5.13.5 : The given configuration

Step 2 : Make the routing table : The routing table is as shown in Table P. 5.13.5.

Table P. 5.13.5 : 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 :

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.

Ex. 5.13.6 : Consider a class C network which needs to be subnetted into 3 subnets. Calculate the appropriate network mask. How many number of hosts can be supported by each subnet?

Dec. 12. 8 Marks

Soln. :**Given :** A class C network, 3 subnets.**To find :****Step 1 : Subnet mask :**

The default mask for a class C network is

$$255 \cdot 255 \cdot 255 \cdot 0$$

In order to have three subnets, we must have 2 extra 1s. Hence the default mask and subnet mask are as shown in Fig. P. 5.13.6.

Step 2 : Number of hosts per subnet :

- The two bits reserved for subnetting will have 4 combinations from 00 to 11, out of which any three combinations can be used for three subnets.
- We will use the combinations from 00 to 10 and will not use the combination 11.
- Thus each subnet will have six bits for host id. Therefore number of hosts per subnet will be $2^6 = 64$.

Ex. 5.13.7 : An ISP is granted a block of addresses starting with 120.60.4.0/22. The ISP wants to distribute these block to 100 (one hundred) organizations with each organization receiving just 8 (Eight) addresses. Design the sub-blocks and give the Slash Notations for each sub-block. Find out how many addresses are still available after these allocations.

Soln. :

Given that,

An ISP is granted a block of addresses starting with 120.60.4.0/22 among 100 organizations wherein each organization receives eight addresses.

Let us consider that the address are divided into 128 sub-blocks each having 8-addresses.



Number of granted addresses to the ISP

$$= 128 \times 8 = 1024$$

\Rightarrow Customer needs 8 addresses,

$\Rightarrow \log 2^8$ bits are needed to define each host.

$$\log 2^8 = \log 2^3$$

$$= 3 \log 2^2$$

$$= 3 \times 1$$

$$= 3$$

$$\text{Prefix length} = 32 - 3 = 29$$

The address starts from 120.60.4.0/29 instead of 120.60.4.0/22

Since, there are 8 addresses distributed among 100 organization therefore, total number of allocated address = $100 \times 8 = 800$.

Sub-block	Starting address	Ending address
1.	120.60.4.0/29	120.60.4.7/29
2.	120.60.4.8/29	120.60.4.15/29
3.	120.60.4.16/29	120.60.4.23/29
4.	120.60.4.24/29	120.60.4.31/29
5.	120.60.4.32/29	120.60.4.39/29
6.	120.60.4.40/29	120.60.4.47/29
:	:	:
10	120.60.4.72/29	120.60.4.79/29
:	:	:
32	120.60.4.248/29	120.60.4.255/29
:	:	:
64	120.60.5.248/29	120.60.5.255/29

Sub-block	Starting address	Ending address
:	:	:
98	120.60.7.8/29	120.60.7.15/29
99	120.60.7.16/29	120.60.7.23/29
100	120.60.7.24/29	120.60.7.31/29

$$\text{Numbers of granted address} = 1024$$

$$\text{Number of allocated address} = 800$$

Number of available address = Number of granted address - Number of allocated address.

$$= 1024 - 800 = 224$$

Ex. 5.13.8 : An organization is granted the block 211.17.180.0/24. The administrator wants to create 32 subnets.

- (a) Find the subnet mask.
- (b) Find the number of addresses in each subnets.
- (c) Find the first and last addresses in subnet 1.
- (d) Find the first and last addresses in subnet 32.

Soln. :

Step 1 : Subnet mask :

This is a class C network. So the default mask is given by,

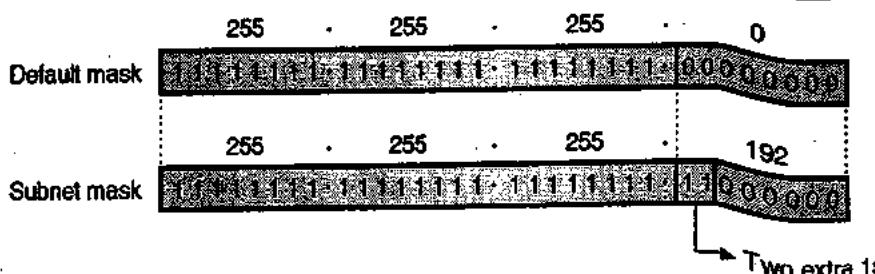
255.255.255.0

As we need 32 subnets we need 5 extra 1's. So the subnet mask will be as follows in the binary form.

Refer Fig. P. 5.13.8(a).

The subnet mask is therefore given by,

255.255.255.248



(G-1512) Fig. P. 5.13.6 : Subnet mask

Step 2 : Number of addresses in each subnet :

The structure of a class C address is as shown in Fig. P. 5.13.8(b).

As seen from Fig. P. 5.13.8(b), we have only 3 bits to decide the number of addresses in each subnet.

$$\therefore \text{No. of addresses per subnet} = 2^3 = 8$$

Step 3 : First and the last address in subnet 1 :

$$\text{First address in subnet-1} = 211.17.180.0$$

$$\text{Last address in subnet-1} = 211.17.180.7$$

Step 4 : First and the last address in subnet 31 :

$$\text{First address in subnet-32} = 211.17.180.248$$

$$\text{Last address in subnet-32} = 211.17.180.255$$

Ex. 5.13.9 : For the given IP address 205.16.37.39/28 in some block of addresses, calculate :

- (a) Address mask
- (b) First address of the block
- (c) Last address of the block
- (d) Number of address in the block

Soln. :

Given IP address is 205.16.37.39/28.

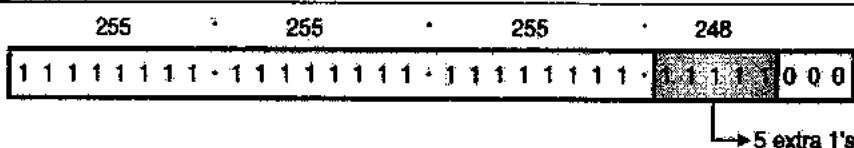
1. To find address mask :

Address mask is /28 which can be represented as

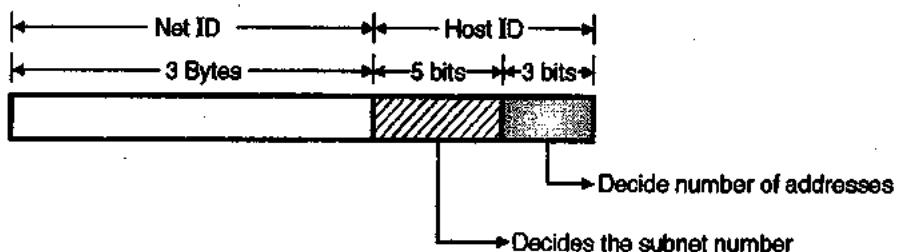
1111111.1111111.1111111.11110000

2. To find first address of block AND the given address with mask :

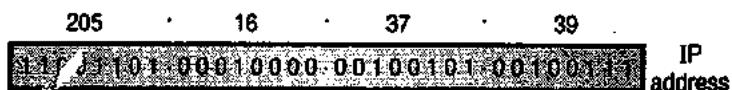
First address of block is 205.16.37.32.Ans.



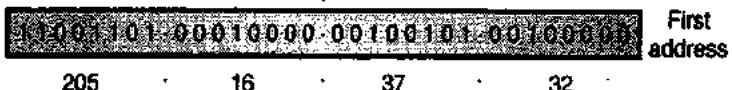
(G-1513) Fig. P. 5.13.8(a) : Subnet mask



(G-1514) Fig. P. 5.13.8(b)



↓
ANDing



(G-1515) Fig. P. 5.13.9



3. To find last address of the block OR the given address with mask :

205	.	16	37	39	
11000010	10000000	00000000	00100101	00100	IP address
00000000	00000000	00000000	00000000	111	Mask
00110100010000	00000000	00000000	00000000	111	Last address
205	.	16	37	47	

(G-1516) Fig. P. 5.13.9(a)

Last address of block is 205.16.37.47.Ans.

4. To find number of address in the block :

The value of n is 28, which means that number of address is,

$$2^{32-n} = 2^{32-28} = 2^4 = 16$$

Ex. 5.13.10 : Consider a class-C network which needs to be subnetted into 5 subnets. Calculate the appropriate network mask. How many number of hosts can be supported by each subnet ?

Dec. 13, 8 Marks

Soln. :

Given : Class-C network, 5 subnets

To find : 1. Network mask 2. Number of hosts per subnet

Step 1 : Subnet mask :

The default mask for a class-C network is,

255.255.255.0

In order to have 5 subnets, we have 3 extra 1's. Hence the default mask and subnet mask are as shown in Fig. P. 5.13.10.

Default mask	255	.	255	.	255	.	0	
	11111111	.	11111111	.	11111111	.	00000000	
Subnet mask	255	.	255	.	255	.	224	

→ 3 extra 1's

(G-1486) Fig. P. 5.13.10 : Subnet mask

Step 2 : Number of hosts per subnet :

- The three bits reserved for subnetting will have 8 combinations from 000 to 111, out of which any 5 combinations can be used for 5 subnets.
- Thus each subnet will have 5 bits for host id. Therefore number of hosts per subnet will be $2^5 = 32$.

Ex. 5.13.11 : Consider a class-C network which needs to be subnetted into 4 subnets. Calculate the appropriate network mask. How many number of hosts can be supported by each subnet ?

May 12, 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. 5.13.11.
- In order to have four subnets we can have the 4 combinations of the two extra 1s as shown in Table P. 5.13.11.

Table P. 5.13.11

Combination n	Subnet number
0 0	Subnet 1
0 1	Subnet 2
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.
- No. of hosts/subnet = $2^6 = 64$.

255	.	255	.	255	.	192	
1 1 1 1 1 1 1 1	.	1 1 1 1 1 1 1 1	.	1 1 1 1 1 1 1 1	.	1 1 0 0 0 0 0 0	

→ 2 Extra 1's

(G-1736) Fig. P. 5.13.11

5.14 MPLS (Multi-Protocol Label Switching) :

SPPU : Dec. 11, Dec. 12, May 13

University Questions

- Q.1 How link virtualization is achieved in MPLS ?**
(Dec. 11, 8 Marks)
- Q.2 Explain in brief working of MPLS. (Dec. 12, 6 Marks)**
- Q.3 Explain the working of MPLS with suitable diagram.**
(May 13, 10 Marks)

- When IETF was developing integrated and differentiated services, several router vendors were developing a new and better forwarding method called as **label switching** or **tag switching**. IETF eventually standardized this idea under the name **MPLS (Multi Protocol Label Switching)**.
- In this method, a label is added in front of each packet and the routing is done on the basis of this label and not on the basis of the destination address.
- This label acts as an index into an internal table. Due to this, it becomes very easy to find the correct output line by referring to the table.
- This idea thus makes the routing process very fast.
- The concept of label switching is very close to that of the virtual circuits (used in X.25, Frame relay and ATM). In the virtual circuits also, they put the labels called **Virtual Circuit Identifier (VCI)**, in each packet and routing is carried out on the basis of VCI.
- MPLS is described in RFC 3031 and many other RFCs.

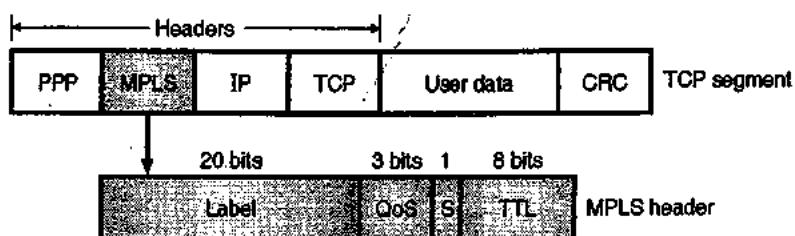
5.14.1 MPLS Header :

- The first step in MPLS will be to decide the place of the label in the IP packet. In the IP packet there is no place available for the label because it was not designed for virtual circuits.

- Therefore a new MPLS header is added in front of the IP header as shown in Fig. 5.14.1.
- The generic MPLS header has four fields :
 - Label
 - QoS
 - S-field
 - TTL
- The **Label** field is a 20 bit field which holds the index as shown in Fig. 5.14.1. The 3-bit QoS (Quality of Service) field indicates the class of service.
- The 1-bit **S-field** relates to stacking of multiple labels in the hierarchical networks. If it hits a 0, then the packet is discarded. This feature avoids the infinite looping in the event of router instability.
- MPLS is to a large extent independent of both data link layer as well as network layer because the MPLS header is not a part of either the network layer packets or data link layer frames.
- It is therefore possible to build the MPLS switches that can forward both IP packets and ATM packets. That is why MPLS is called as a "Multi Protocol" switching technique.

5.14.2 How does MPLS Work ?

- When an MPLS packet or cell arrives at an MPLS router, the label is used as an index into the look up table to find out the correct outgoing line and also the new label to be used.
- This new label contains the address of the next MPLS router. The labels have to be remapped at every hop, similar to that in the virtual circuits.
- The routers normally group multiple flows that end at a particular router or LAN and use a single label for them. The flows grouped under a single label belong to the same FEC (Forwarding Equivalence Class).
- The FEC covers the following aspects :
 - Where the packets are going.
 - Their service class



(G-69) Fig. 5.14.1 : A TCP segment using IP, MPLS and PPP headers



- All the packets under the same FEC are treated in the same way for forwarding purpose.
- With the virtual circuit switching it is not possible to group several distinct paths with different end points onto the same VCI. This is possible with MPLS because the packets contain the destination address as well as the label.

5.14.3 Forwarding Table :

- One main difference between MPLS and conventional VC (Virtual Circuit) is the way in which the forwarding table is constructed. In the VC networks, when a user wants to establish a new connection, it launches a set up packet into the network to create the path and make the entries into the forwarding table.
- The MPLS does not work this way as there is no set up phase for each connection.
- Instead there are two ways of creating the forwarding table entries. The two approaches are :
 1. Data driven approach
 2. Control driven approach.
- In the **data driven approach**, when a packet hits a router, that router will contact the next router where the packet will be going and asks it to generate a label for the flow.
- The protocols used in this approach use a technique called **coloured threads** to avoid loops.
- **Control driven approach**, is used on the networks that are not based on ATM. It has several variants. One of them is as follows :
 - When a router is booted, it checks the roots depending on the final destination. It then creates one or more FECs for them, allocates a label for each one and passes the labels to its neighbours. The neighbouring routers will enter the labels in their forwarding tables and send new labels to their neighbours. This will continue till all the routers have received the information about the path.
 - MPLS can operate at multiple levels simultaneously. The S-bit in Fig. 5.14.1 allows a router to remove a label to know if there are any additional labels left.
 - The S-bit is set to 1 for the bottom label and 0 for all other labels.

5.15 Routing in MANET :

- Routing is an activity which connects calls from source to destination in telecommunication networks which plays an important role in construction, design and operation of the network.
- Ad-hoc networks are wireless networks where multi-hop links are used for communication of nodes with each other.
- Routing is challenging task in MANET because there is constant change in topology of network due to mobility of nodes.
- To accomplish this task various protocols have been developed.

5.15.1 Problems with Routing in Mobile Ad-hoc Networks (MANET) :

1. Asymmetric links :

In ad-hoc networks, nodes are mobile and keeps changing their position in the network. e.g. in MANET, where node A send a signal to node B but this does not tell about quality of connection in the reverse direction.

2. Routing overhead :

Due to change of location of node in the network, unwanted routes may be generated which leads routing overhead.

3. Interference :

Main problem with MANET is interference. As links enter and exit depending on characteristics of transmission, one transmission may interfere other and node may overhear other transmission which can disturb the total transmission.

4. Dynamic topology :

Since the topology of network is not constant, the mobile node may change location or medium characteristics may change.

5.15.2 Characteristics of the Routing Protocol for MANET :

To overcome the problems with routing in MANET, routing protocols should have following characteristics :

1. It should be fully distributed.
2. It should be adjustable to frequent change in topology caused by the nodes mobility.
3. It must be localized.
4. It must be free from stagnant routes.
5. The convergence of routes must be quick.
6. Each node in the network should have to store information regarding local topology which is stable.
7. It should able to give good quality of service.



5.15.3 Classification of Routing Protocols in MANETs :

- Classification of routing protocols in MANET is as shown in Fig. 5.15.1.
- Classification of routing protocols in MANET's depends on routing strategy and network architecture.
- Table driven and source initiated routing protocols are categorized based on routing strategy.
- While flat, hierarchical and geographic position assisted routing are based on structure of the network.
- Table driven (proactive) and on-demand (reactive) protocols are flat routing protocols.

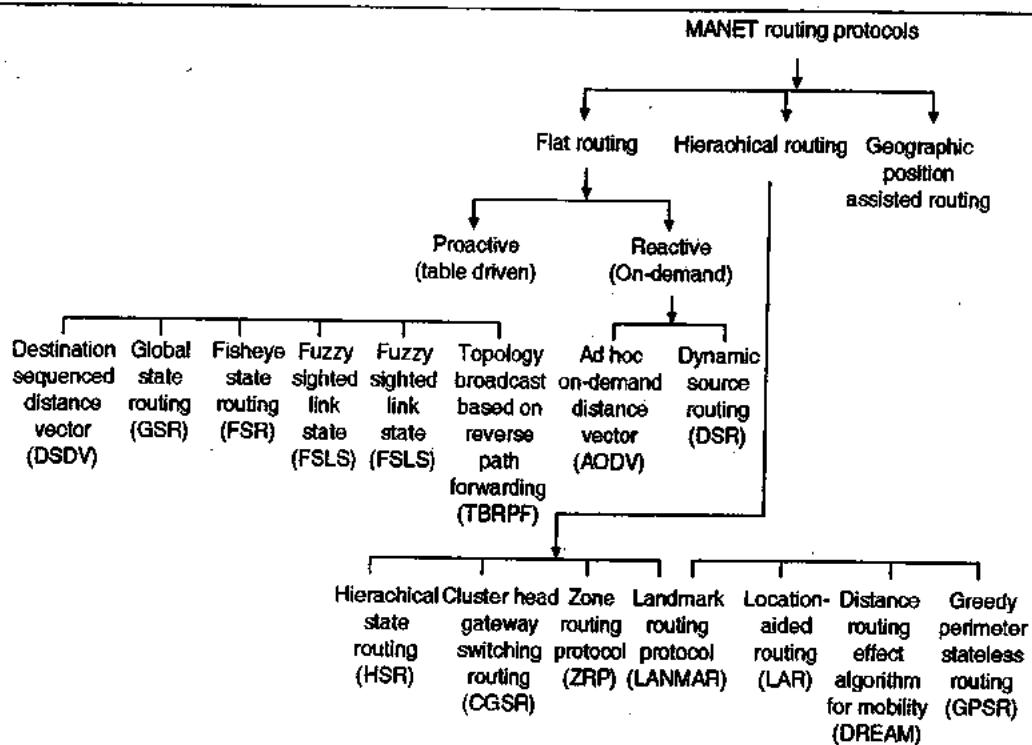
5.16 Table Driven Routing Protocols (Proactive) :

- These protocols are also known as proactive because they maintain the routing information before it is required.
- They maintains topology information at each and every node in the form of tales. To maintain consistent and accurate network state information these tables are frequently updated.
- Examples of table driven routing protocols are DSDV, GSR, FSR, FSLS etc.
- The proactive protocols are not suitable for large networks because they need to maintain table for each and every node.

- In the following subsection we will discuss proactive routing protocol : DSDV (Destination Sequenced Distance Vector Routing Protocol).

5.16.1 Destination Sequenced Distance Vector Routing Protocol (DSDV) :

- DSDV is table routing protocol which is first protocol for ad-hoc wireless networks. DSDV is improved version of Bellman Ford algorithm where each node keeps a table which contain shortest distance and the first node to every other node in the network on the shortest path.
- To prevent loops, to answer the count to infinity problem and faster convergence node includes table updates with increasing sequence number tags.
- As DSDV is table driven routing protocol at all times, routes to all destinations are readily available at every node.
- To maintain an upto date record of the network topology, the tables are exchanged between neighbours at interval.
- If node finds major change in local topology, then tables are forwarded.
- There are two types of table updates :
 1. Incremental updates.
 2. Full dumps.
- Incremental updates :**
 - An incremental update takes single Network Data Packet Unit (NDPU).
 - When there is no significant change observed in topology, incremental updates are used.

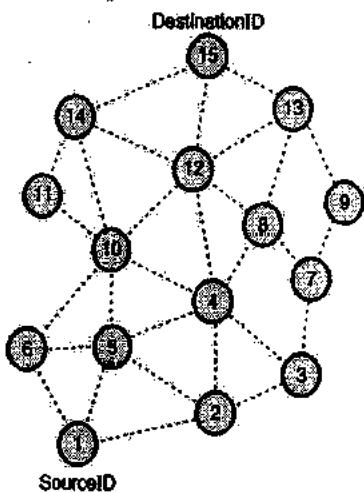


(G-1687) Fig. 5.15.1 : Classification of MANET routing protocols



2. Full dumps :

- Full dump takes multiple NDPU.
- A full dump is performed either when the local topology changes significantly or when an incremental update needs more than single NDPU.
- Destination node initiate table update with new sequence number.
- Initiated sequence number is always greater than previous one.
- Once updated table is obtained, a node either updates its tables with the help of received data or hold it for some time to choose the best metric. (It is the smallest number of hops) received from many kinds of the same update table from various neighbouring nodes.
- A node may forward or decline the table based on the sequence number of the table update.



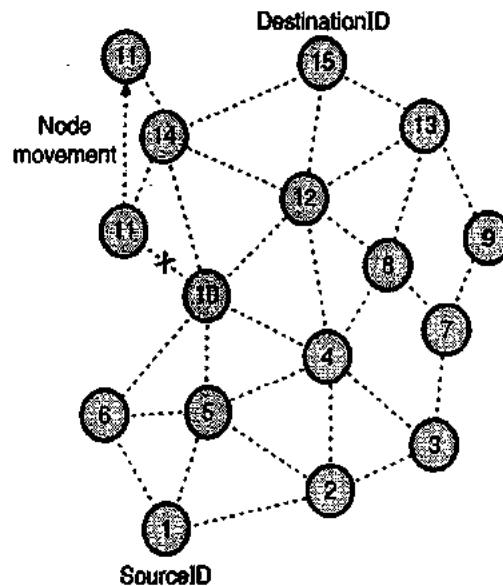
(a) Topology graph of the Network

Dest	NextNod	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	162
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15			250

(b) Routing table for Node 1

(G-169) Fig. 5.16.1 : Route Establishment in DSDV

- Fig. 5.16.1 shows route establishment in DSDV.
- For example as shown in Fig. 5.16.1(a), node 1 is assumed as source node and node 15 is the destination node.
- The route already exists as shown in Fig. 5.16.1(b) because the nodes preserve universal topology data.
- The routing table of source node 1 shows that smallest route to the destination node 15 exist through node 5 and minimum distance of it is 4 hops.
- The reconfiguration of path used by on-going data transfer is handled by the protocol in the following way.
- The last node of broken link begin a table update message with the weight of broken link assigned to ∞ and with a sequence number larger than the registered sequence number for that destination node.
- Once, a node get an update table with weight as ' ∞ ', immediately each node circulate it to its adjacent nodes to broadcast the broken link data to the entire network.
- Hence, breaking of single link leads to the circulation of table update data to the whole network.
- A node all the time allocates an odd sequence number to the link break record to distinguish it from the even sequence number generated by the destination node.



(a)

Fig. 5.16.2 (Contd..)

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	162
9	2	4	186
10	6	2	142
11	4	4	186
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b)

(G-169) Fig. 5.16.2 : Route Maintenance in DSDV

- Consider the case when node 11 moves from its current location, as shown in Fig. 5.16.2(a).
- When an adjacent node observe the link break, it establishes all the paths passing through the broken link with distance as ' ∞ '.
- For example, when node 10 is aware of the link failure, it sets the path to node 11 as ∞ and transmits its routing table to its neighbouring nodes.
- Those neighbouring nodes finding important changes in their routing tables retransmit it to their neighbours.
- In this way, broken link information spreads all over the network.
- Node 1 also establish the distance to node 11 as ' ∞ '.
- When node 14 gets a table update message from node 11, it informs the neighbours about shortest distance to node 11. This information is also circulated throughout the network.
- After receiving new update message with higher sequence number, all nodes saves the new distance to node 11 in their corresponding tables.
- Fig. 5.16.2(b) shows updated table at node 1, where the current distance from node 1 to node 11 is increased from 3 to 4 hops.

Advantages :

- The availability of paths to all destinations in network always shows that less delay is required in the path set up process.

- DSDV protocol guarantees loop free path.
- The method of incremental updates with sequence number labels, makes the existing wired network protocols adaptable to ad hoc wireless networks.
- Therefore, with few modification wired network protocol can be applied to ad-hoc wireless networks.
- Count to infinity problem is reduced in DSDV.
- We can avoid extra traffic with incremental updates instead of full dump updates.
- DSDV maintains only the best path instead of maintaining multiple paths to every destination. Due to this, amount of space is reduced in routing table.

Disadvantages :

- The updates because of broken links lead to a heavy control overhead during high mobility.
- DSDV doesn't support multipath routing.
- The small network with high mobility or big network with less mobility can totally block the existing bandwidth.
- Thus, this DSDV protocol suffers from too much control overhead which is proportional to the number of nodes in the network, this is not scalable in ad hoc network which has restricted bandwidth and network topologies are highly dynamic.
- To obtain information about a specific destination node, a node has to wait for table update message sent by same destination node. This wait could results in old routing information at nodes.
- For larger network it is difficult to maintain routing table.

5.17 On-demand Routing Protocol (Reactive) :

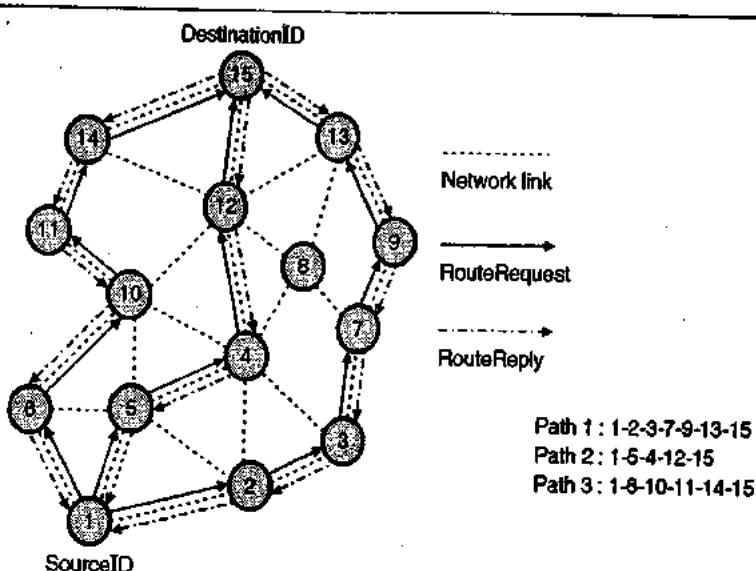
- On demand routing protocol is also called as reactive protocols.
- On demand routing protocol perform path finding procedure and exchange of routing information takes place only when path required by a node to make communication with a destination.
- If there is no communication between nodes they don't maintain routing information or activity hence these protocols are called as reactive protocols.
- If one node want to send packet to other node this protocol finds the route in on-demand manner and it creates connection in order to transmit and receive the packet.
- In the following subsection we will discuss on-demand routing protocols : AODV and DSR.



5.17.1 Dynamic Source Routing Protocol (DSR) :

- Dynamic Source Routing Protocol (DSR) is based on demand routing.
- DSR is designed to control the bandwidth spent by control packets in ad-hoc networks by removing the periodic table update messages needed in the table driven method.
- As DSR protocol is beacon-less and hence do not need periodic hello packet transmissions.
- This periodic beacon packet is used by a node to inform its presence to adjacent node.
- During route construction phase, DSR establish a route by flooding RouteRequest packets in the network.
- After receiving RouteRequest packet, destination node respond by sending a RouteReply packet back to the source node.
- This source node keeps the route traversed by the RouteRequest packet received.
- Let a source node do not have route to the destination. It initiates RouteRequest packet when source node have data packet to be sent to destination.
- This RouteRequest packet is flooded into the entire network.
- Every node after receiving RouteRequest packet retransmits the RouteRequest packet to its adjacent node if it is not sent already or if the node itself is not destination node, within Time to Live (TTL) of RouteRequest packet.

- Every RouteRequest packet contains sequence number produced by the source node and traversed path of it.
- Before forwarding RouteRequest packet node checks the sequence number on packet.
- The packet is forwarded only if it is not duplicate RouteRequest packet.
- The sequence number on the packet is useful to avoid loop formations and to prevent more transmission of the similar RouteRequest packet by intermediate node which receives RouteRequest packet through many routes.
- Hence, during the route construction phase all nodes except destination node forwards a RouteRequest packet.
- Upon receiving first RouteRequest packet, a destination node responds to the source node through the reverse path traversed by RouteRequest packet.
- Fig. 5.17.1 shows route establishment in DSR.
- As shown in Fig. 5.17.1, to obtain a path for destination node 15, source node 1 initiates RouteRequest packet.
- DSR protocol uses a route cache which stores all possible data obtained from the source route obtained in data packet.
- Nodes can also study about the adjacent routes came across by data packets if nodes are operated in the promiscuous mode. (The mode in which node can receive the packet which are neither transmits nor addressed to itself).
- This route cache is also useful during the route construction phase.



(G-1692) Fig. 5.17.1 : Route Establishment in DSR

- If **RouteRequest** packet is received by intermediate node, it has route to the destination node in its route cache then it respond to the source node by sending **RouteReply** with all route data from source to destination node.

Optimizations :

- In order to improve the performance of DSR protocol, many optimization techniques have been proposed. DSR protocol uses route cache at intermediate nodes.
- The route cache is settled with routes which can be removed from the information held in data packets which get forwarded.
- To reply to the source node when they receive a **RouteRequest** packet, intermediate nodes uses this cache information.
- It also uses cache information if they find a route to the respective destination.
- An intermediate node discover about breaks in route when it operates in the promiscuous mode.
- Thus obtained information is useful to update the route cache so that the active routes kept in the route cache do not use such broken links.
- The affected node initiates **RouteRequest** packet at the time of partition of network.
- An exponential back off algorithm is used to prevent **RouteRequest** flooding in the network when the destination node is in another disjoint set.
- Piggy-backing of a data packet on the **RouteRequest** packet is used in DSR so that a data packet can be transmitted along with **RouteRequest** packet.
- Route construction phase becomes simple without optimization.
- If intermediate nodes are not redundant, they flood **RouteRequest** packet.

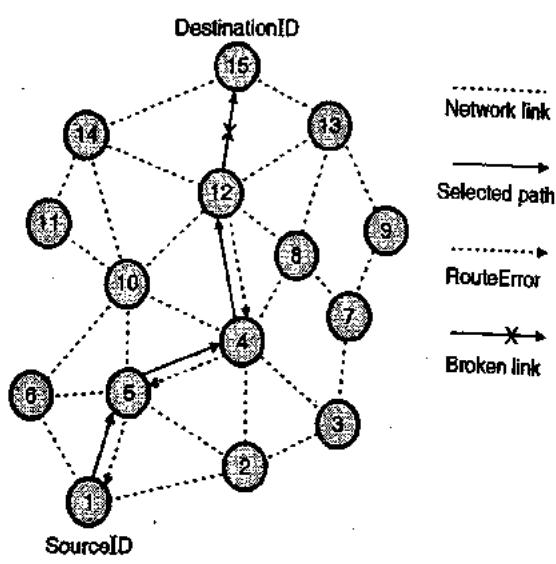
- For example as shown in Fig. 5.17.2 after getting the **RouteRequest** packet from node 1 all its adjacent nodes such as node 2, node 5 and node 6 forward **RouteRequest** packet.
- Node 4 gets **RouteRequest** packet from node 2 and node 5.
- Node 4 sends the first **RouteRequest** packet it gets from either node 2 or node 5 and rejects the other duplication or redundant **RouteRequest** packet.
- The **RouteRequest** is circulated until it reaches at the destination node which is in the **RouteReply**.
- Source node may receive multiple replies if intermediate nodes are allowed to begin **RouteReply** packets.
- Suppose in Fig. 5.17.2 if the node 10 has a path to the destination node through node 14 it also send the **RouteReply** to the source node.
- The source node chooses the recent and best route and selects that route for transmitting data packets. Each data packet contains the entire path to its destination node.
- When intermediate node is out of path causing link break (e.g. link between node 12 and 15), **RouteError** message is produced from the adjacent node of failed link to inform the source node.
- The source node number restarts the route establishment process.
- When **RouteError** message is received at source node, then all the cached entries at intermediate node and source node are eliminated.
- If a wireless link fails due to movement of node edges for example, node 1 and node 15, the source node again starts the discovery process of route.

Advantages :

- DSR protocol eliminates the need of flood in the network with routing table update messages which are needed in a table driven method.
- In on demand protocol, a path is established only when it is needed and hence they need to find paths to all other nodes in the network.
- To minimize the control overhead route cache information is utilized efficiently by intermediate nodes.

Disadvantages :

- Route maintenance method is not able to repair broken link locally.
- During the route reconstruction phase, route cache information may cause inconsistency.



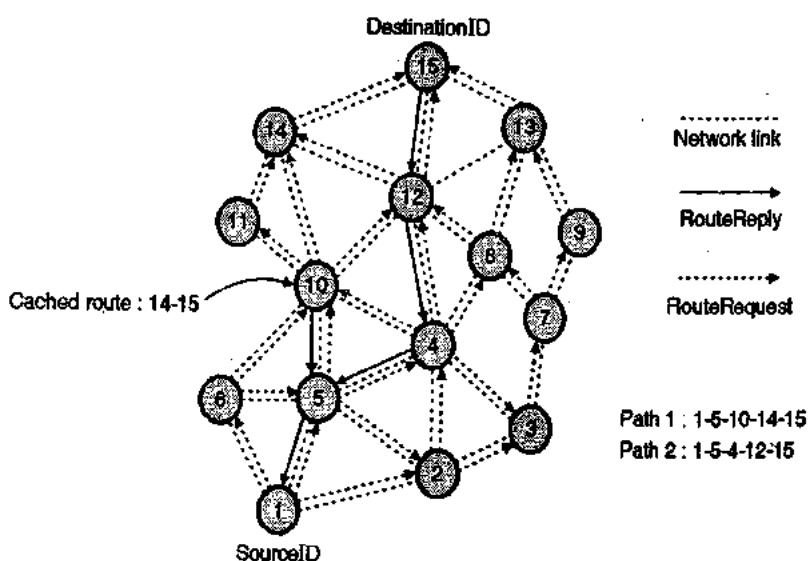


3. The delay is higher in order to establish the connection as compared to table driven protocols.
4. Though DSR protocol works well in static and low mobility environments the performance goes down with increasing mobility the performance goes down rapidly even though DSR works good in static and low mobility environment.
5. As the routing overhead is involved due to source routing method in DSR. This routing overhead is directly proportional to the length of path.

5.17.2 Ad-hoc on Demand Distance Vector Routing Protocol (AODV) :

- AODV routing protocol uses on demand method for discovering routes. i.e. route is created only when it is needed by source node for sending data packets.
- AODV protocol makes use of destination sequence number to identify the latest path.
- The main difference between AODV and Dynamic Source Routing (DSR) protocol comes out from the fact that DSR uses source routing in which a data packet contains the complete path to be traversed.
- In AODV protocol, the source nodes and intermediate nodes keep the next hop information related to each flow for data packet transmission.
- In on demand routing protocol the source node floods the RouteRequest packet in the network when there is no route available for the desired destination.
- From a single RouteRequest, it can obtain many routes of different destination.
- To obtain up-to-date path to the destination AODV protocol uses destination sequence number (DestSeqNum).

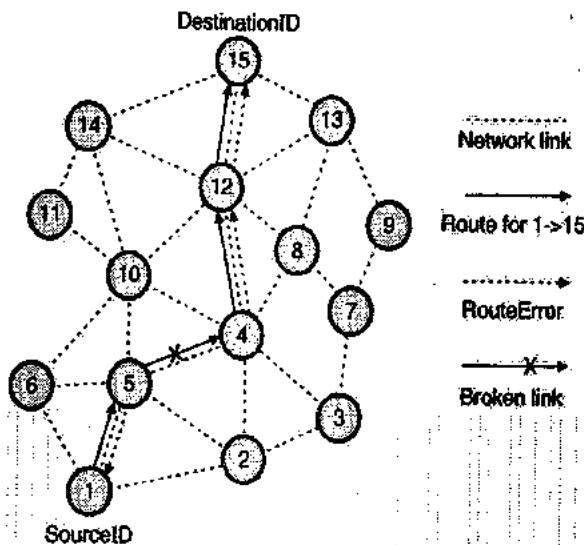
- When the DestSeqNum of current packet is greater than the previous DestSeqNum stored at node, then a node updates its path information.
- A **RouteRequest** packet contains destination identifier (DestID), source identifier (SICID), source sequence number (SrcSeqNum) and destination sequence number (DestSeqNum), broadcast identifier (BcastID) and time to live (TTL) field. DestSeqNum shows that the route is accepted by source.
- When an intermediate node gets a **RouteRequest** packet, it either sends it or makes a **RouteReply** if it has valid routes to the destination.
- The validity of a route at the middle node is decided by comparing sequence number at middle node with the DestSeqNum in the **RouteRequest** packet.
- If a **RouteRequest** is received by many times which is indicated by the broadcast identifier and source identifier, duplicate **RouteRequest** packets are rejected.
- All intermediate nodes having valid routes to the destination or destination node itself can allow to send **RouteRequest** packets to the source node.
- At the time of sending a **RouteRequest** packet, every intermediate node does entry of previous node address and its broadcast identifier (BcastID).
- If **RouteReply** is not received before time expires, a timer is used to this entry.
- As AODV does not employ source routing of data packet, this helps in storing an active path at the intermediate node.



(G-168) Fig. 5.17.3 : Route establishment in AODV

- When a node receives a **RouteReply** packet, data about the previous node from which the packet was obtained is also stored in order to forward the data packet to next node.
- Route establishment in AODV is as shown in Fig. 5.17.3.
- As shown in Fig. 5.17.3 source node starts a path discovery process by initiating **RouteRequest** to the destination node 15 in the network. It assumes the **RouteRequest** which includes destination sequence number as 3 and source sequence number as 1.
- When nodes 2, 5 and 6 gets **RouteRequest** packet, these nodes verify their routes to the destination.
- In case the routes to node 15 do not exist, they send next **RouteRequest** packet to their neighbouring node.
- As shown in Fig. 5.17.3 node 3, node 4 and node 10 are the neighbours of node 2, node 5 and node 6 respectively.
- It is assumed that node 3 and node 10 have already existing routes to destination node 15. The route exists as 10-14-15 and 3-7-9-13-15 respectively.
- If the DestSeqNum at node 10 is 4 and at node 3 is 1, then only node 10 is permitted to reply along the cached route to the source node 1. This is because intermediate node 3 has an oldest route to destination node 15 as compared to the route available at the source node 1.
- The DestSeqNum at node 3 is 1, whereas source node 1 has DestSeqNum 3.
- At the same time node 10 has recent route with DestSeqNum 4 to destination.
- If the **RouteRequest** reaches at destination node 15 through available path 4-12-15 or any other alternative route the destination node 15 also send a **RouteReply** to the source node 1.
- In such case multiple **RouteReply** packets reach the source node.
- All intermediate nodes getting **RouteReply** packet update their route tables with the recent DestSeqNum.
- They also update the routing information if it leads to smaller path between source and destination node.
- AODV do not repair a damaged path locally.
- When a wireless link breaks which is determined by monitoring beacons which are periodical or notification of link level acknowledgements at the destination node.

- Source node restart the route to the destination node by using higher layers when it discovers path break.
- If path break is found at intermediate node, the intermediate node update the source and destination nodes by sending unsolicited **RouteReply** with the value of hop count as ‘∞’.



(G-1689) Fig. 5.17.4 : Route maintenance in AODV

- As shown in Fig. 5.17.4 for example, the path between nodes 4 and 5, both the nodes start **RouteError** message to update their end nodes about the link break.
- The end node remove the related entries from their tables.
- The source restarts the path finding process with new broadcast identifier and previous DestSeqNum.

Advantages :

- In AODV protocol paths are established on demand and DestSeqNum are used to discover the recent route to destination.
- The connection establishment delay is small.
- As AODV is reactive in nature, it can handle highly dynamic behaviour of Ad-hoc networks.

Disadvantage :

- Disadvantages of AODV protocol is that intermediate nodes can lead to conflicting routes if the source sequence number is not recent and intermediate nodes have greater but not the recent DestSeqNum, it results in having hard entries in table.
- No reuse of routing information.
- AODV does not discover a route until a flow is initiated.

**Review Questions**

- Q. 1 Name different protocols in the network layer.
- Q. 2 Explain the purpose of ARP.
- Q. 3 Why is ARP request broadcast but ARP reply unicast ?
- Q. 4 Write a note on IP.
- Q. 5 Explain fragmentation in IP.
- Q. 6 What is the name of a packet in IP ?
- Q. 7 Explain the IP header.
- Q. 8 What is MTU and how is fragmentation related to it ?
- Q. 9 Compare IPv4 and IPv6.
- Q. 10 State limitations of IPv4.
- Q. 11 Write a note on ICMP.
- Q. 12 Name and describe three types of IPv6 addresses.
- Q. 13 What is unicast routing ?
- Q. 14 Write a note on RIP.
- Q. 15 What is multicast routing ?
- Q. 16 Explain IGMP.
- Q. 17 Write a note on mobile IP.
- Q. 18 What is fragmentation ? Explain how is it supported in IPv4 and IPv6.
- Q. 19 Explain the addressing scheme in IPv4 and IPv6. When IPv6 protocol is introduced, does the ARP protocol have to be changed ? Explain.
- Q. 20 What is fragmentation ? Explain how it is supported in IPv4 and IPv6.
- Q. 21 Given an IP address, how will you extract its net id and host id.
- Q. 22 What is PING utility ? How many ways are there to implement PING ? Explain steps.
- Q. 23 What is subnetting in IP network, explain with suitable examples.
- Q. 24 Why is an ARP Query sent within a broadcast frame ? Why is an ARP response sent within a frame with a specific destination LAN address ?
- Q. 25 A network on the internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts it can handle ?

Q. 26 An IP datagram using the strict source routing option has to be fragmented. Do you think the option is copied into each fragment, or is it sufficient to just put it in the first fragment ? Explain your answer.

5.18 University Questions and Answers :

- Q. 1 Describe in short the importance and working of following commands : **(May 2015, 8 Marks)**
1. Ping
 2. Netstat
 3. Traceroute
 4. IP config.

Ans. :

1. The Traceroute Command :

The traceroute command is used to discover the routes that packets actually take when travelling to their destination. The device (for example, a router or a PC) sends out a sequence of User Datagram protocol (UDP) datagrams to an invalid port address at the remote host.

Three datagrams are sent, each with a Time-To-Live (TTL) field value set to one. The TTL value of 1 causes the datagram to "timeout" as soon as it hits the first router in the path ; this router then responds with an ICMP Time Exceeded Message (TEM) indicating that the datagram has expired.

Another three UDP messages are now sent, each with the TTL value set to 2, which causes the second router to return ICMP TEMs. This process continues until the packets actually reach the other destination. Since these datagrams are trying to access an invalid port at the destination host, ICMP port Unreachable Messages are returned, indicating an unreachable port ; this event signals the Traceroute program that it is finished.

The purpose behind this is to record the source of each ICMP Time Exceeded Message to provide a trace of the path the packet took to reach the destination.

2. The Ping Command :

The ping command is a very common method for troubleshooting the accessibility of devices. It uses a series of Internet Control Message Protocol (ICMP) Echo messages to determine :

- Whether a remote host is active or inactive.
- The round-trip delay in communicating with the host.
- Packet loss.

The ping command first sends an echo request packet to an address, then waits for a reply. The ping is successful only if :

The echo request gets to the destination, and

The destination is able to get an echo reply back to the source within a predetermined time called a timeout. The default value of this timeout is two seconds on Cisco routers.

**3. The Netstat Command :**

Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is available on Unix, Unix-like, and Windows NT-based operating systems.

It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.

4. The Ipconfig Command :

Ipconfig (sometimes written as IPCONFIG) is a command line tool used to control the network connections on Windows NT/2000/XP machines. There are three main commands : "all", "release" and "renew". Ipconfig displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays the IP address, subnet mask and default gateway for all adapters.

This utility allows you to get the IP address information of a window computer. It also allows some control over active TCP/IP connections.

Q. 2 What is IP ? Discuss the different classes of IP addressing. Explain classful and classless routing.

Ans. :

For IP and different classes of IP addressing refer sections 5.3 and 5.3.4.

1. Classful routing :

Routing protocols that do not send subnet mask information when a route update is sent out. All the devices in the network have to use the same subnet mask. E.g. RIPv1.

2. Classless routing :

Routing that sends subnet mask information in the routing updates. E.g. RIPv2, OSPF.

Q. 3 What is fragmentation in IPv4 ? Explain with example. An IPv4 datagram arrives with fragmentation offset of 0 and an Mbit (More fragment bit) of 0. Is this a first fragment, middle fragment or last fragment ? (May 2016, 4 Marks)

Ans. :

Refer section 4.15 for fragmentation and 5.3.2 for structure of IP frame header.

Offset = 0 and M = 0 shows that it is the last or the only fragment.

Q. 4 Describe following commands with syntax :

1. Ping
2. Traceroute
3. Telnet

(May 2016, 6 Marks)

Ans. :

Refer Q. 1 from section 5.18 for ping and traceroute.

Telnet :

The telnet commands allow you to communicate with a remote computer that is using the Telnet protocol. You can run telnet without parameters in order to enter the telnet context, indicated by the Telnet prompt (`telnet>`). From the Telnet prompt, use the following commands to manage a computer running Telnet Client.

The tlntradmin commands allow you to remotely manage a computer running Telnet Server. These commands are run from the command prompt. Used without parameters, `tlntradmin` displays local server settings.

CHAPTER

6

Unit V

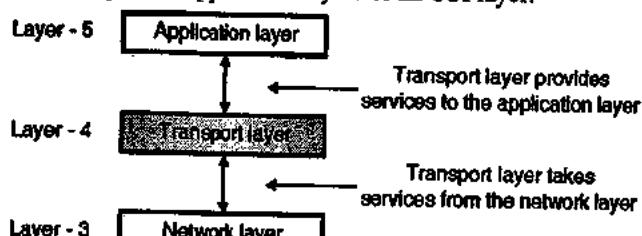
Transport Layer

Syllabus :

Services, Berkley Sockets, Addressing, Connection establishment, Connection release, Flow control and buffering, Multiplexing, TCP, TCP Timer management, TCP Congestion Control, Real Time Transport protocol (RTP), Stream Control Transmission Protocol (SCTP), Quality of Service (QoS), Differentiated services, TCP and UDP for Wireless.

6.1 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. 6.1.1 shows the position of the transport layer in the 5-layer internet model. The transport layer is fourth layer in this model. It connects the lower three layers to upper three layers of an OSI layer.



(G-59) Fig. 6.1.1 : Position of transport layer

6.2 Transport Layer Duties and Functionalities :

SPPU : May 10, May 11, Dec. 11

University Questions

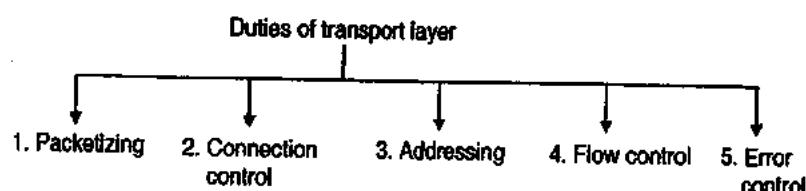
- G. 1** Explain in detail about the functions of transport layer including connection establishment and release procedure. (May 10, 8 Marks)

- Q. 2** What is the task of transport layer ? Explain the services provided to the upper layers by the transport layer. (May 11, 8 Marks)
- Q. 3** What is QoS ? Explain various parameters for QoS in a network. (Dec. 11, 5 Marks)

- Transport layer is meant for the process to process delivery and it is achieved by performing a number of functions.
- Fig. 6.2.1 lists the functions of a 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.



(G-1407) Fig. 6.2.1 : Duties of transport layer

- 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 :
 - Connection oriented.
 - 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.

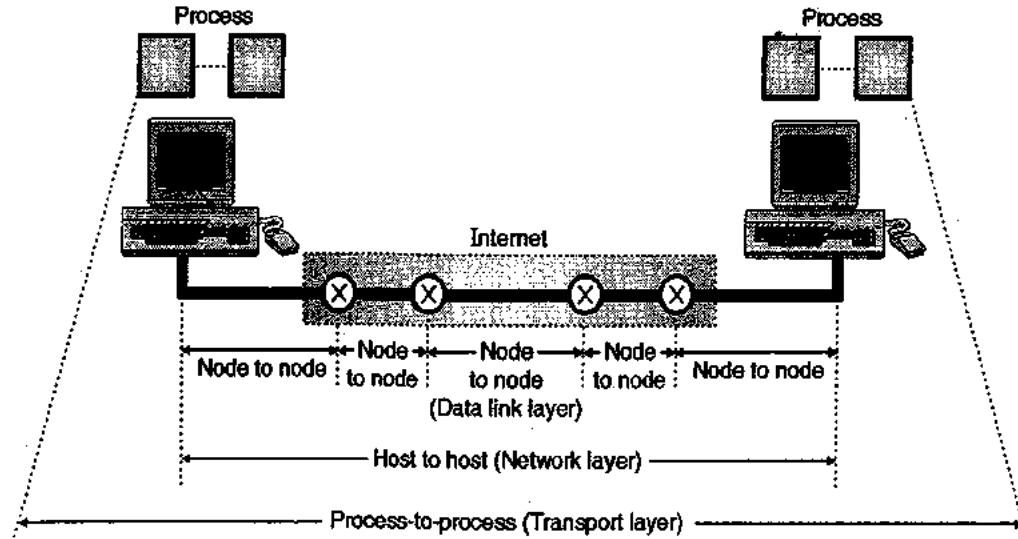
Congestion control and QoS :

- 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.

6.2.1 Process-to-Process Delivery :

- 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. 6.2.2 demonstrates the three processes.



(G-594) Fig. 6.2.2 : Types of data deliveries



6.2.2 Client Server Paradigm :

- 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

6.2.3 Addressing in Transport Layer :

SPPU : May 13

University Questions

Q. 1 Comment on types of ports ? What is the range of port numbers used in each type? (May 13, 6 Marks)

- The addressing requirements at different layer are different.
- 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.

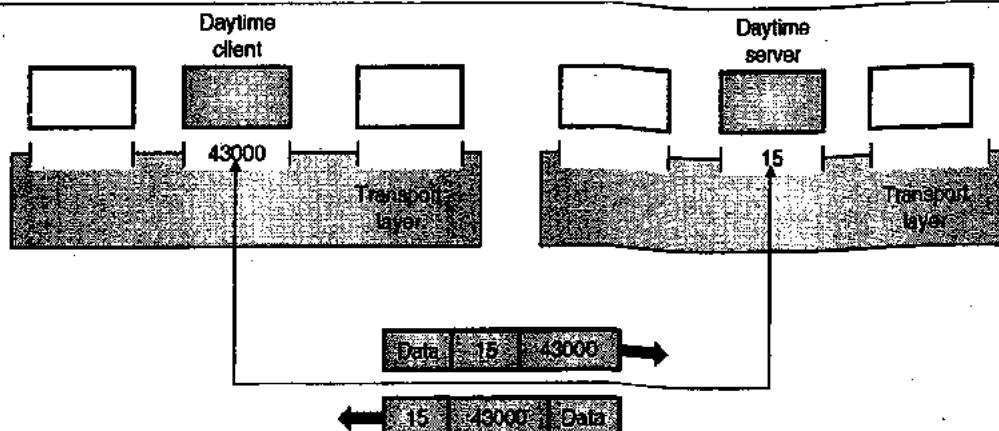
- The client program identifies itself with a port number which is chosen randomly. This number is called as **ephemeral port number**.
- The server process should also identify itself with a port number but this port number cannot be chosen randomly.
- The Internet uses universal port numbers for servers 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. 6.2.3.

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 :
 - Well known ports.
 - Registered ports.
 - Dynamic or private ports.



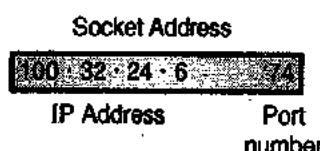
(G-59) Fig. 6.2.3 : Concept of port numbers



- Well known ports :** The ports from 0 to 1023 are known as well known ports. They are assigned as well as controlled by IANA.
- 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.
- 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. 6.2.4 and it is known as the socket address.
- The client socket address defines the client process uniquely whereas the server socket address defines the server process uniquely.



(G-1548) Fig. 6.2.4 : Socket address

- 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.

6.2.4 Multiplexing and Demultiplexing :

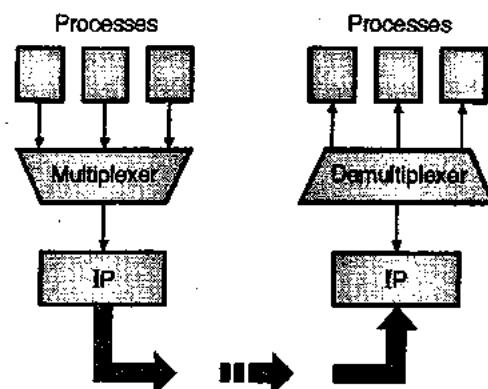
SPPU / May 12, Dec. 12, Dec. 13

University Questions

- Q.1 Explain multiplexing and de-multiplexing in transport layer.

(May 12, Dec. 12, Dec. 13, 6 Marks)

- The addressing mechanism allows multiplexing and demultiplexing taking place at the transport layer as shown in Fig. 6.2.5.



(G-597) Fig. 6.2.5 : 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. 6.2.5.

Demultiplexing :

- At the receiving end, the relationship is one 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.

6.2.5 Connection Oriented Versus Connectionless Service :

SPPU : Dec. 11

University Questions

- Q.1 Explain connection oriented and connection less service. Which protocols at each layer in TCP/IP protocol stack supports these services ?

(Dec. 11, 8 Marks)

A transport layer protocol can be either connectionless or connection oriented.

1. Connection Oriented Service :

- The connection oriented services, as the name suggests establishes a dedicated connection between the users before data is exchanged.
- The establishment of connection may take place on the physical level or logical level and needs some kind of signalling.



- This type of connection establishment needs some form of resource reservation (such as bandwidth).
- After the connection establishment, the actual data transfer will take place. After the exchange of data, the connection is cleared or broken.
- The best known example of a connection oriented service is the telephone network.
- The TCP is a connection oriented transport layer protocol.

2. Connectionless Service :

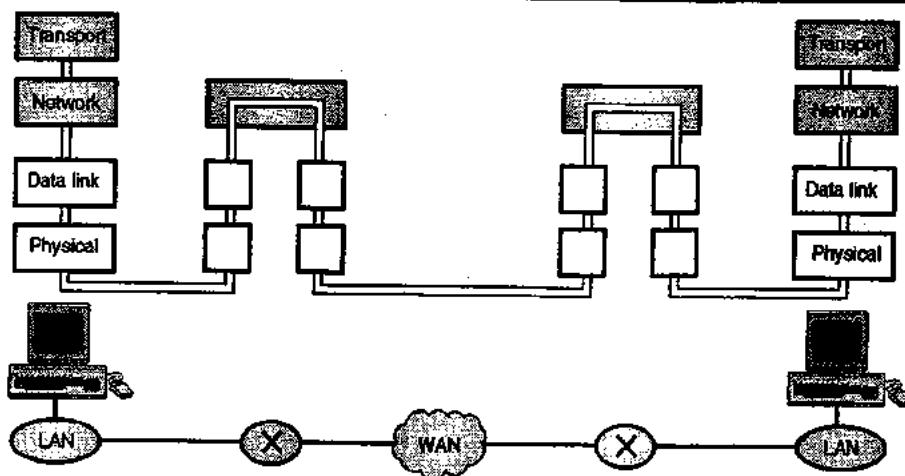
- This type of service does not require a connection to be established in order to exchange data.
- Instead, information is transferred by using **independent data units**. Each data unit contains the complete destination address. This is analogous to the postal mailing service.
- This connectionless service can exchange data without setting an explicit communication path or connection.
- The packets are not numbered. They can get delayed, lost or can arrive out of sequence. There is no acknowledgement, UDP is a connectionless protocol.

6.2.6 Reliability at Transport Layer Versus Reliability at DLL :

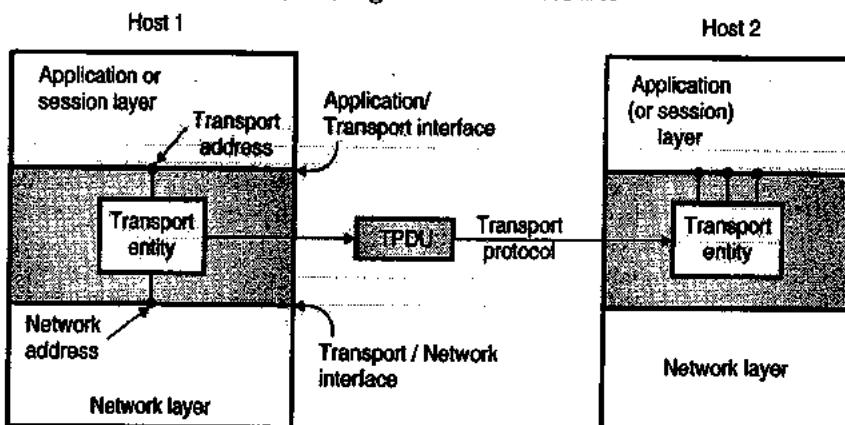
- The transport layer services can be of two types :
 1. Reliable services
 2. Unreliable services.
- If the application layer program needs reliability then the reliable transport layer protocol is used which implements the flow and error control at the transport layer. But this service will be slow and more complex.
- 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.
- 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.

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



(G-598) Fig. 6.2.6 : Error control



(G-599) Fig. 6.3.1 : Relation between network, transport and application layers

Note that the error is checked only upto the data link layer by the data link error control system.

6.3 The Transport Layer Services :

SPPU : May 11

University Questions

Q. 1 What is the task of transport layer ? Explain the services provided to the upper layers by the transport layer. (May 11, 8 Marks)

- The task of transport layer is to provide reliable, cost effective transport of data from source machine to destination machine.
- To achieve this goal the transport layer makes use of the services provided by the network layer.

Transport entity :

- The hardware and/or software within the transport layer which does the work of making use of the services provided by the network layer is called as transport entity.
- The relationship (logical) between the network, transport and application layers is shown in Fig. 6.3.1.

- The transport services are of two types :
 - Connection oriented
 - Connectionless
- In the connection oriented transport service, there are three phases namely : establishment, data transfer and release.
- Addressing and flow control in transport layer is similar to that in the network layer.
- The connectionless transport service also is very similar to connectionless network layer service.
- Eventhough the network and transport layers provide the similar services, the transport layer can improve the quality of service which a network layer cannot do.
- If a transport entity is told that its network connection is abruptly terminated, then it can set up a new network connection to the remote transport entity.
- Through this new connection, it can ask about which data has already arrived and which is yet to arrive.
- In other words the transport layer makes the transport service more reliable than the network layer service.
- Lost packets and damaged data can be detected and compensated for by the transport layer.



- The transport service primitives can be designed to be independent of the network service primitives.
- The transport layer makes it possible for application layer programs to be written using a standard nonvarying set of primitives (network layer service primitives vary a lot).
- These programs can work on a wide variety of networks due to transport layer.
- Thus the transport layer isolates the upper layers from the technology, design and imperfections of the subnet.
- Hence the layers of reference model are divided into two groups.
- Layers 1 to 4 form the first group called **transport service provider** and the layers above 4 are in the second group called **transport service users**.

6.3.1 Quality of Service (QoS) :

SPPU : Dec. 11

University Questions

Q.1. What is QoS? Explain various parameters for QoS in a network. (Dec. 11 5 Marks)

- As mentioned earlier, the QoS parameters are as follows :

1. Connection establishment delay :

- The time difference between the instant at which a transport connection is requested and the instant at which it is confirmed is called as **connection establishment delay**.
- The shorter the delay the better the service.

2. Connection establishment failure probability :

- It is the probability that connection is not 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 measures the number of bytes of user data transferred per second, measured over some time interval.
- It is measured separately for each direction.

4. Transit delay :

It is the time between a message being sent by the transport user on the source machine and its being received by the transport user on the destination machine.

5. Residual error ratio :

- It measures the number of lost or garbled messages as a fraction 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 from being read or modified by some unauthorised parties.

7. Priority :

- This parameter provides a way for the user to show that some of its connections are more important (have higher priority) than the other ones.
- This is important while handling the congestions. 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.

6.4 Transport Service Primitives :

SPPU : Dec. 08

University Questions

Q.1. List and explain any four transport service primitives. (Dec. 08 5 Marks)

- The transport service primitives allow the transport user such as application programs to access the transport service.
- Each transport service has its own access primitives.
- The transport service is similar to network service but there are some important differences. The main difference is that the connection-oriented transport service is reliable.
- The second difference between the network service and transport service is whom the services are intended for. The transport primitives are seen by many programs and programmers. Hence the transport service is convenient and easy to use.
- We can get the idea about the transport services by referring to Table 6.4.1 which lists the five primitives.



Table 6.4.1 : Primitives for a simple transport service

No.	Primitive	TPDU sent	Meaning
1.	LISTEN	None	Block until some process tries to connect
2.	CONNECT	Connection request	Actively attempt to establish a connection
3.	SEND	Data	Send data
4.	RECEIVE	None	Block until a data TPDU arrives
5.	DISCONNECT	Disconnection request	Release the connection

- The transport interface allows the application programs to establish, use and release connections.
- Let us see how these primitives are used in actual applications.
 - The server executes a LISTEN primitive. This will make a system call to block the server until a client turns up.
 - When a client wants to talk to the server it executes the CONNECT primitive.
 - In response the transport entity blocks the caller and sends a packet to the server. The transport layer message is encapsulated in the payload of this packet for the server's transport entity.

TPDU :

The message sent from transport entity to transport entity is called as transport protocol data unit or TPDU.

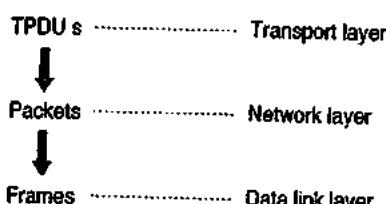
6.4.1 Nesting of TPDUs, Packets and Frames

SPPU : May 06

University Questions

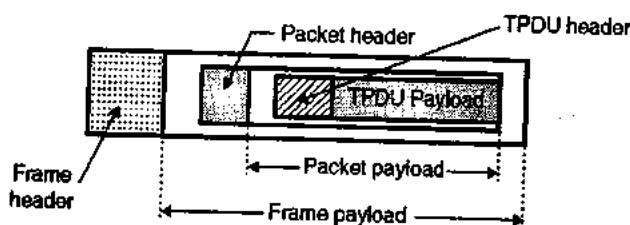
Q.1 Under the transport service what is meant by nesting TPDUs ? Illustrate with diagram a connection establishment between a client and server using TPDUs ? (May 06, 9 Marks)

- The TPDUs which are exchanged by the transport layer are contained in the packets that are exchanged by the network layer.



(G-599(a)) Fig. 6.4.1

- These packets are in turn contained in the frames which are exchanged by the data link layer.
- When a frame arrives, the data link layer processes the frame header and passes the contents of the frame payload field to the network entity.
- The network entity processes the packet header and passes the contents of the packet payload to the transport entity.
- This is called as "Nesting" and it is illustrated in Fig. 6.4.2.



(G-600) Fig. 6.4.2 : Nesting of TPDUs, packets and frames

Connect primitive :

- If a client gives the CONNECT call, then a connection request TPDU is sent to the server.
- When this TPDU arrives, the transport entity checks if the server is blocked on a LISTEN. It then unblocks the server and sends a connection accepted TPDU back to the client.
- On arrival of this TPDU, the client is unblocked and connection is established.

SEND and RECEIVE Primitives :

- The SEND and RECEIVE primitives can be used for exchange of data.
- The data exchange at the network layer is more complicated than that at the transport layer.
- In transport layer data exchange, every data packet is eventually acknowledged. The packets carrying control TPDUs are also acknowledged.
- All these acknowledgements are managed by the transport entities using the network layer protocols.
- The transport entities have to take care of issues like timers and retransmission.
- The transport layer connection acts as a reliable bit pipe through which the bits sent by a sender come out from the other side of pipe.

Connection release :

- A connection should be released when it is no longer needed. This is essential in order to free up the table space within the two transport entities.
- Disconnection can be of two types :
 - Asymmetric
 - Symmetric



6.5 Sockets and Their Programming :

SPPU : Dec. 06, May 12, Dec. 12, May 13.
Dec. 13, Feb. 16

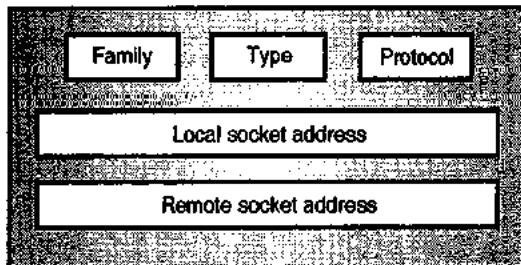
University Questions

- Q. 1** What is socket ? Explain with suitable example the connection between client and server with the help of socket. (Dec. 06, 8 Marks)
- Q. 2** What is socket ? List and explain various socket primitives required in UDP socket program on client and server side. (May 12, Dec. 12, May 13, Dec. 13, 6 Marks)
- Q. 3** What is socket ? Which are various socket primitives used in client server communication. (Feb. 16, 5 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. 6.5.1 shows a simplified socket structure.



(G-61) Fig. 6.5.1 : Socket structure

- Various fields in the socket structure are as follows :
 - Family** : This field is used for defining the protocol group such as IPv4 or IPv6, UNIX domain protocol etc.
 - Type** : This field is used for defining the type of socket such as stream socket, packet socket or raw socket.
 - Protocol** : This field is usually set to zero for TCP and UDP.
 - 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.
 - 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.

6.5.1 Socket Types :

SPPU : Feb. 16

University Questions

- Q. 1** What is socket ? Which are various socket primitives used in client server communication. (Feb. 16, 5 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 :

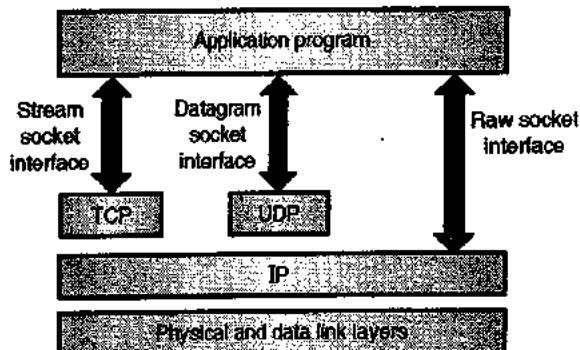
This is designed for the connection oriented protocol such as TCP. The TCP uses a pair of stream sockets one each on either ends for connecting one application program to the other across the Internet.

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. 6.5.2 shows the three types of socket types.



(G-62) Fig. 6.5.2 : Type of sockets

6.5.2 Berkeley Sockets :

SPPU : May 08, May 11, May 12, Dec. 12,

May 13, Dec. 13, Dec. 15, Feb. 16

University Questions

- Q. 1** What is Berkeley Sockets ? Explain the primitives in it. (May 08, 8 Marks)

- Q. 2** 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 no confusion in the concurrent approach ? (May 11, 8 Marks)



- Q. 3** What is socket ? List and explain various socket primitives required in TCP socket program on client and server side.

(May 12, Dec. 12, May 13, Dec. 13, 6 Marks)

- Q. 4** Explain socket programming with its primitives. (Dec. 15, 6 Marks)

- Q. 5** What is socket ? Which are various socket primitives used in client server communication. (Feb. 16, 5 Marks)

- Table 6.5.1 lists various transport primitives used in Berkeley UNIX for TCP.

Table 6.5.1

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 6.5.1 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.

6.5.3 Steps Followed for Socket Programming :

SPPU : Dec. 15, Feb. 16

University Questions

- Q. 1** Explain socket programming with its primitives. (Dec. 15, 6 Marks)

- Q. 2** What is socket ? Which are various socket primitives used in client server communication. (Feb. 16, 5 Marks)

- The steps followed for the socket programming are as follows :

Server side :

- Server creates a socket and checks for errors using SOCKET.
- Assign address to the newly created socket using BIND.
- Use the LISTEN to allocate space for the queue which is used for the incoming calls.
- Execute an ACCEPT for blocking the waiting incoming connections.

Client side :

- Create a socket using SOCKET.
- Use CONNECT to initiate connection process.
- Establish the connection.

6.5.4 Connectionless Iterative Server (Datagram Socket) :

SPPU : Dec. 06, Dec. 11, May 12

University Questions

- Q. 1** What is the socket ? Explain with suitable example, the connection between client and server with the help of socket. (Dec. 06, 8 Marks)

- Q. 2** Write a pseudo code for client and server to setup a connectionless service between them. (Dec. 11, 8 Marks)

- Q. 3** What is socket ? List and explain various socket primitives required in UDP socket program on client and server side. (May 12, 6 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.

6.5.5 Connection Oriented Concurrent Server (Stream Socket) :

SPPU : Dec. 06, May 11

University Questions

- Q. 1** What is the socket? Explain with suitable example, the connection between client and server with the help of socket. (Dec. 06, 8 Marks)
- Q. 2** 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 no confusion in the concurrent approach? (May 11, 8 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.

6.6 Elements of Transport Protocols :

- In order to implement the transport layer services between the two transport entities, we have to use a **transport protocol**.
- The transport protocols have to deal with the following tasks.
 - 1. Error control 2. Sequencing and
 - 3. Flow control
- The transport protocols are similar to the data link protocols in many ways but there are some dissimilarities as well.
- At the data link layer two router communicate directly via a physical channel as shown in Fig. 6.6.1(a), whereas at the transport layer the physical channel is replaced by the entire subnet as shown in Fig. 6.6.1(b).
- The difference between data link and transport layer communication is as follows :

Table 6.6.1

Sr. No.	Data-link layer	Transport layer
1.	Communication is through a physical channel.	Communication is through a subnet
2.	It is not necessary to specify the destination router.	Explicit addressing of destination is essential.

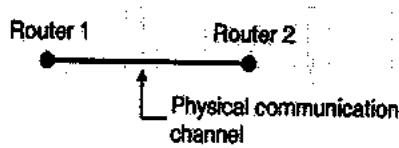
Sr. No.	Data link layer	Transport layer
3.	Establishing a connection is simple	Initial connection establishment is more complicated.
4.	No storage capacity	There is some storage capacity in the subnet.
5.	No additional delay	Delay is introduced due to the storing capacity of subnets.
6.	Different approaches are used for buffering and flow control by the two layers.	

Elements of transport protocols :

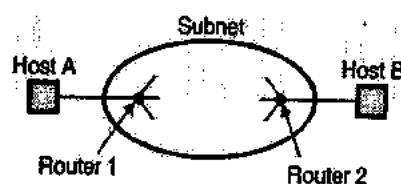
- Following are some of the important elements of transport protocols.
 1. Addressing
 2. Establishing a connection
 3. Releasing a connection
 4. Flow control and buffering
 5. Multiplexing
 6. Crash recovery
- In the following sections we will discuss these elements.

6.7 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.



(a) Router connection at data link layer



(b) Router connection at transport layer

(G-603) Fig. 6.6.1

6.8 User Datagram Protocol (UDP) :

SPPU : May 10

University Questions

Q. 1 What are the functions of UDP ? Explain the UDP header format in detail. (May 10, 8 Marks)

- 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).

6.8.1 Well Known Ports for UDP :

Table 6.8.1 shows some well known port numbers used by UDP. Some of these ports can be used by UDP as well as TCP.

Table 6.8.1 : 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	BOOTP _s	This is the server port to download the bootstrap information.
68	BOOTP _c	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).

6.8.2 User Datagram :

SPPU : May 12, Dec. 12, Dec. 13

University Questions

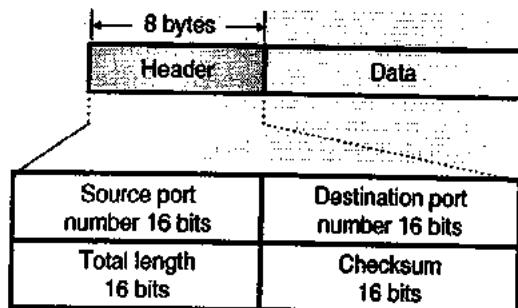
Q. 1 Draw UDP header structure. Explain significance of each field in UDP header. What is pseudo-header? (May 12, Dec. 12, 6 Marks)

Q. 2 "UDP does not guarantee reliability in data transfer but delivered data is error free". Justify this statement. (Dec. 12, Dec. 13, 6 Marks)

- 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. 6.8.1.



(G-62)Fig. 6.8.1 : User datagram format

The UDP header is divided into the following four 16-bit fields :

1. Source port
2. Destination port
3. Total length
4. Checksum.

Source port :

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.

Destination port :

Destination port has a meaning within the context of a particular Internet destination address.

Length :

This is the size in bytes of the UDP packet, including the header and data. The minimum length is 8 bytes, the length of the header alone.

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.

6.8.3 UDP Pseudo Header :

SPPU : May 08, May 10, May 12, Dec. 12, Dec. 13

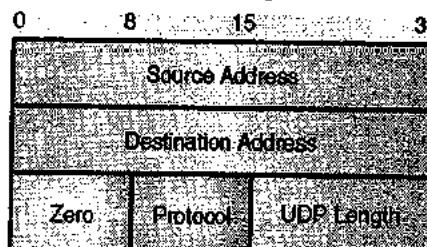
University Questions

- Q. 1** Explain UDP header. Explain RPC in detail.

(May 08, 8 Marks)

- Q. 2** What are the function of UDP? Explain the UDP header format in detail. (May 10, 8 Marks)
- Q. 3** Draw UDP header structure. Explain significance of each field in UDP header. What is pseudo-header? (May 12, Dec. 12, 6 Marks)
- Q. 4** Draw and explain UDP header. What is pseudo header? Why it is required? (Dec. 13, 6 Marks)

- 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.
- 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.



(G-62)Fig. 6.8.2 : UDP pseudo header

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.

6.8.4 UDP Operation :

- The UDP uses concepts that are common to the transport layer. We will discuss the following concept in brief :

- Connectionless services.
- Flow control and error control.
- Encapsulation and Decapsulation.
- Queuing.

1. Connectionless services :

- As discussed earlier the type of service provided by UDP is a connectionless service. That means all the datagram sent to user by UDP are independent datagrams.
- All the user datagrams are totally independent of each other even though they are emerging from the same source process and going to the same destination process.
- These datagrams are not numbered. No connection establishment or connection release (termination) is necessary. Each datagram can follow a different path.

2. 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.

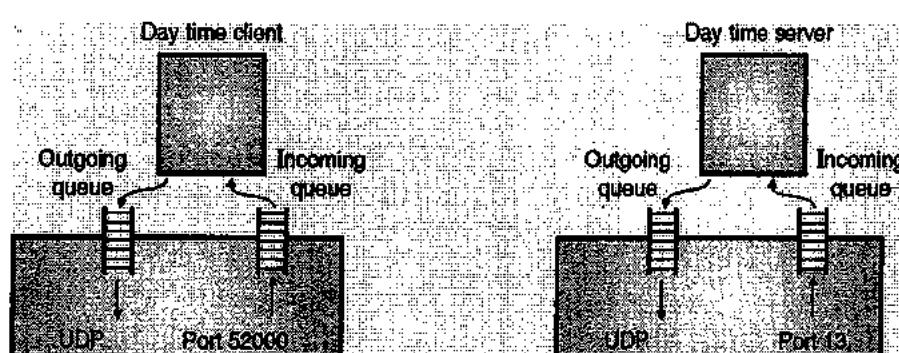
3. Encapsulation and decapsulation :

The UDP encapsulates and decapsulates messages in an IP datagram in order to exchange the message between two communicating processes.

4. Queuing :

The queues in UDP are related with ports as shown in Fig. 6.8.3.

- 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.



(G-62) Fig. 6.8.3 : Queues in UDP



- 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.

6.8.5 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.

6.9 Transmission Control Protocol (TCP) :

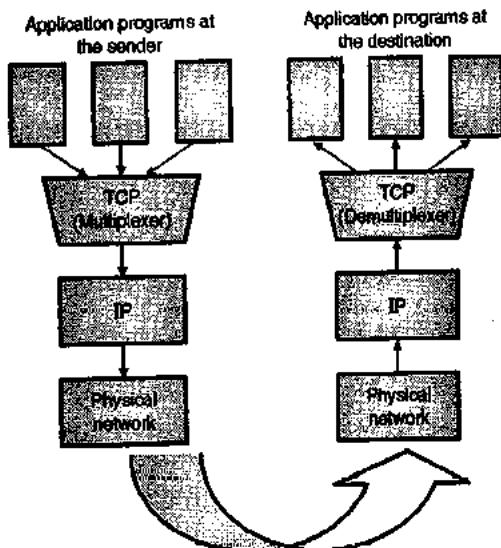
- The Internet has two main protocols in the transport layer. One of them is connection oriented and the other one supports the connectionless service.
- TCP (Transmission control protocol) is a connection oriented protocol and UDP (User Datagram Protocol) is the connectionless protocol.
- UDP is basically just IP with an additional short header.
- 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.
- 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.

6.9.1 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. 6.9.1.

- 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. 6.9.1.

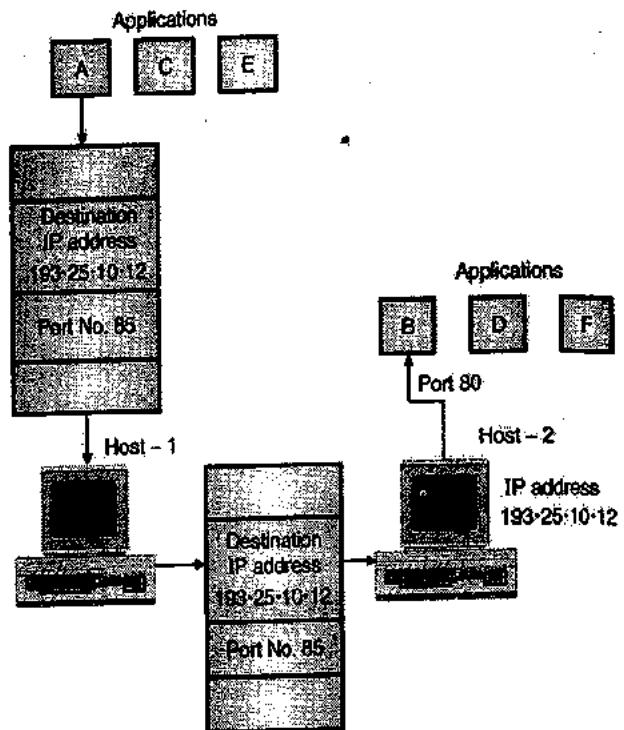


(G-144) Fig. 6.9.1 : Multiplexing and demultiplexing using TCP

6.9.2 Ports and Sockets :

1. Ports :

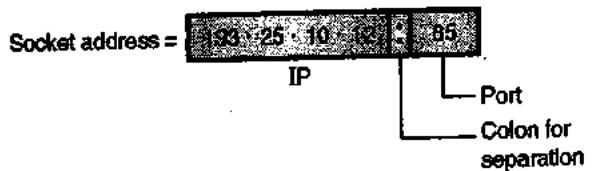
- Applications running on different hosts communicate with TCP with the help of ports. Every application has been allotted a unique 16 bit number which is known as a port.
- When an application on one computer wants to communicate using a TCP connection to another application on some other computers 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. 6.9.2 and explained below.
- 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. 6.9.2.
- Computer 1 communicates with computer 2 using the IP address and computer 2 uses the port number to direct the message to application B.



(G-145) Fig. 6.9.2 : Use of port numbers

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. 6.9.3.
- 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.

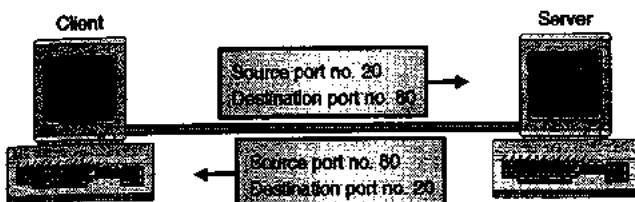


(G-146) Fig. 6.9.3

- 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. 6.9.4.
- 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. 6.9.4.



(G-143) Fig. 6.9.4 : Source and destination port numbers

6.10 Features of TCP :

- TCP is a process-to-process protocol.
- TCP uses port numbers.
- It is a connection oriented protocol (creates a virtual connection).
- It uses flow and error control mechanisms.
- TCP is a reliable protocol.

6.11 TCP Services :

SPPU : Dec. 13

University Questions

- Q. 1 Explain functionality of TCP. Explain flow control in detail. (Dec. 13, 6 Marks)**

Following are some of the services offered by TCP to the processes at the application layer :

- Stream delivery service
- Sending and receiving buffers
- Bytes and segments
- Full duplex service
- Connection oriented service
- Reliable service.
- Process to process communication.

1. Process to process communication :

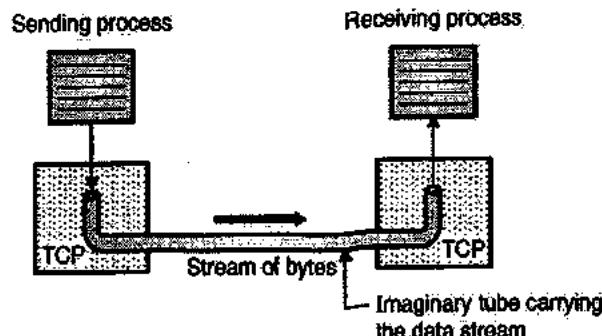
- The TCP uses port numbers as transport layer addresses. Table 6.11.1 shows some well known port numbers used by TCP.
- Note that if an application can use both UDP and TCP, the same port number is assigned to this application.

Table 6.11.1 : Well known ports used by TCP

Port	Protocol	Description
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

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. 6.11.1.
- This is called as stream delivery service.

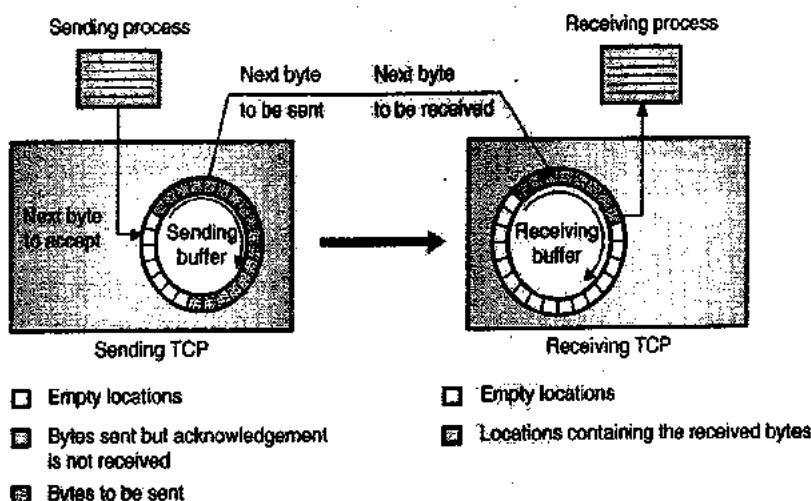


(G-62) Fig. 6.11.1 : Stream delivery service

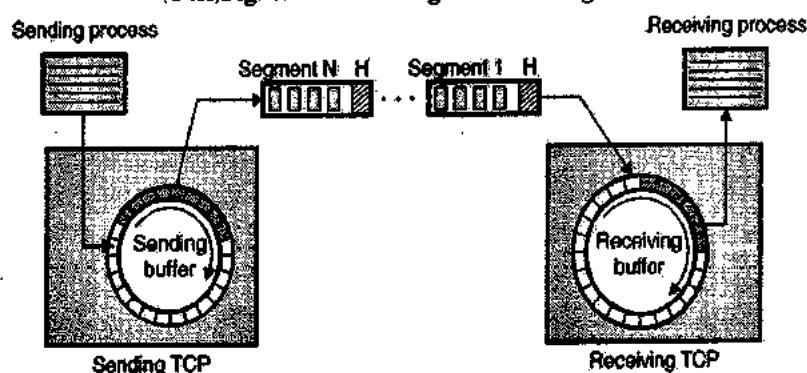
3. Sending and receiving buffers :

- 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 :
 - Sending buffer
 - Receiving buffer.
- A buffer can be implemented by using a circular array of 1 byte locations as shown in Fig. 6.11.2.
- Fig. 6.11.2 shows the direction of movement of data. The sending buffer has three types of locations :

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



(G-62)Fig. 6.11.2 : Sending and receiving buffers



(G-62)Fig. 6.11.3

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.
- 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. 6.11.3 shows the creation of segments from the bytes in the buffers.
- The segments are not of the same size. Each segment can carry hundreds of bytes.

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.

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.

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.

6.12 TCP Features :

SPPU : May 12

University Questions

Q.1 Explain error control and flow control in TCP.

(May 12, 6 Marks)

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.

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.

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.

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.

6.13 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 :
 - Each segment including the TCP header, must fit in the 65535 byte IP payload.
 - 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.

6.13.1 TCP Segment :

The TCP segment as shown in Fig. 6.13.1 consists of two parts :

1. Header 2. Data



(G-142)Fig. 6.13.1 : TCP segment

6.13.2 The TCP Segment Header :

SPPU : May 06, Dec. 09, May 12,
Dec. 12, May 13, Dec. 13

University Questions

Q. 1 Draw and explain TCP header format.

(May 08, 8 Marks)

Q. 2 Describe the format of TCP header.

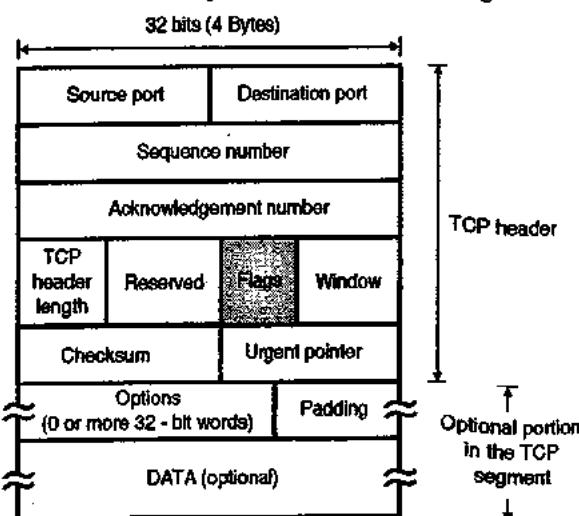
(Dec. 09, 8 Marks)

Q. 3 Explain significance of following flags in TCP header.
SYN, RST, FIN, PSH.

(May 12, Dec. 12, May 13, 6 Marks)

Q. 4 Draw TCP header. Explain significance of each field in TCP header. (Dec. 13, 6 Marks)

- Fig. 6.13.2 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.
- The TCP segment without data are used for sending the acknowledgements and control messages.



(G-61)Fig. 6.13.2 : TCP header format

**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 49151) and private ports (49152 through 65535). 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.

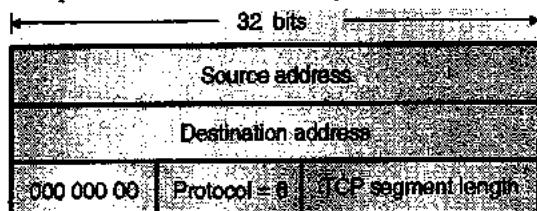
Data :

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.



6.13.3 Checksum :

- A checksum is provided to ensure extreme reliability. It checksums the header, the data and the conceptual pseudo header shown in Fig. 6.13.3.



(G-612)Fig. 6.13.3 : 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. 6.13.3.

6.14 TCP Connections :

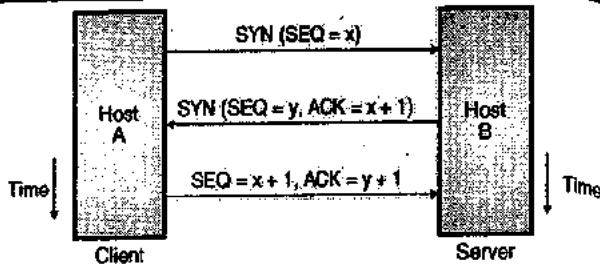
6.14.1 TCP Connection Establishment :

SPPU : May 13

University Questions

Q. 1 Draw and explain three way handshake process of TCP. (May 13, 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. 6.14.1(a).

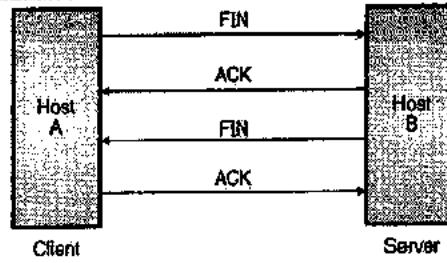


(G-613) Fig. 6.14.1(a) : TCP connection establishment (Three-way handshake)

- 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.

6.14.2 Connection Termination Protocol [Connection Release] :

- 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. 6.14.1(b). 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.



(G-614) Fig. 6.14.1(b) : TCP termination

- 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. 6.14.1(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.

6.14.3 TCP Connection Management :

- 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. 6.14.2(a).
- 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.

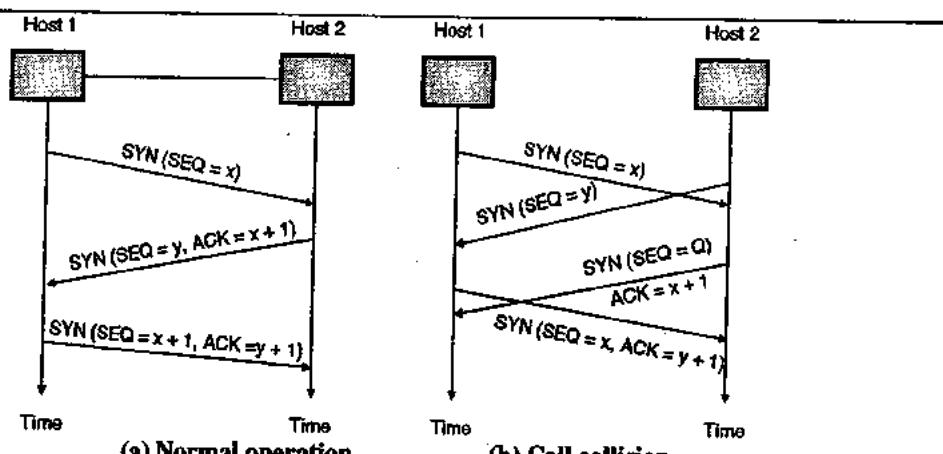
- Otherwise it gives the TCP segment to the listening process, which can accept or refuse (e.g. if it does not like the client) the connection. On acceptance a SYN is send, otherwise a RST. Note that a SYN segment occupies 1 byte of sequence space so it can be acknowledged unambiguously.

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. 6.14.2(b).
- Under such circumstances only one connection is established. Both the connections cannot 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.

6.14.4 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.



(G-615) Fig. 6.14.2 : TCP connection management

- 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.

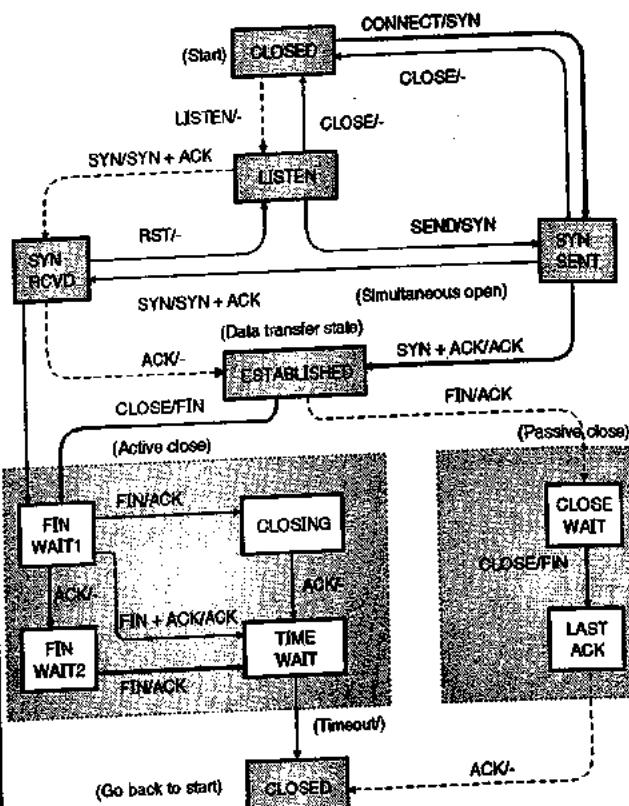
6.15 TCP State Diagram :

- The steps to be followed in TCP connection establishment and release can be represented using a finite state machine.
- The total eleven states in such a state machine are given in Table 6.15.1.

Table 6.15.1 : Different states in TCP finite state machine

State	Description
CLOSED	No connection is active or pending
LISTEN	The server is waiting for an incoming call
SYN RCVD	A connection request has arrived; wait for ACK
SYN SENT	The application has started to open a connection
ESTABLISHED	The normal data transfer state
FIN WAIT 1	The application has said it is finished
FIN WAIT 2	The other side has agreed to release
TIMED WAIT	Wait for all packets to die off
CLOSING	Both sides have tried to close simultaneously
CLOSE WAIT	The other side has initiated a release
LAST ACK	Wait for ack of FIN of last close

- In each of the 11 states shown in Table 6.15.1, some specific events are considered to be legal events. Corresponding to every legal event some action may be taken, but if some event other than the legal one happens, then error is reported.
- The finite state machine is shown in Fig. 6.15.1.



(G-69) Fig. 6.15.1 : TCP connection management final state machine

- Each connection is always in the CLOSED state initially. It comes out of this state when it does either the passive open (LISTEN) or an active open (CONNECT).
- A connection is established, if the other side does the opposite and the state becomes ESTABLISHED.
- When both the sides initiate a connection release the connection is terminated and the state returns to CLOSED state.

Various types of lines in the finite state machine drawing :

- Various types of lines are used in the finite state machine drawing of Fig. 6.15.1. They have different meanings as stated below :
 - Heavy solid lines** : These lines show a client actively connecting to a passive server.
 - Heavy dotted lines** : These lines are used for the server.
 - The light faced lines** : These are for unusual event sequences.
- Over each line in Fig. 6.15.1 we have written the event / action pair.
- The event can either be a user-initiated system call (CONNECT, LISTEN, SEND or CLOSE), a segment arrival (SYN, FIN, ACK or RST), or a time-out.

- For the TIMED WAIT state the event can only be a time-out of twice the maximum packet length. The action is the sending of a control segment (SYN, FIN or RST) or nothing.
- The time-outs to guard for lost packets (e.g. in the SYN SENT state) are not shown here.
- There are 11 states used in the TCP connection management finite state machine. Data can be send in the ESTABLISHED and the CLOSE WAIT states and received in the ESTABLISHED and FIN WAIT1 states.

Explanation :

- To understand the finite state machine of Fig. 6.15.1, first follow the path of a client i.e. the heavy solid line. After that follow the path of the server (the heavy dashed line).

6.16 TCP Sliding Window (TCP Transmission Policy) :

SPPU : Dec. 07, Dec. 08, May 13

University Questions

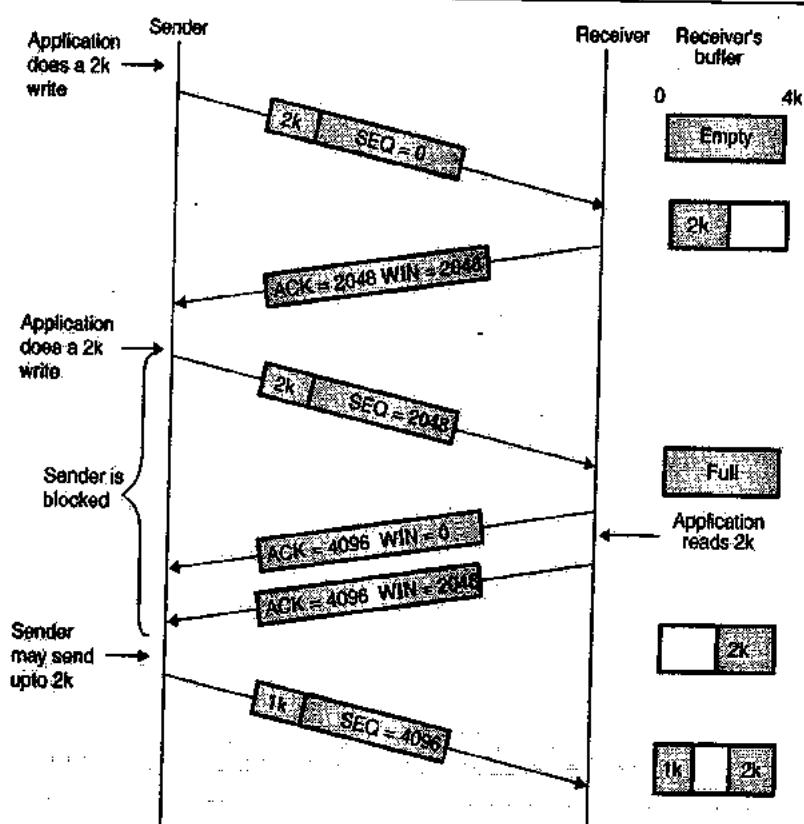
- Q.1** How Nagle algorithm helps in TCP transmission policy? Explain the Clark's solution to overcome the silly window syndrome. (Dec. 07, 8 Marks)
- Q.2** What do you mean by silly window syndrome problem? Explain the Clark's and Nagle algorithm to overcome this problem. (Dec. 08, 8 Marks)

Q.3 Explain flow control in TCP (May 13, 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. 6.16.1.

Explanation :

- Let the receiver in Fig. 6.16.1, 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.



(G-616) Fig. 6.16.1 : Windows management in TCP

- 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.
 - First, urgent data may be send, e.g. to allow the user to kill the process running on the other machine.
 - 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. It can be stated as follows.

6.16.1 Nagle's Algorithm :

- When data come into the sender one byte at a time (e.g. on a Telnet connection), just the first byte is send and the rest is buffered until the outstanding byte is acknowledged.
- Nagle's algorithm is widely used but sometime it is better not to use it. For example consider an X-windows application being run over the Internet.
- The mouse movements are to be sent to the remote computer.
- If we gather the mouse movements together and send them in the form of a burst then the mouse cursor movements will be erratic. So each mouse movement must be sent separately. This degrades the TCP performance.

6.16.2 Silly Window Syndrome :

SPPU : May 06, Dec. 07, Dec. 08, May 09, May 10

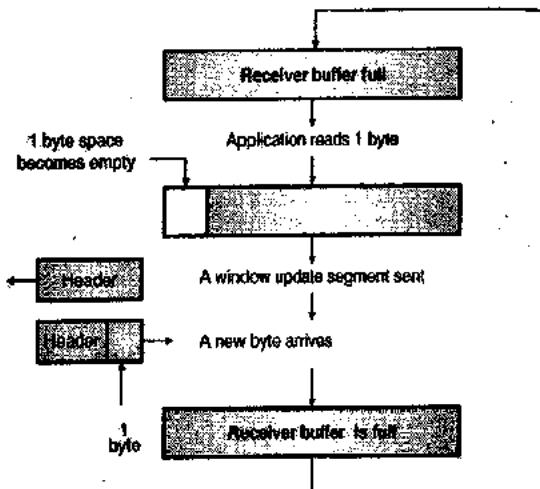
University Questions

- Q. 1** Illustrate the phenomenon of silly window syndrome in TCP ? (May 06, 8 Marks)
- Q. 2** How Nagle algorithm helps in TCP transmission policy ? Explain the Clark's solution to overcome the silly window syndrome. (Dec. 07, 8 Marks)

Q. 3 What do you mean by silly window syndrome problem ? Explain the Clark's and Nagle algorithm to overcome this problem. (Dec. 08, 8 Marks)

Q. 4 What is silly window syndrome problem ? Suggest two solutions to overcome the silly window syndrome problem. (May 09, May 10, 8 Marks)

- This is another problem that can degrade the TCP performance.
- This problem occurs when the sender transmit 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. 6.16.2.



(C-617) Fig. 6.16.2 : Silly window syndrome

- Initially the receiver's buffer is full so it send a window size 0 to block the sender.
- But the interactive application reads one byte from the buffer. So one byte space becomes empty.
- The receiving TCP sends a window update to the sender informing that it can send 1 byte.
- The sender send 1-new byte.
- The buffer is full again and the window size is 0. This process can continue forever. This is known as the silly window syndrome.

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 receiver's buffer size.

6.17 TCP Congestion Control :

SPPU : Dec. 11, May 12

University Questions

- Q. 1** Explain TCP congestion control algorithm with respect to additive increase, multiplicative decrease, slow start mechanism and reaction to timeout events. (Dec. 11, 8 Marks)
- Q. 2** Describe TCP congestion control approach. (May 12, 8 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 detect 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 :

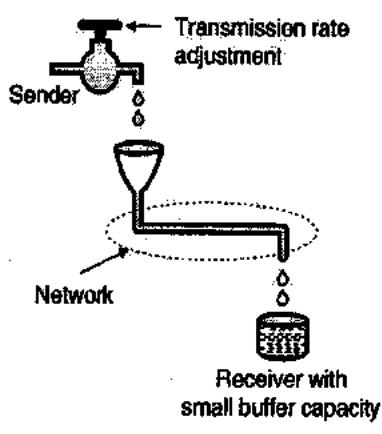
- This is the first step in congestion control. Now-a-days packet loss due to transmission errors is very rare because the optical fiber links are being used. So most transmission time-outs (loss of packets) are due to congestions.
- So all the Internet TCP algorithms assume that time-outs are caused by congestion and so time outs can be used to detect the congestion.

Step 2 : Try to prevent congestion :

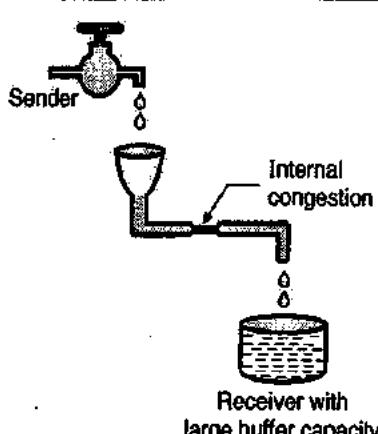
- After establishing a connection, a suitable window size is to be chosen. The receiver window size is based on its buffer capacity. If the sender adjusts its transmission rate according to this capacity as shown in Fig. 6.17.1(a), the congestion due to buffer overflow will never take place.
- Now consider Fig. 6.17.1(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.

Conclusion :

To prevent congestion TCP has to deal with two problems separately – receiver capacity and network capacity.



(a) No congestion



(b) Internal

(G-618) Fig. 6.17.1 : Congestion

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 :
 - 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.
 - 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**.

6.17.1 Slow Start Algorithm :

SPPU : Dec. 11

University Questions

- Q.1** Explain TCP congestion control algorithm with respect to additive-increase, multiplicative-decrease, slow start mechanism and reaction to timeout events. (Dec. 11, 8 Marks)

- 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.
- 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.
- 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. 6.17.2. This is the exponential growth of the congestion window size.
- 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.
- 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.
- 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.
- Once this is done, no data bursts longer than 2048 bytes will be sent by the sender even if receiver grants a wider window.
- The name of this algorithm is slow algorithm and it is required to be supported by all the TCP implementations.

6.17.2 Internet Congestion Control Algorithm :

SPPU : May 07, May 11, Dec. 11

University Questions

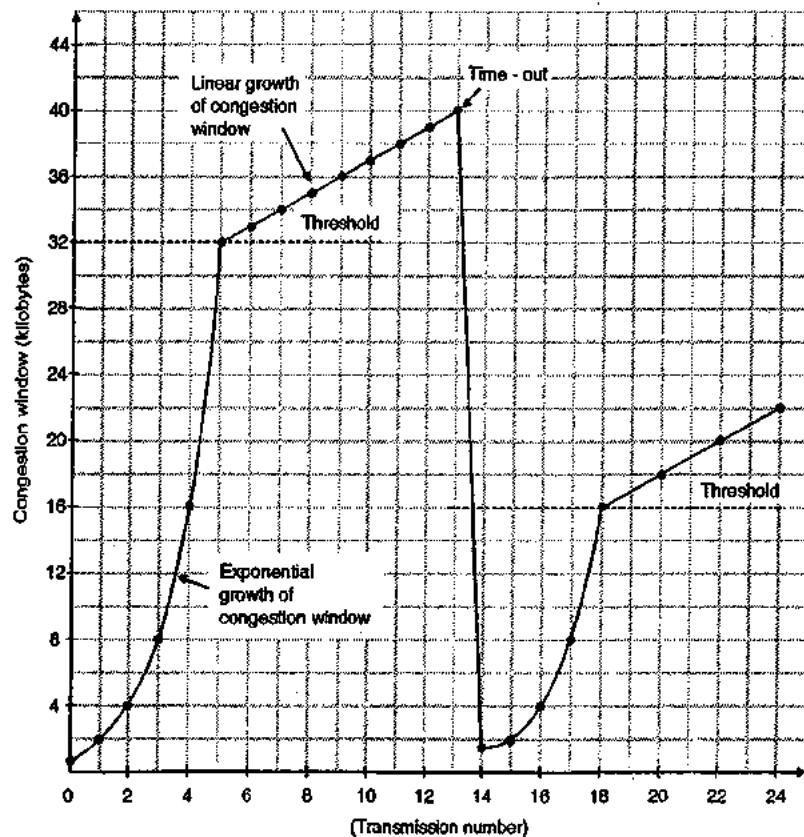
- Q. 1** Define threshold condition in congestion. How does TCP tackle congestion problem using internet congestion control algorithm? **(May 07, May 11, 8 Marks)**

Q. 2 Explain TCP congestion control algorithm with respect to additive-increase, multiplicative-decrease, slow start mechanism and reaction to timeout events. **(Dec. 11, 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. 6.17.2.
 - Table 6.17.1 is used to plot the graph of Fig. 6.17.2. See how the threshold point acts as the boundary of the exponential growth and linear growth of the congestion window.
 - 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. 6.17.2.)

(G-6I^(a)) Table 6.17.1



(G-619) Fig. 6.17.2 : Internet congestion control algorithm

- Then the congestion window grows exponentially till the congestion window size reaches the threshold of 32 kB.
- The threshold occurs at 32 kB 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 kB) 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.

6.17.3 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. 6.17.3.

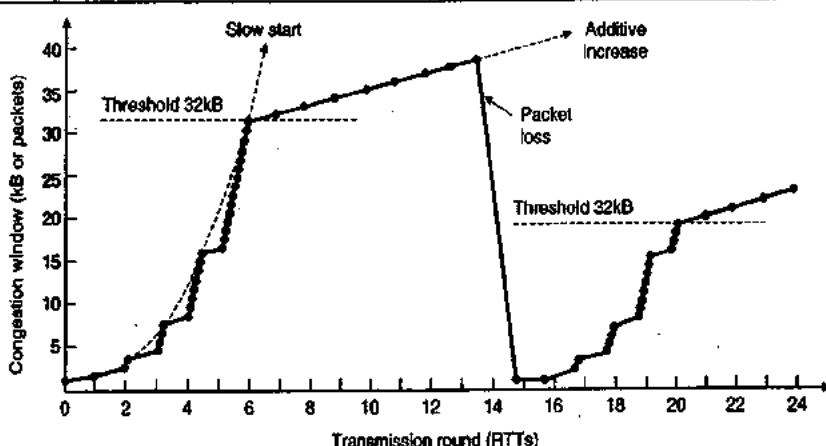
6.17.4 Fast Retransmission :

- The defect in the previous algorithm is waiting for timeout, because time outs are usually long.
- This is what happens after a packet is lost. If a packet is lost the receiver cannot acknowledge it. That means the acknowledgement number will remain fixed and the sender is unable to send any new packets because its congestion window remains full.

- This condition can continue for a long time until the timer goes out (time out occurs) and the lost packet is retransmitted (At this moment the TCP slow starts again).
- In order to save all this time, a fast way for the sender to understand that one of the packets is lost had been devised. It is as follows :
- When the packets beyond the lost packet reach the receiver, they sent back acknowledgements bearing the same number to the sender. Such acknowledgements are called as **duplicate acknowledgements**.
- Thus receiving duplicate acknowledgements is an indication that a packet has been lost. TCP arbitrarily assumes that receiving three duplicate acknowledgements imply a lost packet.
- This lost packet can be retransmitted immediately before the retransmission timer times out.
- This is known as **Fast Retransmission**. Then the slow start threshold is set to half the current congestion window. This is same as what is done after timeout.
- The slow start can be restarted by setting the congestion window to one packet.
- After one RTT (Round Trip Time) the acknowledgement of the retransmitted packet will be received and a new packet can be transmitted.
- This type of congestion control algorithm is as shown in Fig. 6.17.3.

6.17.5 TCP Tahoe :

- The TCP version using the fast retransmitting concept (Fig. 6.17.3) is called as **TCP Tahoe** after the 4.2 BSD Tahoe released in 1988 in which it was included.



(G-1523) Fig. 6.17.3 : Slow start followed by additive increase

- As shown in Fig. 6.17.3, the maximum segment size is 1 kB. Initially the size of congestion window was 64 kB but due to occurrence of timeout the threshold is set to 32 kB, and the congestion window to 1 kB for transmission 0 (that means initially).
- Upto the threshold of 32 kB the congestion window will grow exponentially. Note the discrete staircase pattern graph. This happens because the window size is increased corresponding to receiving a new acknowledgement and not continuously.
- Once the threshold is reached, the congestion window grows linearly. Its increase by one segment for every RTT (every acknowledgement).
- When a packet is lost (see Fig. 6.17.3), its loss is detected by three duplicate acknowledgements as discussed earlier, and the lost packet is immediately retransmitted.
- The threshold is set to half the current size of congestion window. The current size at the time of packet loss was 40 kB (Fig. 6.17.3) hence the new threshold is set to 20 kB, and the slow start is initiated again.
- TCP Tahoe provided a good working congestion control algorithm which sorted out the problem of congestion collapse.

6.17.6 Fast Recovery :

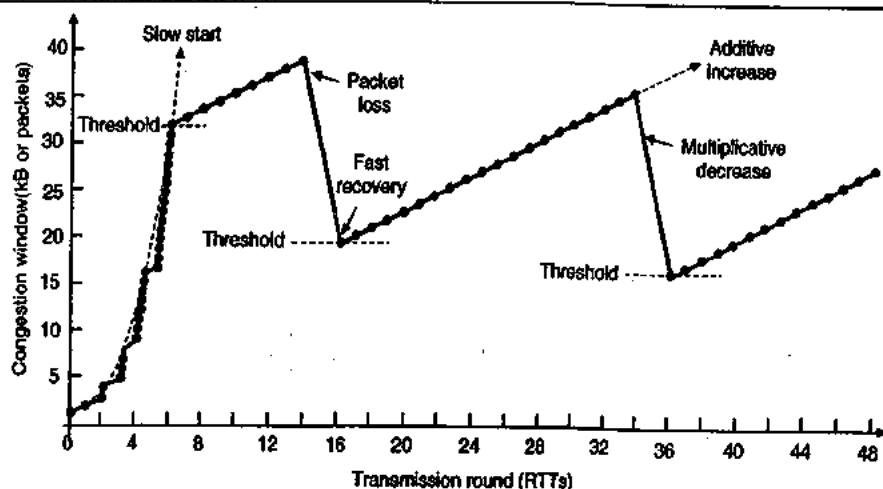
- Jacobson realized that it is possible to improve the performance of TCP further.
- At the time of fast retransmission, the TCP connection is operating with a congestion window which is too large yet it is running with working ACK clock.
- Every time a duplicate acknowledgement arrives, there is a possibility that another packet has been lost. Jacobson thought that if duplicate

acknowledgements are used to count the packets in the network then it is possible to let some packets leave the network and continue to send a new packet for each additional duplicate acknowledgement.

- This concept is implemented in the **Fast Recovery** feature to TCP. It is a temporary mode of operation and it has an aim to maintain the ACK clock running with a large congestion window at the time of fast retransmission.
- In order to achieve this, duplicate acknowledgements including those three which initiated the fast retransmission are counted until the number of packets in the network has fallen to the new threshold.
- This needs about half a round trip time. As soon as the new threshold has been reached, a new packet can be sent for each duplicate acknowledgement received, as shown in Fig. 6.17.4.
- After one RTT, following fast retransmission, the lost packet will be retransmitted and the stream of duplicate acknowledgements will stop and the system will come out of the fast recovery mode. The congestion window will be set to a new slow start threshold and grows linearly as shown in Fig. 6.17.4.

Advantage :

- Due to fast recovery, the TCP avoids the slow start after each fast retransmission. Now the slow start will occur only when the connection is first started or when the time out has occurred.
- Thus repeated slow starts are avoided and the TCP window size now follows a **sawtooth** pattern of additive increase and multiplicative decrease as shown in Fig. 6.17.4.



(G-1524) Fig. 6.17.4 : Fast recovery and sawtooth pattern of TCP Reno



- This behaviour is produced by TCP Reno, named after the 4.3 BSD Reno release in 1990 in which it was included. TCP Reno is TCP Tahoe plus fast recovery.

6.18 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 retransmitted and the timer is started again.

What should be the time-out interval ?

- The most important question about the retransmission 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. 6.18.1 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. 6.18.1(b). If the value of time-out is too small (T_1 for example) then unnecessary re-transmission will take place. 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.

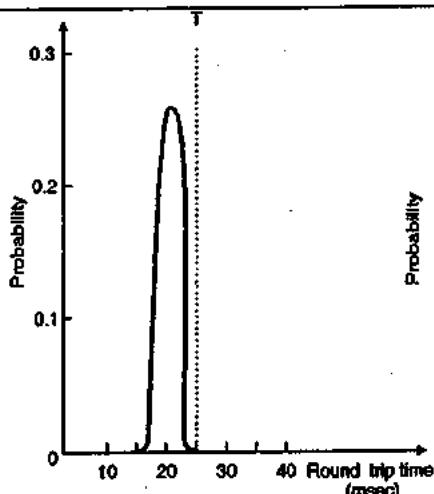
- The solution to this problem is to use a highly dynamic algorithm which adjusts the time-out interval constantly. This adjustment is based on continuous measurement of network performance.

6.18.1 Jacobson's Algorithm :

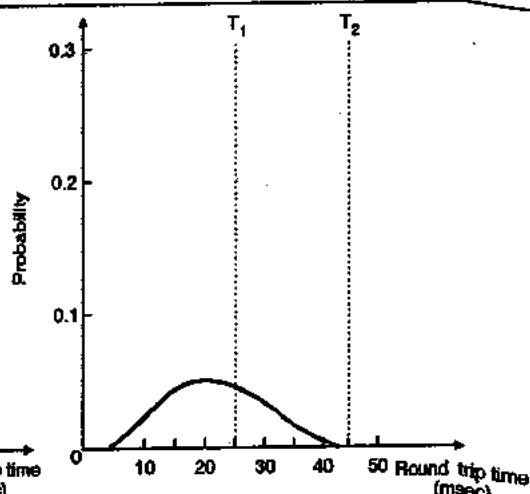
- This is the algorithm, generally used by the TCP.
- For each connection, TCP maintains a variable Round Trip Time (RTT) which is also called as SRTT (Smoothed Round Trip Time). Its value will be equal to the best current estimate of the round trip time to the desired destination.
- When a segment is 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,

$$\text{SRTT} = \alpha \text{SRTT} + (1 - \alpha) R \quad \dots(6.18.1)$$

- 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.



(a) Data link layer



(b) For TCP

(G-620) Fig. 6.18.1 : Probability density of acknowledgement arrival times

- 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,

$$\text{RTTVAR} = \beta (\text{RTTVAR}) + (1 - \beta) |\text{SRTT} - R| \quad \dots(6.18.2)$$

- The typical value of $\beta = 3/4$. The retransmission timeout RTO is set by the following expression,

$$\text{RTO} = \text{SRTT} + (4 \times \text{RTTVAR}) \quad \dots(6.18.3)$$

- 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.

6.18.2 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.

6.18.3 Other Timers in TCP :

SPPU : Dec. 08, Feb. 16

University Questions

- Q. 1** Why TCP need four different timers ? Explain the functions of retransmission, persistence, keep alive and time-waited timer. (Dec. 08, 9 Marks)
- Q. 2** Why TCP need four different timers ? Explain the functions of each. (Feb. 16, 5 Marks)

1. Persistence timer :

- The second timer in TCP is called **persistence timer**. It is designed to solve the following problem :
 - The receiver sends an ACK with window size = 0. So the sender will wait for the receiver's buffer to have some free space.

- After the receiver buffer becomes partially empty it sends a window update to the sender asking it to send.
- But the packet containing this window update is lost on its way to sender.
- 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.

2. 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.

3. 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.

6.18.4 Comparison of UDP and TCP :

SPPU : Dec. 11, May 13, Feb. 16

University Questions

- Q. 1** Explain pros and cons of TCP over UDP. (Dec. 11, 4 Marks)
- Q. 2** Differentiate between TCP and UDP protocol. Also comment on the applications supported by them. (May 13, 6 Marks)
- Q. 3** Differentiate between TCP and UDP. (Feb. 16, 5 Marks)

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.



Characteristic / Description	UDP	TCP
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; 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.

6.19 Socket Programming with TCP :

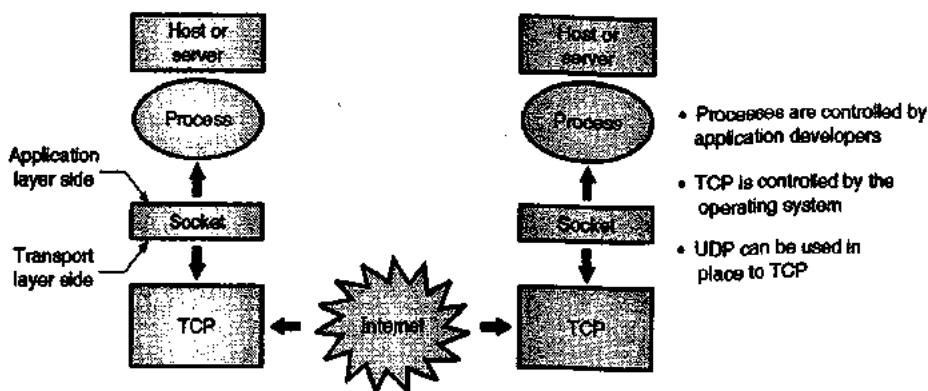
- Many network applications consist of two programs namely a client program and a server program.
- When these programs are executed a client and a server process are created which communicate with each other by reading from and writing through the sockets.
- When creating a network application, a developer has to write the code for both client and server 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 :

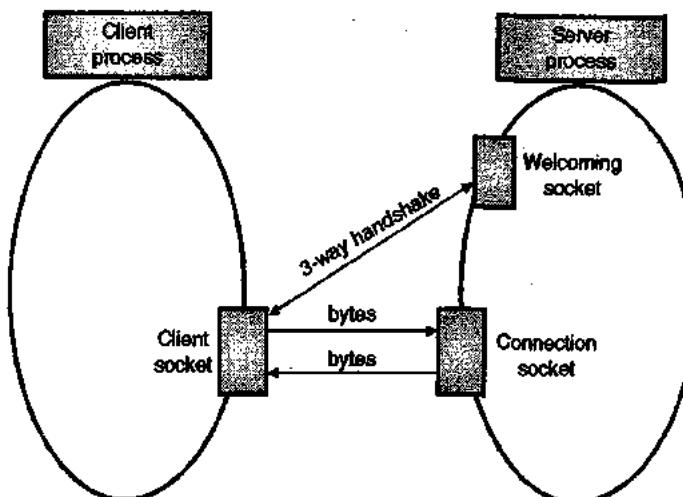
- When developing a proprietary type application, the developer needs to first decide whether the application is to run over TCP or UDP.
- TCP is connection oriented and provides a reliable byte-stream channel for the data to flow between the end systems.
- The UDP is connectionless and sends data in 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.

6.19.1 Socket Programming with TCP :

- The processes running on different machines communicate with each other by sending messages into sockets. This is demonstrated in Fig. 6.19.1.



(G-630) Fig. 6.19.1 : Communicate between processes through TCP sockets



(G-1247) Fig. 6.19.2 : Different types of sockets

- Socket acts as a door between the application process and TCP as shown in Fig. 6.19.1. 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. 6.19.2.
- 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. 6.19.2.
- 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.

6.19.2 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 :
 - No need for a welcoming socket as no handshaking is needed.
 - No streams are attached to the socket.
 - The sending host has to create packets.
 - The receiving process has to obtain information from each received packet.

6.20 Protocols for Real Time Interactive Applications :

- Real time interactive applications such as Internet phone and video conferencing have become extremely popular, now a days.
- So the standard bodies such as IETF and ITU are busy in laying out standards for this class of applications.
- The protocols used for real time interactive applications are as follows :
 - RTP (Real time protocol)
 - SIP
 - H.323

6.20.1 RTP [Real Time Protocol] :

SPPU : Feb 16

University Questions

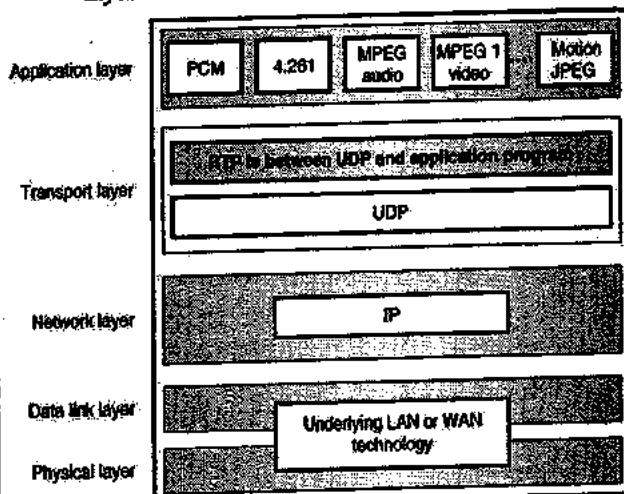
Q. 1 Explain in detail RTP with packet header format.

(Feb. 16, 6 Marks)

- RTP is the protocol designed to handle real time traffic on the Internet. It does not have a delivery mechanism like multicasting, port numbers and so on. Therefore we must use it with UDP.
- The position of RTP is between UDP and the application program as shown in Fig. 6.20.1.
- The main uses of RTP are as follows :
 - Time stamping
 - Sequencing
 - Mixing facilities.

Position of RTP in protocol suite :

- Fig. 6.20.1 shows the position of RTP in the Internet protocol suite. As shown, RTP is placed in the transport layer between UDP and the application layer.



(G-742) Fig. 6.20.1 : Position of RTP

RTP packet format :

- Fig. 6.20.2 shows the format of the RTP packet header. The format is very simple and general in nature so as to cover all real time applications.
- The description of various fields is as given below :
 - Ver :** This 2-bit field is used to define the version number of the RTP. The current version is 2.
 - P :** This is a 1-bit field, If P = 1, then it indicates that padding is present at the end of the packet.
If P = 0, it indicates that there is no padding.



3. **X :** This is a 1-bit field,

If X = 1 then it indicates the presence of an extra extension header between the basic header and the data.

If X = 0 then, no extra extension header is present.

4. **Contributor count :** This 4-bit field indicates the number of contributors. We can have at the most 15 contributors because a 4-bit field can form combinations only between 0 and 15.

V	P	X	Contributor count	M	Payload type	Sequence number
Time stamp						
Synchronization source identifier						
Contributor identifier						
:						
Contributor identifier						

Fig. 6.20.2 : RTP packet format

5. **M :** This 1-bit field is used as marker. The application used it to indicate, the end of its data.
6. **Payload type :** This is a 7-bit field which indicates the type of the payload. Different types of payloads have been defined so far. Some common applications are listed below :

Payload types :

Type	Application	Type	Application
0	PCMM audio	7	LPC audio
1	1016	8	PCMA audio
2	G721 audio	9	G722 audio
3	GSM audio	14	MPEG audio

7. **Sequence number :** This is a 16-bit field. It is used to assign number to the RTP packets. The sequence number of the first packet is randomly selected and it is incremented by 1 for each subsequent packet. The sequence number is used by the receiver to detect lost or out of order packet.

8. **Time stamp :** This is a 32-bit field that indicates the time relationship between packets. The value of time stamp for the first packet is a random number. For each succeeding packets, the value of time stamp is equal to the sum of the preceding time stamp and the time the first byte is produced (sampled).

9. **Synchronization source identifier :** If there is only one source, this 32-bit field defines the source. However if there are multiple sources, the mixer is treated as the synchronization source and the other sources will be considered as contributors. The protocol provides a strategy if there is any conflict.

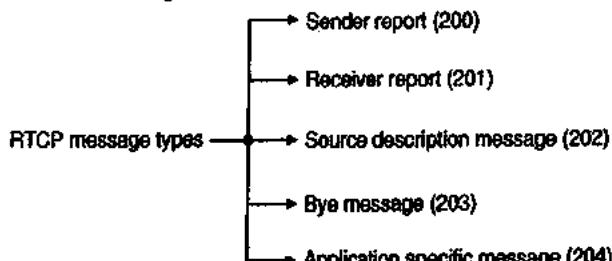
10. **Contributor identifier :** This is a 32-bit field. Each identifier (a maximum of 15) defines a source. When there is more than one source in a session, the mixer is treated as the synchronization source and the remaining sources are considered as the contributors.

UDP port :

- RTP is a transport layer protocol, but the RTP packet is not directly encapsulated in the IP datagram.
- RTP is treated like an application program and is encapsulated in a UDP user datagram. However no well-known port is assigned to RTP. This is different as compared to other application programs.
- The port can be selected whenever required with only one restriction. The port number must be an even number. The next number (an odd number) is used by the companion of RTP which is the Real Time Transport Protocol (RTCP).

6.20.2 RTCP [RTP Control Protocol] :

- RTP supports only one type of message, i.e. the one that is used to send data from source to the destination. But only one message type won't always be enough.



(C-74) Fig. 6.20.3 : RTCP message types

- Sometimes additional message types are required to be used, for controlling the flow and quality of data and to permit the destination to send feedback to the source or sources.

- The protocol designed for this purpose is Real time Transport Control Protocol (RTCP). This protocol supports five types of messages as shown in Fig. 6.20.3. The number next to each message type indicates the type of the message (200, 201....., 204 in Fig. 6.20.3).

1. Sender report :

All the active senders send the sender report periodically in a conference which tells about transmission and reception statistics for all RTP packets sent during the interval. The sender report includes an absolute time stamp, which helps the receiver to synchronize different RTP message. This is very important when both audio and video are being transmitted. Note that the relative time stamps used for audio and video transmission are different from each other.

2. Receiver report :

The receiver report informs the sender and other receivers about the quality of service. This is for passive participants, i.e. the participants which do not send, RTP packets.

3. Source description message :

Some additional information about itself like name, e-mail address, telephone number and address of the owner or controller of the source could be given by the source by periodically sending a source description message.

4. Bye message :

A stream can be shut down if a source sends a bye message. By sending the bye message the source will announce that it is leaving the conference. The other sources can as it is detect the absence of a source. But this message is considered as a direct announcement. It is also very useful to a mixer.

5. Application specific message :

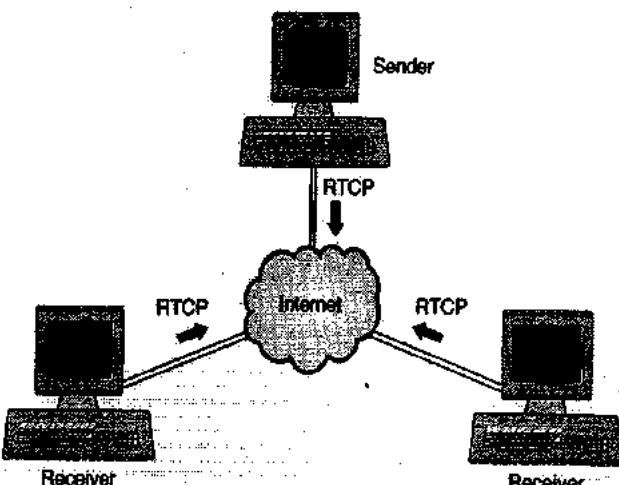
The application specific message is a packet for the application that wants to use new applications. This message is used for defining a new message type.

6. UDP port :

RTCP uses a temporary port and not a well known UDP port like RTP. The UDP port selected should have a number that immediately follows the UDP port selected for RTP i.e. it will be an odd numbered port.

6.20.3 RTCP Packets :

- Fig. 6.20.4 shows that in the multicast scenario the RTCP packets are transmitted by each participant in RTP session to all other participants using IP multicast.



(G-745) Fig. 6.20.4 : Both sender and receiver send RTCP messages

- We can distinguish between the RTP and RTCP packets by using the distinct port numbers. The RTCP port number is chosen to be equal to the RTP port number plus 1.
- The RTCP packets do not contain audio and/or video information but they contain the sender and/or receiver reports.
- They also contain the information about number of packets sent, number of packets lost and interpacket jitter.

RTCP packet types :

- For each RTP stream received by a receiver, the receiver generates a reception report. The receiver puts all its reception reports into a single RTCP packet. We have already discussed different types of RTCP packets.
- This packet is then sent to all the participants.
- The reception report is made of many fields. Some of the important ones are as follows.

Reception report fields :

- The SSRC of the RTP stream for which the reception report is being generated.
 - The fraction of packets lost within the RTP stream.
 - The last sequence number received in the stream of RTP packets.
 - The inter arrival jitter.
- For each RTP stream transmitted by the sender it creates and transmits RTCP sender report packets.
 - These packets include following information about RTP stream :
 - The SSRC of the RTP stream.
 - The time stamp and wall clock time of the most recently generated RTP packet in the stream.
 - The number of packets sent in the stream.
 - The number of bytes sent in the stream.

RTCP Bandwidth Scaling :

- RTCP has a potential scaling problem. Consider an RTP session which consists of one sender and a large number of receivers.
- If all the receivers periodically generate RTCP packets, then the total transmission rate of RTCP packets can be much higher than the rate of RTP packets sent by the sender.
- Note that the amount of RTP traffic does not change with the change in number receivers. But the amount of RTCP will increase linearly with increases in the number of services. This is known as the scaling problem.
- In order to solve this scaling problem, the RTCP modifies the rate at which a participant sends RTCP packets into the multicast tree as a function of the number of participants in the session.
- Also because each participant sends control packets to everyone else, each participant can estimate the total number of participants in the session.
- RTCP attempts to limit its traffic to 5% of the session bandwidth. That means if there is only one sender, sending at a rate of say 2 Mbps, then RTCP tries to limit its traffic to 100 kbps (5% of 2 Mbps) as follows.
- The protocol RTCP gives 75% of this rate i.e. 75 kbps to the receivers and it gives the remaining 25% of the rate i.e. 25 kbps to the senders.
- The 75 kbps is devoted to the receivers is equally shared among the receivers.
- So if there are X number of receivers, then each one of them gets $75/X$ kbps.
- A participant (sender or receiver) determines the RTCP packet transmission period by dynamically calculating the average RTCP packet size and dividing the average RTCP packet size by its allocated rate.
- The period for transmitting RTCP packets for a sender is given by,

$$T = \frac{\text{Number of senders}}{0.25 \times 0.05 \times \text{Session bandwidth}} \\ (\text{average RTCP packet size})$$

- The period for transmitting RTCP packets for a receiver is,

$$T = \frac{\text{Number of receivers}}{0.75 \times 0.05 \times \text{Session bandwidth}} \\ \times (\text{average RTCP packet size})$$

i.21 Stream Control Transmission Protocol (SCTP) :**i.21.1 Introduction :**

SCTP (Stream Control Transmission Protocol) is a protocol for transmit numerous streams of data at the

time between two terminal points that have established a connection using network.

SCTP referred as next generation TCP (Transmission Control Protocol), SCTP is planned to build it easier to hold a telephone connection over the Internet (and specifically to support the telephone system's Signaling System 7 - SS7 - on an Internet connection).

A telephone connection need that signaling information (which controls the connection) be sent with voice and other data at the same time.

SCTP also is planned to make it easier to handle connections over a wireless network and to handle the transmission of multimedia data.

SCTP is standard protocols define under RFC 2960 and was invented by the Internet Engineering Task Force (IETF).

Like TCP, SCTP handle "reliable transport" over the Internet's mostly connectionless Internet Protocol (IP), the protocol responsible for transfer the data but not for handling if all the data arrives.

Contrasting to TCP, SCTP guarantee the complete simultaneous transmission of several streams of data (in units called messages) between connected end terminals.

SCTP also supports multi homing, which means that a connected end point can have alternate IP addresses associated with it in order to route around network failure or changing conditions.

TCP transmits data in a single stream (sometimes called a bytestream) and guarantees that data will be delivered in sequence to the application or user at the end point.

If there is data loss, or a sequencing error, delivery must be delayed until lost data is retransmitted or an out-of-sequence message is received.

SCTP's multi-streaming allows data to be delivered in multiple, independent streams, so that if there is data loss in one stream, delivery will not be affected for the other streams.

For some transmissions, such as a file or record, sequence preservation is essential.

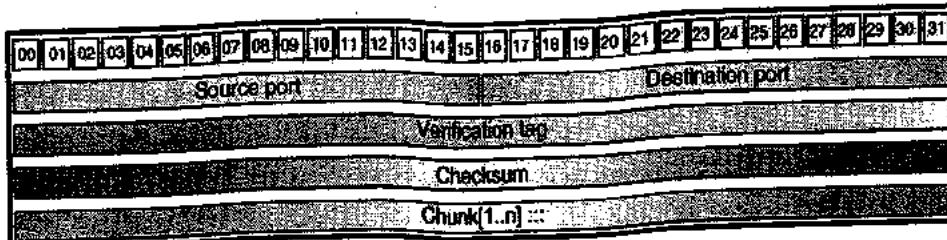
However, for some applications, it is not absolutely necessary to preserve the exact sequence of data.

For example, in signaling transmissions, sequence preservation is only essential for messages that affect the same resource (such as the same channel or call).

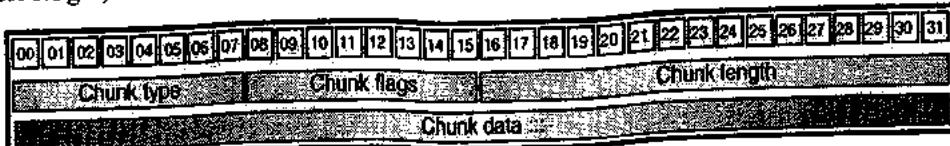
Because multi-streaming allows data in error-free streams to continue delivery when one stream has an error, the entire transmission is not delayed.

i.21.2 Stream Control Transmission Protocol Message Format :

- Stream Control Transmission Protocol is defining under RFC 2960.

SCTP header :

(G-1642) Fig. 6.21.1 : SCTP PDU structure

Chunk (Variable length) :

(G-1643) Fig. 6.21.2

- SCTP is designed to transfer PSTN signaling messages over IP networks, but is able of broader applications.
- SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers the following services to its users :
 - Acknowledged error-free non-duplicated transfer of user data.
 - Data fragmentation to conform to discovered path MTU size.
 - Sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages.
 - Optional bundling of multiple user messages into a single SCTP packet.
 - Network-level fault tolerance through supporting of multi-homing at either or both ends of an association.
- The design of SCTP includes appropriate congestion avoidance behavior and resistance to flooding and masquerade attacks.

Total size of SCTP PDU is 32 bit, explanation of each field in SCTP PDU is as follows.

Source port (16 bits) :

- The SCTP sender's port number. It can be used by the receiver in combination with the source IP address, the SCTP destination port and possibly the destination IP address to identify the association to which this packet belongs.

Destination port (16 bits) :

- The SCTP port number to which this packet is destined. The receiving host will use this port number to de-multiplex the SCTP packet to the correct receiving endpoint/application.

Verification tag (32 bits) :

- The receiver of this packet uses the Verification Tag to validate the sender of this SCTP packet. On transmit, the value of this Verification Tag MUST be set to the value of the Initiate Tag received from the peer endpoint during the association initialization, with the following exceptions :
 - A packet contain an INIT chunk MUST have a zero Verification Tag.
 - A packet containing a SHUTDOWN-COMPLETE chunk with the T-bit set MUST have the Verification Tag copied from the packet with the SHUTDOWN-ACK chunk.
 - A packet containing an ABORT chunk may have the verification tag copied from the packet which caused the ABORT to be sent.
- An INIT chunk MUST be the only chunk in the SCTP packet carrying it.

Checksum (32 bits) :

- Contains the checksum of this SCTP packet. SCTP uses the Adler-32 algorithm for calculating the checksum.

Chunk type (8 bits) 0 to 255 :

- Identifies the type of information contained in the Chunk data. The value of 255 is reserved for future use as an extension field.
- Chunk types are encoded such that the highest-order two bits specify the action that must be taken if the processing endpoint does not recognize the Chunk type.

00 - Stop processing this SCTP packet and discard it, do not process any further chunks within it.

- 01 - Stop processing this SCTP packet and discard it, do not process any further chunks within it, and report the unrecognized parameter in an 'Unrecognized Parameter Type' (in either an ERROR or in the INIT ACK).

- 10 - Skip this chunk and continue processing.
- 11 - Skip this chunk and continue processing, but report in an ERROR Chunk using the 'Unrecognized Chunk Type' cause of error.

- The total length of a chunk MUST be a multiple of 4 bytes. If the length of the chunk is not a multiple of 4 bytes, the sender MUST pad the chunk with all zero bytes and this padding is not included in the chunk length field.
- The sender should never padding with more than 3 bytes. The receiver MUST ignore the padding bytes.

6.21.3 SCTP Compared to TCP :

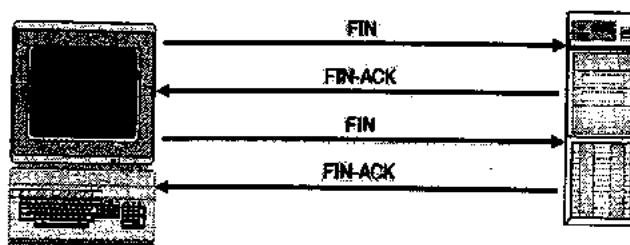
- There are various parameter we can consider on which we can compare with TCP are as follows.

1. Allow half-closed connections :

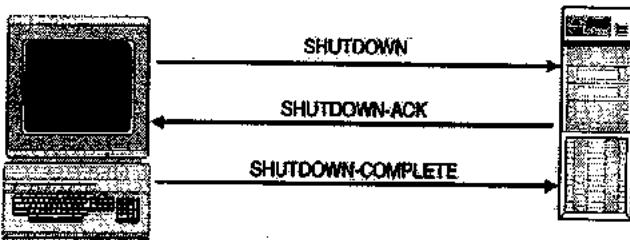
- Half-closed connections can arise when one side of the conversation consider the connection is closed, but the other consider it is still open.
- TCP uses a four-way finish command consist of bidirectional FIN and FIN-ACK messages. The half-open link could exist if the red messages are not sent.
- SCTP eliminate this option by using a three-way shutdown consists of SHUTDOWN, SHUTDOWN-ACK, and SHUTDOWN-COMPLETION.
- Once this is beginning, both sides immediately cease connections. If more information needs to be sent, then a new connection is required.

2. Preservation of message boundaries :

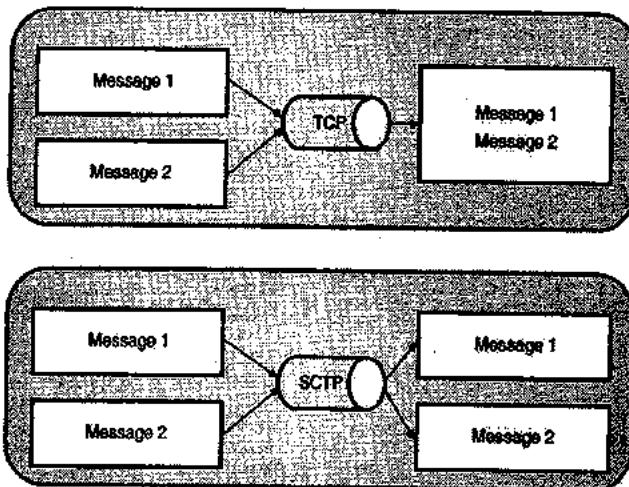
- If a client sends a 100 byte and then a 50 byte message, the data is presented to the server with hold message boundaries.
- With SCTP and UDP the messages are sent as 100 bytes and 50 bytes. With TCP the messages may be sent / received as a 150 byte message.
- In the example below, the message was acknowledged as one message. This forces the application to separate the messages back into their original format.
- With SCTP and UDP, the message's boundaries are upheld and the application does not have to split the messages.



(G-1598) Fig. 6.21.3 : TCP connection termination



(G-1599) Fig. 6.21.4 : SCTP connection close



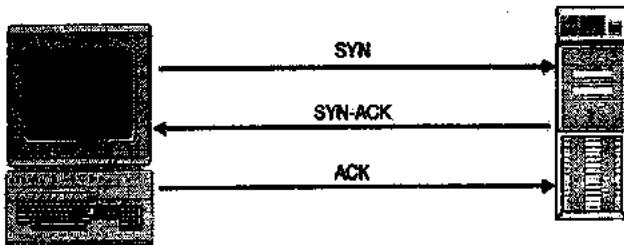
(G-1600) Fig. 6.21.5

3. Protect against SYN flooding attacks :

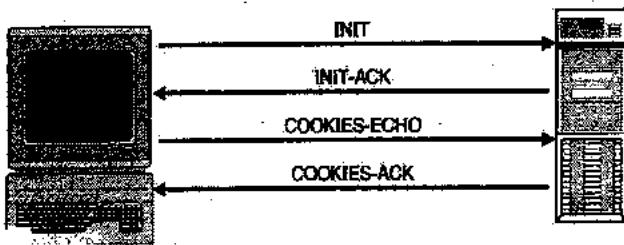
- In order to know SYN flooding attacks, a typical connection is established.
- With TCP the client start communications with a synchronize request or a SYN packet. The server act in response acknowledging with a SYN-ACK, and finally the client acknowledges the acknowledgement with an ACK packet.
- This is usually referred to as a "three-way handshake." Once all three steps are complete, communications can begin.
- By contrast SCTP uses a "four-way handshake," but may begin sending information on the third step. Then, the SCTP client initiates communications with an INIT packet.



- The server acknowledges with the INIT-ACK packet and a cookie (unique context that identifies the connection).
- The client then sends the server's cookie back to the server; the client can also send additional information after the COOKIE-ECHO.
- The server then acknowledges the COOKIE-ECHO with a COOKIE-ACK. A SYN flood attack occurs when a client or multiple clients send SYN packets to a server.
- This causes the target to commit resources and will usually overload the server, causing it to reboot or worse.
- Within TCP, the server has already committed resources for the connection. Within a TCP connection, the two endpoints must commit ephemeral ports, memory, and CPU processing for each new connection.
- For the purposes of committing resources, TCP connections begin with receiving a SYN packet. Since UDP is a connection-less protocol it does not apply. Using SCTP, the servers do not commit resources for the connection until the COOKIE-ECHO is received.
- This means that the SCTP client must initially commit resources in order to be able to send information.



(G-160) Fig. 6.21.6 : TCP connection initialization



(G-160) Fig. 6.21.7 : SCTP connection initialization

4. Selective acknowledgements :

- In standard TCP, every message, or packet of information must be accounted for, resent as necessary, and processed in the order they were sent.

- SCTP has the ability to selectively acknowledge receipt of missing, disordered, or duplicated messages.
- Due to the nature of telecommunications most applications would end up discarding any unsynchronized messages.
- Therefore, the need to send and receive the information is forgone. This would mean that a portion of a word, a portion of a video, or a piece of the whiteboard refresh would be skipped over.
- The applications and users may notice a slight skip in the voice, video, or refresh.
- This is referred to as jitter within the telecommunications world and a small amount of jitter is often preferred to having the packet resent and reprocessed which would double the amount of jitter, usually making it more noticeable to the users.

5. Unordered data delivery :

- Due to the very nature of networks not all packets may travel across the exact same path. If there is a time-delay using one path over another, the original messages could be out of order when received.
- Unordered data delivery allows for this instance and can correct the issue by reordering the messages correctly.
- Using TCP's reliable data transfer feature requires that packets be processed in order.
- If one is missing or out of order, the packet must be reordered before processing can continue.
- SCTP would process the messages in the order they arrived, not waiting for them to be numerically ordered.
- With SCTP's reliable transfer, many networked disk solutions already provide ordering service; SCTP's ability to simply pass the data on relieves the server of the unnecessary overhead of reordering.

6.21.4 Message-Based Multi-Streaming :

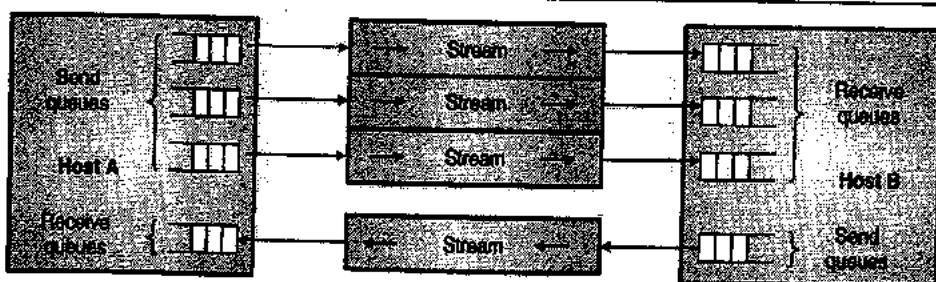
- SCTP applications submit their data to be transmitted in messages (groups of bytes) to the SCTP transport layer.
- SCTP places messages and control information into separate chunks (data chunks and control chunks), each identified by a chunk header.
- The protocol can fragment a message into a number of data chunks, but each data chunk contains data from only one user message.



- SCTP bundles the chunks into SCTP packets. The SCTP packet, which is submitted to the Internet Protocol, consists of a packet header, SCTP control chunks (when necessary), followed by SCTP data chunks (when available).
- SCTP may be characterized as message-oriented, meaning it transports a sequence of messages (each being a group of bytes), rather than transporting an unbroken stream of bytes as does TCP.
- As in UDP, in SCTP a sender sends a message in one operation, and that exact message is passed to the receiving application process in one operation.
- In contrast, TCP is a stream-oriented protocol, transporting streams of bytes reliably and in order. However TCP does not allow the receiver to know how many times the sender application called on the TCP transport passing it groups of bytes to be sent out.
- At the sender, TCP simply appends more bytes to a queue of bytes waiting to go out over the network, rather than having to keep a queue of individual separate outbound messages which must be preserved as such.
- The term multi-streaming refers to the capability of SCTP to transmit several independent streams of chunks in parallel, for example transmitting web page images together with the web page text.
- In essence, it involves bundling several connections into a single SCTP association, operating on messages (or chunks) rather than bytes.
- TCP preserves byte order in the stream by assigning a sequence number to each packet.
- SCTP, on the other hand, assigns a sequence number to each message sent in a stream. This allows independent ordering of messages in different streams.
- However, message ordering is optional in SCTP; a receiving application may choose to process messages in the order of receipt instead of the order they were sent.
- Multistreaming, illustrated in Fig. 6.21.8 is the second of the newly introduced SCTP features. Multistreaming allows the establishment of associations with multiple streams.
- Streams are uni-directional data flows within a single association.
- The number of requested streams is declared during the association setup and the streams are valid during the entire association lifetime.
- Each stream is distinguished with the Stream Identifier field included in each chunk, so that chunks from different streams can be bundled inside one SCTP PDU.
- To preserve order within a stream the Stream Sequence Number (SSN) is used. Consequently, TCP's HoL blocking problem stalling entire TCP connection is reduced to the affected SCTP stream only, as data received in order within a stream (handled by SSN) but not within the entire association (counted using TSN) can be delivered to the application.
- Among the most important applications of multistreaming are priority stream scheduling, preferential treatment, and reducing the latency of streaming multimedia in high-loss environments.
- Last but not least, multistreaming, jointly with the partially reliable extension to SCTP (PR-SCTP) can be used to support real-time applications.

Features of SCTP include :

- Multihoming support in which one or both endpoints of a connection can consist of more than one IP address, enabling transparent fail-over between redundant network paths.
- Delivery of chunks within independent streams eliminates unnecessary head-of-line blocking, as opposed to TCP byte-stream delivery.
- Path selection and monitoring select a primary data transmission path and test the connectivity of the transmission path.
- Validation and acknowledgment mechanisms protect against flooding attacks and provide notification of duplicated or missing data chunks.
- Improved error detection suitable for Ethernet jumbo frames.
- The designers of SCTP originally intended it for the transport of telephony over Internet Protocol, with the goal of duplicating some of the reliability attributes of the SS7 signaling network in IP.



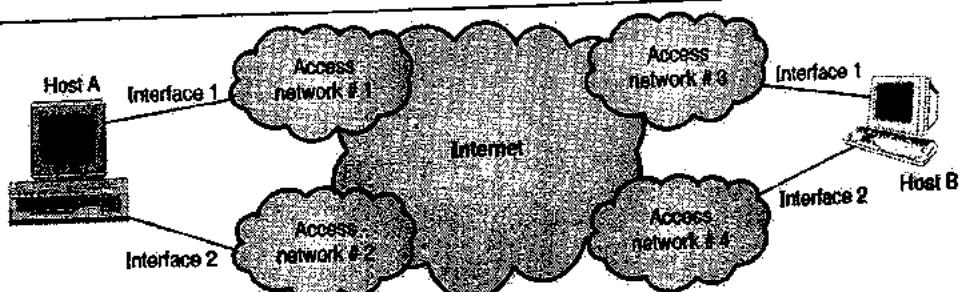
(G-1603) Fig. 6.21.8 : SCTP multistreaming

6.21.5 SCTP Multihoming :

- One of the new features provided by the standard SCTP is transport-layer multihoming. Multihoming binds multiple source-destination IP addresses for a single association between two SCTP endpoints.
- These IP addresses are exchanged and verified during the association setup, and each destination transport address is considered as a different path towards the corresponding endpoint.
- An important remark regarding the path concept in the SCTP must be made here. SCTP specification defines the path as: the route taken by the SCTP packets sent by one SCTP endpoint to a specific destination transport address of its peer SCTP endpoint.
- This definition is a consensus achieved at the early stage of the protocol specification development and was specifically not changed since then.
- The main argument in favour of the current path definition is that source based routing is not widely deployed over the Internet, so the SCTP implementation does not need to control the source address on which packets are sent to a given destination.
- One could argue that in case there are multiple local interfaces and multiple remote addresses, the number of possible paths should be simply a combination of all possible source-destination IP address pairs.
- Such an approach would be more robust in case of failures affecting both endpoints and also would provide additional benefits for load sharing applications. Nevertheless, at this stage there are several procedures that are handled as per destination address 2.
- For example, path verification, that would have to be adjusted to such a modified path definition. Also the necessary changes would have to affect congestion control as well as error counting in its current shape.
- During the association setup, one of the available paths is selected as the primary path, used for transporting all new data chunks during normal data

transmission, whereas all remaining paths, called alternate paths, serve only for retransmissions.

- Alternate paths are often referred in the literature as backup paths, especially in the robustness context of multihoming. Multihoming, in the case of IP networks, means multiple IP addresses, and typically (but not necessarily) implies multiple link-layer interfaces.
- Multihoming was originally designed for environments requiring high application availability and reliability, such as the delivery of Signaling System No. 7 (SS7) messages.
- Despite the evolution of SCTP towards a general transport protocol, this design principle has been kept.
- Consequently, the scope of use for multihoming defined within RFC 4960 is only for handling single retransmissions and performing primary path failover in case of a permanent link failure. Any other applications.
- For example, transport-layer handover or load sharing over multiple network paths, are not supported within the standard SCTP specification, and instead should be covered by dedicated protocol extensions.
- With this limitation, SCTP multihoming seems a promising protocol feature that may easily be leveraged to provide support for both mentioned applications.
- When considering the use of multihoming in transport-layer handover context, it is very important to keep in mind that standard SCTP has no mechanisms to allow dynamic changes to the set of IP addresses specified for an active association (at the association setup).
- Thus, in a mobile network scenario, if an association has already been established for a given IP address and a new PoA with a different IP address becomes available, there is no way to include it in the association and switch the primary path over to the new network connection.



(G-1604) Fig. 6.21.9 : SCTP multihommin



- Another important consideration about handover application of multihoming is that with standard SCTP only a single path is used for data transmission (i.e., the primary path) while all other available paths can handle retransmissions only.
- Then, the decision of changing the primary path relies mainly on the failover mechanism.
- The biggest challenge for load sharing application of multihoming is that simultaneous data transfer over multiple paths can provoke packet reordering at the receiver, what would deteriorate SCTP performance, since congestion control algorithms in standard SCTP are derived from TCP, and hence do not work well when reordering is common.
- Thus, to accomplish load sharing the SCTP send-buffer management and congestion control must be updated to take into account the problems of sending data over multiple paths using a single sequence-number space, and the consequences of sender-introduced reordering.
- So far, there is no commonly defined extension that facilitates load sharing for SCTP.

6.22 Quality of Service (QoS) :

SPPU : Dec. 08, May 10, Dec. 12, May 13, May 15

University Questions

- What do you mean by quality of service in network services ? Explain it with respect to reliability, delay, jitter and bandwidth. (Dec. 08, 8 Marks)
- Define quality of service and list the parameters typical to transport layer. (May 10, 8 Marks)
- Describe metrics measuring QoS (Quality of Service). (Dec. 12, 8 Marks)
- What is QoS ? Explain QoS parameters. (May 13, May 15, 8 Marks)

- The long form of QoS is Quality of Service and it is an internetworking issue. We can define quality of service in simple words as something flow seeks to attain.

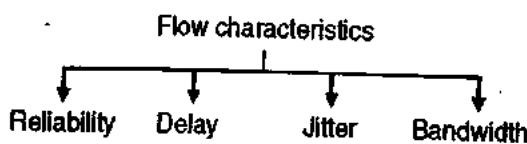
6.22.1 Flow Characteristics :

SPPU : May 13, May 15

University Questions

- What is QoS ? Explain QoS parameters. (May 13, May 15, 8 Marks)

- There are four important characteristics of data flow : reliability, delay, jitter and bandwidth.
- These characteristics are shown in Fig. 6.22.1.



(G-48) Fig. 6.22.1 : 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.

6.22.2 Techniques for Achieving Good QoS :

SPPU : May 07, Dec. 13, May 15

University Questions

- What are the techniques for achieving good quality of services in the network layer ? (May 07, 8 Marks)
- Discuss techniques used for achieving QoS (Quality of Service). (Dec. 13, 8 Marks)
- What are four general techniques to improve quality of service ? Explain any one in detail. (May 15, 8 Marks)



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. |

6.22.3 Traffic Shaping :

SPPU : Dec. 11, Dec. 13, May 16

University Questions

- Q. 1 What is traffic shaping ? How is it used in congestion control ? (Dec. 11, 5 Marks)
- Q. 2 What is traffic shaping ? Discuss any two algorithms used for traffic shaping. (Dec. 13, 8 Marks)
- Q. 3 What are four general techniques to improve quality of service ? Explain any one in detail. (May 16, 6 Marks)

- 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 :
 - Drop packets that violate the rules.
 - 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 :
 - Leaky bucket
 - Token bucket.

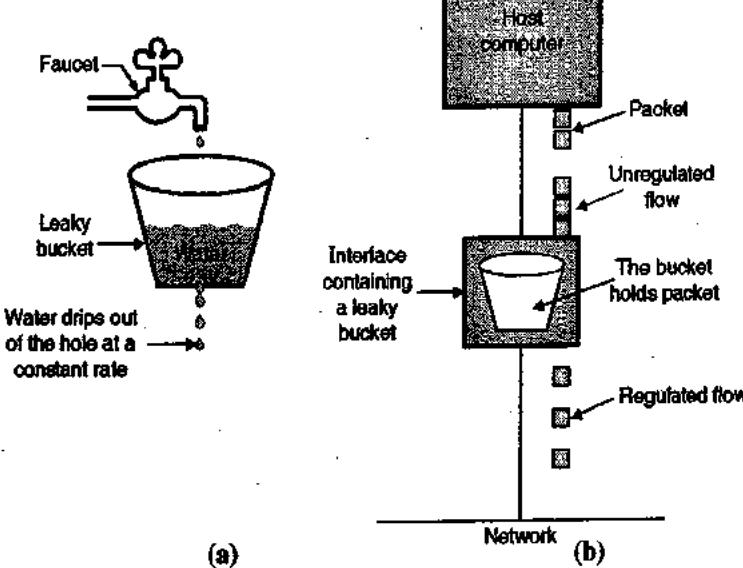
6.22.4 Leaky Bucket Algorithm :

SPPU : May 08, Dec. 11, Dec. 13, Dec. 15

University Questions

- Q. 1 What is Leaky bucket algorithm ? What are the drawbacks of this algorithm ? (May 08, 8 Marks)
- Q. 2 Explain Leaky Bucket algorithm, which quality parameter is ensured by Leaky Bucket algorithm. (Dec. 11, 5 Marks)
- Q. 3 What is traffic shaping ? Discuss any two algorithms used for traffic shaping. (Dec. 13, 8 Marks)
- Q. 4 Explain token-bucket and leaky bucket algorithm with diagram. (Dec. 15, 8 Marks)

- Leaky bucket algorithm is used to control congestion in network traffic. As the name suggests it's working is similar to a leaky bucket in real life.

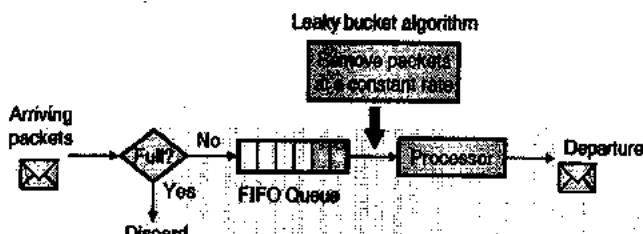


(G-48) Fig. 6.22.2 : Leaky bucket algorithm

- 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. 6.22.2 the data flow at the input of the bucket is unregulated but that at the bucket output is a regulated one.

Leaky bucket implementation :

- Fig. 6.22.3 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. 6.22.3 can be discussed under two different operating conditions, namely :
 - For packets of fixed size.
 - For packets of variable size.



(G-482) Fig. 6.22.3 : 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. 6.22.3 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 :

- Initialize a counter to a number "n" at the tick of the clock.

- If "n" is greater than the packet size, then send the packet and decrement the counter by the packet size.
- Repeat step 2 until "n" becomes smaller than the packet size.
- 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.

6.22.5 Token Bucket Algorithm :

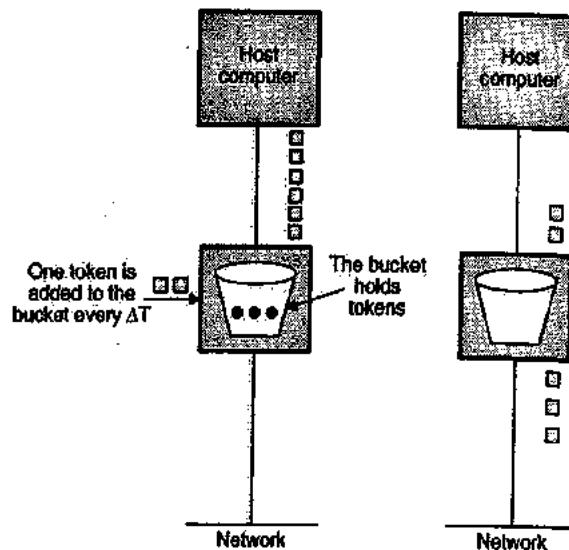
SPPU : Dec. 13, Dec. 15

University Questions

Q. 1 What is traffic shaping ? Discuss any two algorithms used for traffic shaping. (Dec. 13, 8 Marks)

Q. 2 Explain token bucket and leaky bucket algorithm with diagram. (Dec. 15, 8 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) Before

(b) After

(G-483) Fig. 6.22.4 : Token bucket algorithm

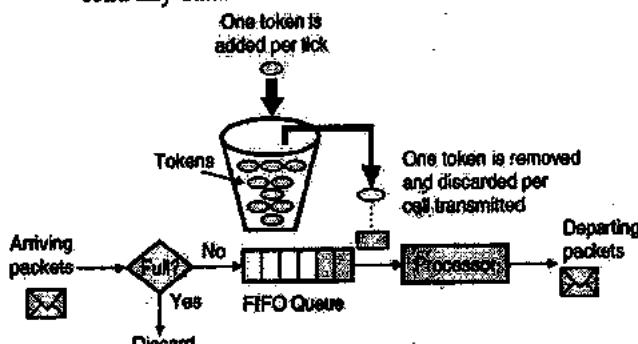
- A token generator continuously produces tokens at a rate of R tokens per second and puts them into a token bucket with a depth of D tokens as shown in Fig. 6.22.4. If the token bucket gets full then the extra tokens are discarded.
- Token bucket algorithm is a variant of leaky bucket algorithm discussed 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. 6.22.5 shows the implementation of token bucket.
- The token bucket can be easily implemented with a counter. The token is initialised 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-44) Fig. 6.22.5 : 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 ?

- Maximum bytes sent from the token bucket during a burst is

$$c + \rho \cdot s$$

- Maximum bytes the source can send during a burst is

$$m \cdot s$$

- Setting the two equal and solving for s

$$s = \frac{c}{m - \rho}$$

6.22.6 Combination of Token Bucket and Leaky Bucket :

- The token bucket and leaky bucket techniques can be combined to obtain the following advantages :
 - To credit an idle host
 - 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.

6.22.7 Resource Reservation :

SPPU : Dec. 11

University Questions
Q.1 Explain resource reservation protocol in detail (Dec. 11, 6 Marks)

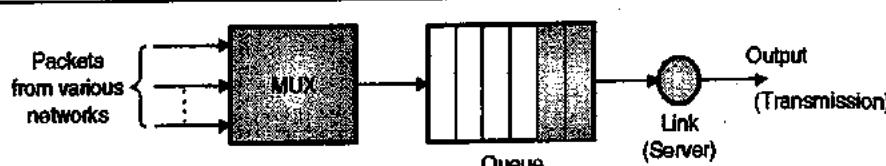
- The data flow is dependent on the following resources :
 - Buffer
 - Bandwidth and
 - CPU time
- The QoS can be improved by reserving these resources. The QoS model called integrated services operates on the principle of resource reservation, for improvement in QoS.

6.23 Scheduling and Policing :

- In this section, we will examine various mechanisms that are used to provide the QoS guarantees.
- In the following section, we will then examine how these mechanisms can be combined to provide various forms of Quality of Service in the Internet.

Scheduling mechanisms :

- The packets coming from various networks are multiplexed and then arranged in a queue for transmission at the output buffers associated with a link as shown in Fig. 6.23.1.



(G-75) Fig. 6.23.1 : Multiplexing and queuing

6.23.1 Link Scheduling Discipline :

SPPU : May 12, Dec. 12

University Questions

Q.1 Describe any link scheduling algorithm.

(May 12, Dec. 12, 8 Marks)

The manner in which the queued packets are selected for transmission on the link is called as link scheduling discipline. It plays an important role in providing QoS guarantees.

- Some of the important link scheduling disciplines are as follows :

- First in First Out (FIFO) queuing
- Priority queuing
- Round robin and Weighted Fair Queuing (WFQ).

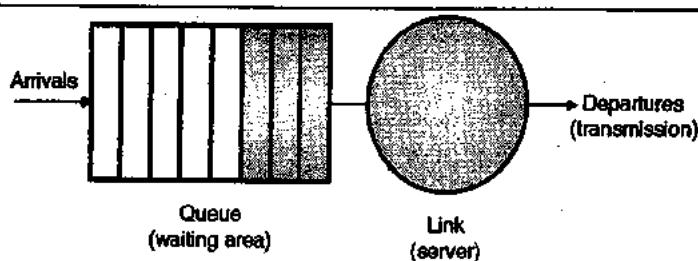
1. First in First Out (FIFO) queuing :

- Refer Fig. 6.23.2 to understand the concept of FIFO queuing.
- The incoming packets are applied to the queue and the queue output is applied to the link for transmission.

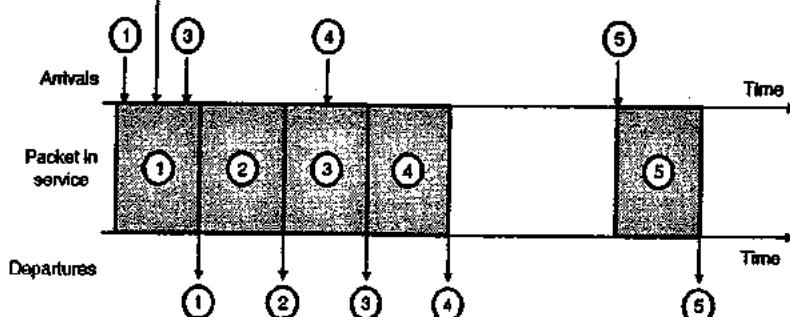
- Packets coming to the link output will wait if the link is busy in transmitting some other packet.
- If sufficient buffer space is not available to hold the incoming packet, then the packet will be either discarded or kept on the basis of packet discarding policy.
- When a packet is completely transmitted over the outgoing link, it is removed from the queue.
- FIFO stands for first-in-first-out. So packet arrived first at the input is considered first for transmission.
- This principle of operation is illustrated in Fig. 6.23.3.

2. Priority Queuing :

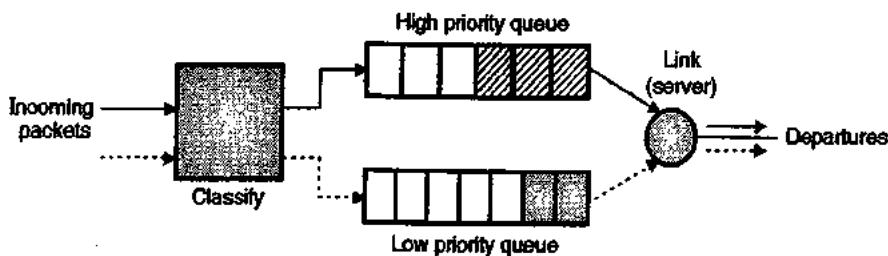
- Refer Fig. 6.23.4 for understanding the concept of priority queuing.
- Here the packets are divided into low priority and high priority categories. Two different queues are set up for these two classes as shown in Fig. 6.23.4. That means one queue is set up for the high priority packets while the other one is set up for the low priority packets.



(G-754) Fig. 6.23.2 : Principle of FIFO queuing



(G-755) Fig. 6.23.3 : Principle of FIFO queuing



(G-756) Fig. 6.23.4 : Priority queuing

- The high priority packets are always transmitted first. When the high priority queue becomes empty the transmission of the low priority packets is initiated.
- The packets in the higher priority or lower priority class are transmitted on the FIFO basis.
- In Fig. 6.23.4 only two priorities have been considered. But in general, there can be many more priorities and each one has its own queue, assigned to it.

3. Round Robin and Weighted Fair Queuing (WFQ) :

- In the round robin queuing the packets are classified into different classes, like class 1,2,3... etc.
- The round robin scheduler will transmit the packets on the round robin basis i.e. first class 1 packets are transmitted, then class 2 packets, then class 3 packets are transmitted.
- The advantage of this technique is that the link will never be kept idle. The principle of round robin queue is illustrated in Fig. 6.23.5. It is a two class round robin discipline.
- Packets 1, 2 and 4 belong to class 1 and class 2 contains the packets 3 and 5. The packets from the two classes are transmitted alternately as shown in Fig. 6.23.5.

Weighted Fair Queuing (WFQ) :

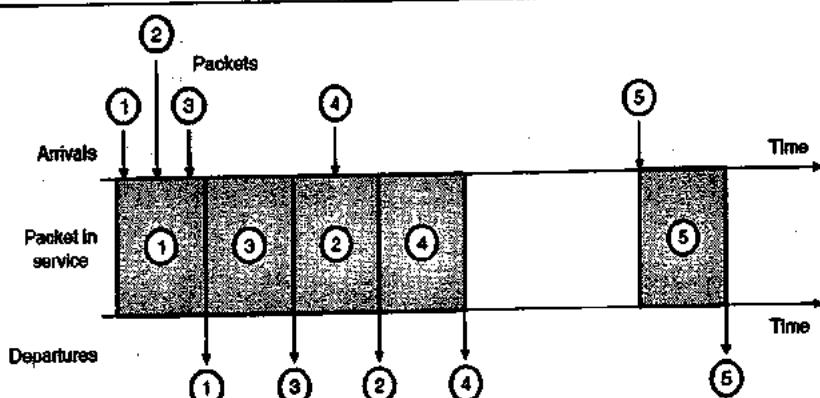
- Refer Fig. 6.23.6 to understand weighted fair queuing.
- The incoming packets are classified into different classes (1, 2, 3 etc) and stored in separate queues (W1, W2, W3 etc).
- Similar to the round robin technique the WFQ scheduler, will output the packets from W1, W2, and W3 one after the other in a circular manner. This is similar to the Time Domain Multiplexing (TDM) technique.
- If a queue is empty the WFQ scheduler will move immediately to the next queue. It will never keep the link idle.

Difference between round robin and WFQ :

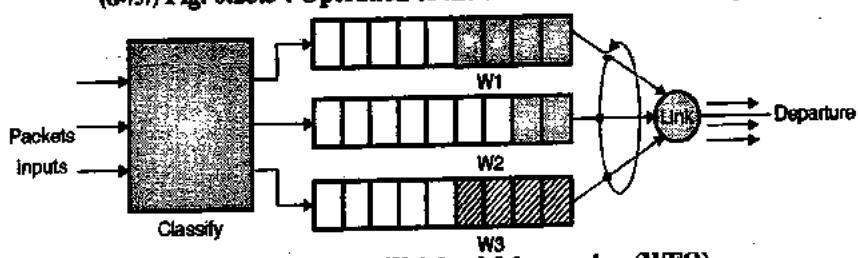
- In round robin the service received by each class is same but in WFQ, each class may receive a differential amount of service in any interval of time, depending on the weightage associated to that class.

6.24 Policing :

- As discussed in relation with QoS, the regulation of the rate at which a packet input flow is allowed into a network is one of the important parameter.
- In order to regulate this flow certain flow rate aspects should be policed. Following are the important policing criteria.
 - Average rate
 - Peak rate
 - Burst rate.



(G-757) Fig. 6.23.5 : Operation of the two-class round robin queue



(G-758) Fig. 6.23.6 : Weighted fair queuing (WFQ)



1. Average rate :

- Average rate of packet transmission is defined as the number of packets per unit time. A network may wish to limit the long term average rate.
- The most important point is over which time slot the average rate is to be policed ?

2. Peak rate :

- Not only the average rate of transmission, but also the peak packet rate is important and hence should be policed.
- Maximum allowed value of data rate, limits the maximum number of packets that can be sent over a short period of time.

3. Burst size :

- Burst is a group of packets which is sent over a network in a very short duration of time.
- A network may also wish to limit the burst rate that means the maximum number of packets which can be sent into the network over a very short duration.
- As this duration approaches zero, the burst size limits the number of packets that can be sent instantly into the network.

Characterization of policing limits :

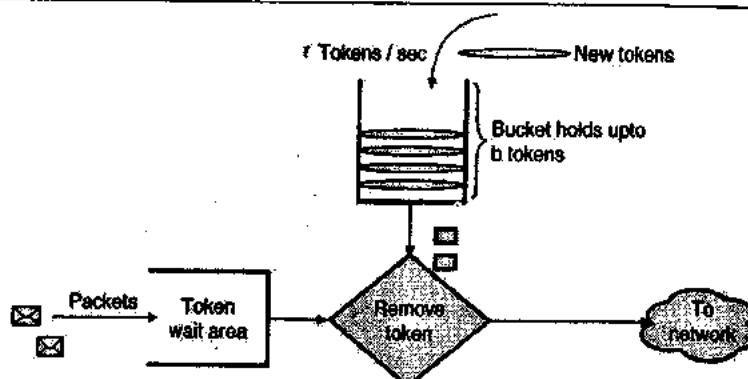
- The leaky bucket mechanism can be used for characterizing the three policing limits mentioned above. Fig. 6.24.1 shows the principle of leaky

bucket mechanism. A leaky bucket can hold up to "b" tokens.

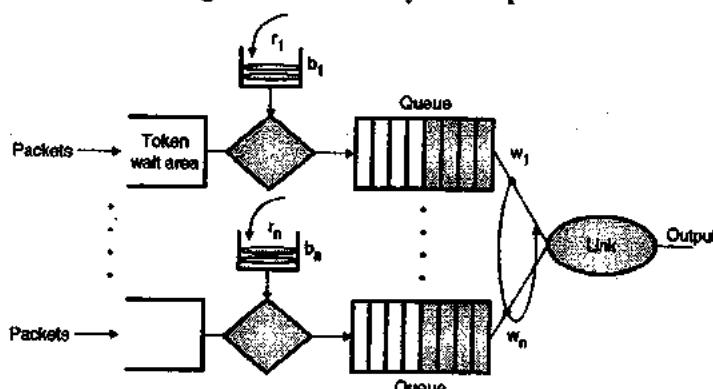
- The procedure for adding the packets is as follows :
 1. New tokens are being added to the bucket at a rate of "r" tokens per second.
 2. The bucket is capable of holding "b" tokens. If the bucket contains less than "b" tokens, when a new token is generated, then the newly generated token is added to the bucket, else the newly generated token is ignored and the bucket remains full with "b" tokens.

Use of leaky bucket for policing :

- Before a packet is transmitted into the network, it must first remove a token from the bucket.
- If the token bucket is empty, then the packet must either wait for a token or the packet may be dropped. This behaviour is useful for policing.
- As there are at the most "b" tokens in the bucket, the maximum burst size is restricted to "b" packets.
- The tokens are generated at a rate "r", hence the number of packets which can enter the network during a time interval "t" is given by, $(rt + b)$.
- So the token generation rate "r" decides the limit on the long term average packet rate.
- We can use two leaky buckets for policing the peak flow rate along with the average flow rate.



(G-759) Fig. 6.24.1 : The leaky bucket policer



(G-760) Fig. 6.24.2 : n multiplexed leaky bucket flows with WFQ scheduling

Leaky bucket + weighted fair queuing = provable maximum delay in a queue :

- Both leaky bucket policing and WFQ scheduling can play an important role in providing QoS in the Internet.
- Refer Fig. 6.24.2. Consider a router's output link which multiplexes "n" number of flows. Each flow is policed by a leaky bucket with holding capacity " b_i " and token producing rate of " r_i ", with i taking values from 1 to n .
- For a WFQ each flow " i " is guaranteed to receive a share of the common link bandwidth equal to at least.

$$R \cdot w_i / \sum w_j$$

Where R is the transmission rate of the link in packets/sec.

- Then what is the maximum delay experienced by a packet while waiting in WFQ after passing through the leaky bucket?
- As an example, consider this situation, suppose flow 1 token bucket is initially full with b_1 tokens in it. A burst of exactly b_1 packets arrives to the leaky bucket policer for flow 1.
- These packets will then remove all the tokens from the bucket and joint the WFQ waiting area for flow 1.
- These b_1 packets are served at a minimum rate of

$$R \cdot w_1 / \sum w_j \text{ packets/sec.}$$

Hence the last packet will experience a maximum delay d_{max} before it is completely transmitted. The maximum delay is given by,

$$d_{max} = \frac{b_1}{R \cdot w_1 / \sum w_j}$$

6.25 Integrated Services and Differentiated Services :

SPPU : Dec. 11, May 12

University Questions

- Q.1 Differentiate between class based and flow based QoS. Explain differentiated services for QoS. (Dec. 11, 11 Marks)
- Q.2 Describe in brief Integrated Services and Differentiated Services. (May 12, 11 Marks)

- To provide the required QoS, two architectures have been proposed. They are as follows :
 - The integrated services (Intserv)
 - The differentiated services (Diffserv).

Intserv is defined as a framework which is developed within the IETF for providing QoS guarantees to individual application sessions.

The goal of **Diffserv** is to provide the ability to handle different classes of traffic in different ways within the Internet.

6.25.1 Intserv :

SPPU : May 12

University Questions

- Q.1 Describe in brief Integrated Services and Differentiated Services. (May 12, 9 Marks)

The intserv architecture has two key features

1. Reserved resources
2. Call set up.

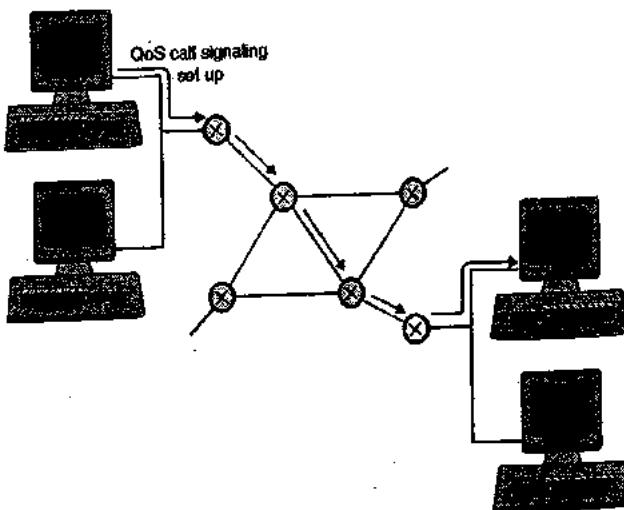
1. Reserved resources :

A router must know about how much of its resources such as buffers, link bandwidth have already reserved for the current or ongoing session.

2. Call set up :

- A session requires certain QoS guarantee. Therefore to fulfil the requirements sufficient resources at each router should be first reserved.
- The call set up is also called as call admission. Each router has to determine the local resources required by the session and also should fined the amounts of its resources that are already occupied etc.
- Refer Fig. 6.25.1 to understand the call set up procedure. The steps involved in call set up process are as follows :

1. Traffic characterization and specification of desired QoS.
2. Signaling for call set up.
3. Pre-element call admission.



(G-76) Fig. 6.25.1 : The call set up procedure



1. Traffic characterization and specification of desired QoS :

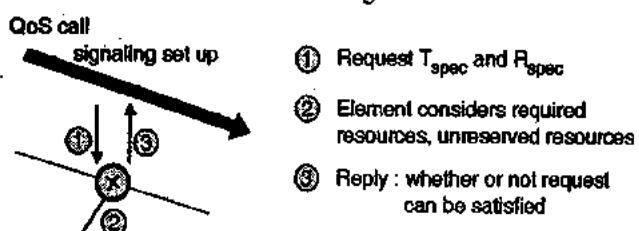
- The session has to declare its QoS requirement. Then the router can determine whether its resources are sufficient to meet these requirements or not.
- The session must also characterize the traffic that it will be sending into the network.
- In the Intserv architecture the R_{spec} (R for reservation) defines the specific QoS being requested by a connection and the T_{spec} (T for traffic) characterizes the traffic sent by the sender.
- Depending on the type of service requested the specific form of R_{spec} and T_{spec} will vary. The R_{spec} and T_{spec} are defined in part in RFC 2210 and RFC 2215.

2. Signaling for call set up :

- In order to reserve the resources for the session, a session's T_{spec} and R_{spec} should be conveyed to the router.
- The signaling protocol in the Internet is the RSVP protocol. RFC 2210 describes how to use the RSVP resource reservation protocol with the Intserv architecture.

3. Pre-element call admission :

- The router receives the T_{spec} and R_{spec} for a session. Then it can determine whether it is possible to go ahead with the call or not.
- The decision of call admission is dependent on factors like traffic specification, requested type of service, and existing resource allotment made by the router to the ongoing session.
- The pre-element call behaviour of a router has been illustrated in Fig. 6.25.2.



(G-762) Fig. 6.25.2 : Pre-element call behaviour

6.25.2 Classes of Service :

- The Intserv architecture defines two classes of services as follows :
 - Guaranteed service.
 - Controlled-load service.

1. Guaranteed quality of service :

- This type of service specifications are defined in RFC 2212. It defines limits on the queuing delays experienced by a packet when it is routed through a router.

- The traffic characterization of a source are given by a leaky bucket with parameters (r, b) and the characteristics of the requested service are given by the transmission rate R at which the packets are transmitted.
- Thus a session requesting guaranteed service is expecting that the bits in its packet be transmitted at the forwarding rate of R bits / sec.
- As the traffic is specified by leaky bucket characterization and transmission rate is R , it is possible to limit the maximum queuing delay at the router.

2. Controlled load network service :

- The RFC 2211 states that a session receiving controlled load service, will receive a QoS which is very close the QoS received from an unloaded network element.
- That means it is assumed that a very high percentage of the packets will be successfully passed through the router without getting dropped. The delay in the router experienced by these packets is assumed to be equal to zero.
- However note that the controlled load service does not make any quantitative guarantees about performance.
- The controlled load service is used for real time multimedia applications on the Internet.
- That is why the performance of these applications is load dependent. Their performance is good well when the load on the network is small, but the performance degrades with increase in load.

Problems in the Intserv model :

- Some of the problems encountered with the Intserv model and per flow reservation of resources are as follows :

- Scalability
- Flexible service model.

1. Scalability :

- For per flow resource reservation, the router needs to process resource reservations and maintain the per flow state for each flow passing through the router.
- Per flow reservation can increase the overhead in large networks to a great extent.

2. Flexible service models :

The Intserv framework provides for a small number of pre specified service classes. Class A service is preferred over class B service and so on.

Remedy :

The solution to these difficulties is to use the differentiated service (DiffServ) which provides a scalable and flexible service differentiation.

6.25.3 Differentiated Services (DiffServ) :

SPPU : May 12, May 13

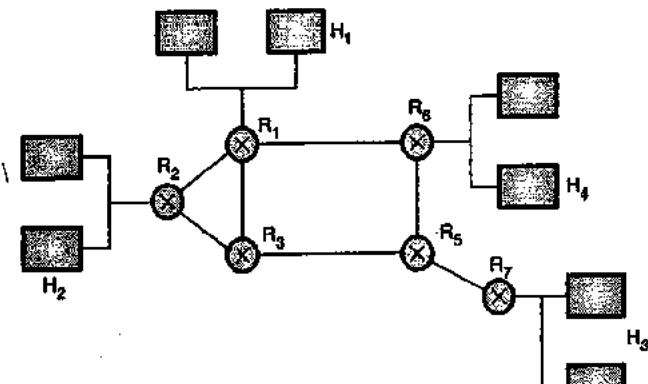
University Questions

Q.1 Describe in brief Integrated Services and Differentiated Services. (May 12, May 13; 8 Marks)

- DiffServ has the ability to handle different classes of traffic in different ways within the Internet.
- The scalability is needed because hundreds of thousands of source-destination traffic flows may be present at the router of the Internet.
- The flexibility is required because new service classes may arise and old service classes may become obsolete.
- The DiffServ architecture is flexible. It does not define specific service classes. Instead DiffServ provides the functional components.
- Functional components are pieces of the network architecture with which such services can be built.

A simple Diffserv network example :

- Refer Fig. 6.25.3 which shows a simple diffserv network. We will use this network in order to set the framework for defining the architectural components of the Diffserv model.
- The Diffserv architecture consists of two sets of functional elements namely:
 - Edge function
 - Core function.



(G-763) Fig. 6.25.3 : A simple diffserv network example

1. Edge functions : Packet classification and traffic conditioning

- At the input of the network the incoming packets are marked. The differentiated service (DS) field of the packet header is set to some value.
- For example in Fig. 6.25.3 packets which are sent from H₁ to H₃ travel through the routers R₁, R₃, R₅ and R₇ and they may be marked at R₁.
- Whereas the packets being routed from H₂ to H₃ travel through R₂, R₁ and R₆ and they may be marked at R₂.

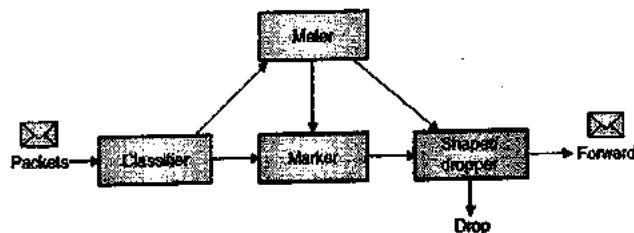
- Such type of mark received by a packet will identify the class of traffic to which it belongs. Different classes of service will then receive different service within the core network.

2. Core functions : Forwarding

- The DS marked packet arrives at the Diffserv capable router. The router understands the class of received packet.
- The per hop behaviour of the router is associated with the packet class. The router will forward the packet onto their hop according to the per hop behaviour.
- The per hop behaviour is important because it decides how a router's buffers and link bandwidth are shared among various service classes.

Diffserv traffic classification and conditioning :

- Refer Fig. 6.25.4 which provides a classification and marking function within the edge router.
- Packets arriving at the input of edge router are first applied to a classifier. The packets are classified in this block.



(G-764) Fig. 6.25.4 : Logical view of packet classification and traffic conditioning at the end

- The classifier makes the packet selection on the basis of the values of one or more packet header fields and forwards the packet to the proper marking function.
- As long as the user is sending packets into the network without violating the negotiated traffic rules, the packets get their priority marking and they are forwarded towards the destination without any penalty.
- But if the traffic rules are violated, then the out of profile packets might be marked in a different way and as a penalty they might be shaped or might be dropped.
- The metering block in Fig. 6.25.4 has a function of comparing the incoming packet flow with the negotiated traffic profile and to find out whether the packet is following the negotiated traffic profile or not.



- The actual decision making such as remark, forward, delay or drop a packet is not the Diffserv architecture's job. Instead it is done by the network administrator.

Per-hop behaviours :

- The second key component of the Diffserv architecture involves the per hop behaviour (PHB) which is performed by Diffserv capable routers.
- PHB is defined as a description of the externally observable forwarding behaviour of a diffserv node applied to a particular diffserv behaviour aggregate.

6.26 RSVP :

SPPU : May 13

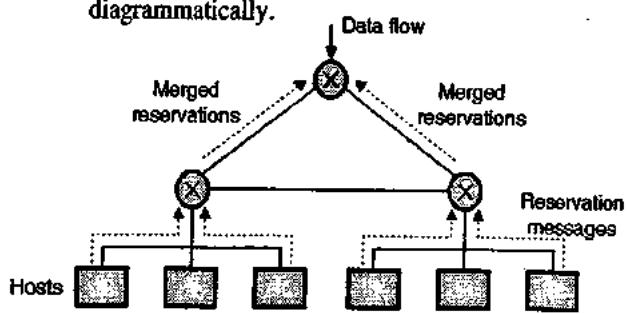
University Questions

Q.1 Explain significance and working of RSVP protocol. (May 13, 8 Marks)

- The long form of RSVP is resource ReSerVation Protocol. This protocol is a signaling protocol which allows applications running in the host computer to reserve resources in the Internet.
- The resources in the Internet are : link bandwidth and router buffers. But we will use the word resource as a synonym with bandwidth.
- RSVP is used mainly for resource (bandwidth) reservation.
- It allows the applications to reserve bandwidth for their data flows.
- RSVP is also used by the routers to forward their bandwidth reservation requests.
- So as to implement RSVP, the RSVP software has to be present in the receivers, senders and routers.

Characteristics of RSVP :

- The two important characteristics of RSVP are as follows:
 - It provides reservations for bandwidth in multicast trees.
 - RSVP is receiver oriented. i.e. the data receiver initiates and maintains the resource reservation used for that flow.
- Fig. 6.26.1 illustrates these characteristics diagrammatically.



(G-765) Fig. 6.26.1 : Characteristics of RSVP

- Fig. 6.26.1 shows a multicast tree with data flowing from the top of the tree to the hosts at the bottom of the tree.
- Note that data originates from the sender but the reservation messages originate from the receivers.
- When a router forwards a reservation message upstream toward the sender, the router may merge all the reservation messages together.

Session :

- A session can consist of many multicast data flows. Each sender in a session can transmit one or more data flows.
- Each data flow in the session has the same multicast address.
- Within a session, it is necessary to identify the data flow to which a particular packet belongs to. This can be done with the flow identifier field in IPv6.

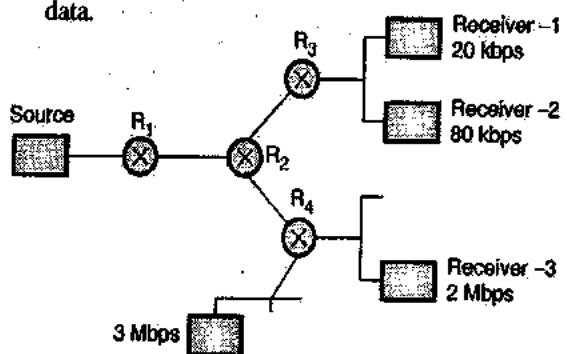
Things that RSVP cannot do :

There are certain things which cannot be done by the RSVP.

- The RSVP standard does not specify how exactly the reservation of bandwidth to the data flow is provided.
- RSVP is not a routing protocol. It depends on an underlying unicast or multicast protocol for routing.
- RSVP is called as a signaling protocol. But actually it does not perform any signaling. The meaning of signaling is that RSVP allows hosts to establish and terminate reservations for data flows.

An RSVP example :

- Refer Fig. 6.26.2 which illustrates a simple RSVP example. The source is transmitting some video information over the Internet.
- The numbers written next to the receivers indicate the data rates at which the receivers want to receive data.



(G-766) Fig. 6.26.2 : An RSVP example

Sequence of events :

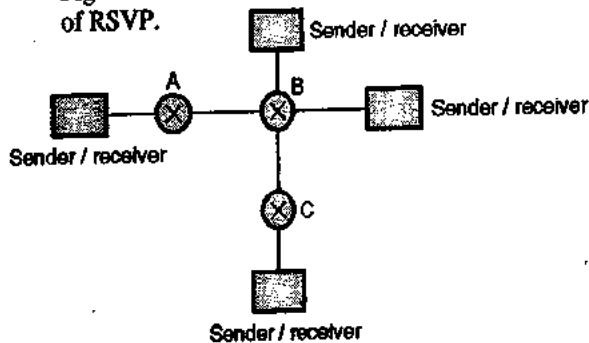
The sequence of events takes place as follows :

- The transmitting source advertises its contents by sending the RSVP path messages through the multicast tree.

- These messages indicate the bandwidth required for the contents, time out interval, upstream path to the sender etc.
- Each receiver sends an **RSVP reservation message** upstream to the sender.
- Each reservation message specifies the rate at which that receiver wants to receive data.
- When the reservation message reaches a router, it will adjust its packet scheduler for accommodating the reservation. It then sends the reservation upstream.
- The amount of bandwidth reserved upstream from the router is dependent on the bandwidths reserved downstream.

RSVP for video conferencing :

- Fig. 6.26.3 shows the video conferencing application of RSVP.



(G-75) Fig. 6.26.3 : RSVP video conference example

Call admission :

- The router should never reserve the amount of bandwidth which is higher than the bandwidth of the link.
- So whenever a router receives a new reservation message it should first find out if its downstream links can accommodate the reservation.
- This is called as an **admission test** and it is performed every time when a router receives a reservation message.
- If the admission test is unsuccessful, the router will reject the reservation and sends an error message to the appropriate receiver.

6.27 Wireless TCP and UDP :

- Theoretically the transport protocols should be independent of the technology of the underlying network layer.

- However in practice most TCP implementations have been carefully optimized on the basis of some assumptions that are true for wired networks but not true for wireless networks.
- Therefore, they work correctly for wireless network, but the performance is not optimum.

Problem :

- The main problem in application of TCP on wireless networks is the congestion control algorithm.
- As stated earlier, almost all the TCP implementations assume that time-outs take place due to congestion and not due to lost packets.
- So when a timer times-out, the TCP assumes that congestion has taken place and slows down the transmission rate of the sender. This is to reduce the load on the network and avoid congestion.
- But the wireless links are not very reliable and they always keep loosing packets.
- So if a packet is lost, then the sender should retransmit it as early as possible and should not slow down.

Conclusion :

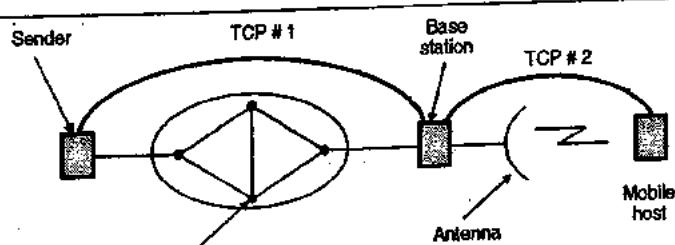
- The conclusion is when a packet is lost on the wired network, the sender should slow down. But when a packet is lost on a wireless network the sender should retransmit.
- This problem arises when the sender does not know the type of network (wired or wireless).

Practical difficulty :

- In practice, the path from sender to receiver is not homogeneous. A part of it can be over a wired network and the remaining may be wireless.
- Under such circumstances the decision about time-out becomes more difficult.

6.27.1 Solution (Indirect TCP) :

- The solution suggested for this problem is to use indirect TCP in which the TCP connection is split into two separate connections as shown in Fig. 6.27.1.



(G-67) Fig. 6.27.1 : Wireless TCP

- The first connection is between sender and base station and the second one is between base station and receiver which is a mobile host.
- The base station only copies the packets between the connections in both the directions.
- The first connection is on the wires whereas the second one is wireless.
- The problem of non-homogeneous connections has been solved. The first connection can respond to the time-outs by slowing down the sender where the second one will speed up the sender if time-outs take place.

6.27.2 Alternative Solution :

- In an alternative solution, the TCP is not split as discussed earlier but modifications are made to network layer code in the base station.
- One of the important change is that a **snooping agent is added**. It observes and caches TCP segments going out to the mobile host and the ACKs being received from it.
- The snooping agent has a timer, which is set every time a segment goes out to the mobile host. If no ACK is received before the expiry of the timer, then the snooping agent re-transmits that segment without informing the source.
- A disadvantage of this scheme is that if the wireless link is loosing too many packets, then the source may time-out waiting for ACK and will go into the congestion control mode.
- This problem will not be there with indirect TCP because there the congestion control will be exercised if and only if there is congestion in the wired part of the network.
- What if segments originating from the mobile host are lost ? The solution is when the base station observes that there is a gap in the inbound sequence numbers then, it sends a request for selective repeat.
- Thus the alternative solution proposed by Balakrishnan will ensure that the wireless link

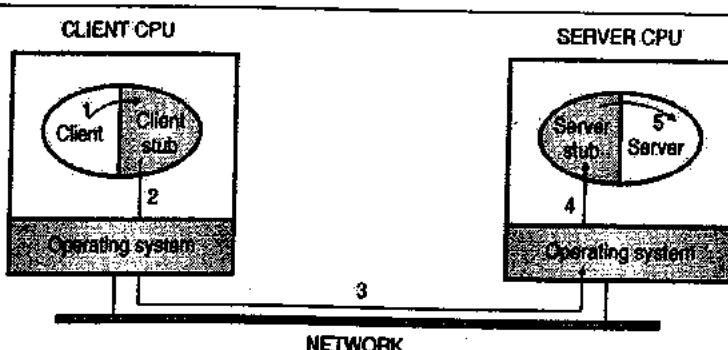
becomes more reliable in both the direction without the source even knowing about it and there is no change in the semantics of TCP.

6.27.3 Wireless UDP :

- UDP does not suffer from the same problems of TCP but wireless communication introduces some other problems in UDP.
- The main problem with UDP is that its reliability decreases to a great extent as compared to that over the wired networks.

6.27.4 RPC (Remote Procedure Call) :

- Sending message to a remote host and getting a reply is very similar to making a function call in a programming language.
- In both the cases the user starts with one or more parameters and get back a result. Due to this people have tried to arrange request reply interactions on networks in the form of procedure calls. This makes network applications very easy to program and deal with.
- For example, consider a procedure called `get-IP-address (host-name)` in which a UDP packet is sent to a DNS server and the reply is awaited. If timed out, it tries again. In this way all the details of networking can be hidden from the programmer.
- An extremely important work in this area was done by Birrell and Nelson. They suggested to allow programs to call procedures located on remote hosts.
- When a process on machine-1 calls a procedure on machine-2, then the calling process on 1 is suspended and execution of the called procedure takes place on machine-2. No message passing is visible to the programmer. This technique is called as **RPC (Remote Procedure Call)**. Traditionally the calling procedure is known as client and the called procedure is known as the server. These names are used for RPC too.
- The principle behind RPC is to make a remote procedure call look like a local call.



(G-628) Fig. 6.27.2 : Steps in making RPC

- To call a remote procedure, the client program should be bound with a small library procedure called as **client stub** which represents the server procedure in the client's address space.
- Similarly a server is bound with a procedure called as the **server stub**.
- Fig. 6.27.2 shows the actual steps in making an RPC.

- Step 1:** Client calls the client stub. This is a local procedure call and the parameters are pushed on to the stack in the normal way.
- Step 2:** Client stub encapsulates the parameters into a message and makes a system call and sends the message. Packing the parameters into a message is called as **marshaling**.
- Step 3:** The message is sent from client machine to server machine.
- Step 4:** The received packet by the server is passed to the server stub.
- Step 5:** Server stub calls the server procedure with the unmarshaled parameters.

- The reply from server to client follows the same path in the opposite direction.
- It is important to note that, the client procedure written by the user makes a normal (local) procedure call to the client stub (which has the same name as the server procedure). The client procedure and client stub are in the same address space. Therefore the parameters are passed in the normal manner. On the server side, for the server procedure nothing is new. Thus instead of I/O being done on socket, the network communication takes place by faking a normal procedure call.

Problems with RPC :

- RPC is conceptually good but has some problems. The biggest one is the use of pointer parameters. Generally passing a pointer to a procedure is not a problem. The called procedure can use the pointer in the same way the caller procedure uses it, because both the procedures have the same virtual address space. But with RPC it is not possible to pass pointers because client and server are in different address space.
- It is however possible to use tricks to pass pointers. But even this can not pass all the pointers. (pointers pointing to a graph or other complex data structure). Hence some restrictions should be placed on parameters in case of RPC.
- The second problem is that in the languages such as C, we can write a procedure to compute the inner product of two vectors (arrays) even though the size

of vectors is not specified. Each vector could be terminated by a special value which is known only to the calling and called procedures. Under these circumstances, it becomes impossible for the client stub to pack those parameters, the size of which is not known.

- The third problem is that it is not always possible to find out the types of the parameters, not even from a formal specification or code itself. For example `printf`, it can have any number of parameters of different types. Trying to call `printf` as a remote procedure would not be practically possible.
- The fourth disadvantage is related to the use of global variables. Generally the calling and called procedures can communicate by using global variables in addition to using parameters. But if the called procedure is present on a remote machine, then the code will fail because the global variables are not being shared anymore.
- All these problems put some limitations on the use of RPC.
- It is not compulsory that we use UDP packets for RPC but UDP is very well suited for RPC.
- But sometimes a TCP connection is required to be set up rather than using UDP.

6.28 Solved Examples :

Ex. 6.28.1 : An ATM network uses a token bucket scheme for traffic shaping. A new token is put into bucket every $5 \mu\text{s}$. What is the maximum sustainable net data rate (excluding the header bits) ?

Soln. :

Given : Net token is put every $5 \mu\text{s}$.

To find : Maximum output data rate m.

$$\text{The token arrival rate } \rho = \frac{1}{5\mu\text{s}} = \frac{1}{5 \times 10^{-6}} = 200 \text{ kbps.}$$

The maximum output rate can be obtained from the following expression.

$$C = S(m - \rho)$$

Where C = Bucket capacity

$$M = \text{Maximum output rate}$$

$$\rho = \text{Token arrival rate}$$

$$S = \text{Time for which the maximum output is obtained}$$

$$\therefore m = \frac{C}{S} + \rho$$

Assume C = 1 Mbps and S = 20 msec to get

$$m = \frac{1 \times 10^6}{20 \times 10^{-3}} + (200 \times 10^3)$$

$$\therefore m = 50.2 \text{ Mbps}$$

...Ans.



Ex. 6.28.2 : A computer on a 6 Mbps network is regulated by token bucket. Token bucket filled at a rate of 1 Mbps. It is initially filled to a capacity with 8 megabits. How long can computer transmit at the full 6 Mbps?

May 06, Dec. 09, 8 Marks

Soln. :

Given : C = Bucket capacity = 8 M bits

m = Maximum output rate = 6 Mbps

p = Token arrival rate = 1 Mbps

To find : S = Time for which maximum output is obtained.

$$S = \frac{C}{m-p}$$

$$\therefore S = \frac{8 \text{ M bits}}{6 \text{ Mbps} - 1 \text{ Mbps}}$$

$$= \frac{8}{5} = 1.6 \text{ sec}$$

- So the computer can transmit at the full 6 Mbps for 1.6 seconds.

Ex. 6.28.3 : Explain UDP header. The following is a dump of a UDP header in hexadecimal format: 06 32 00 0D 00 1C E2 17

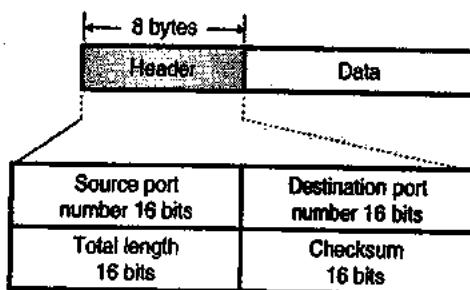
1. What is source port number?
2. What is destination port number?
3. What is the total length of the user datagram?
4. What is the length of the data?
5. Is the packet directed from a client to a server or vice versa?
6. What is the client process?

May 16, 8 Marks

Soln. :

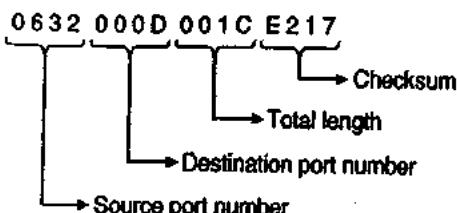
Refer section 6.8.3 for UDP header.

Fig. P. 6.28.3 shows the UDP header.



(G-624) Fig. P. 6.28.3 : UDP header

The given UDP header is as follows :



(G-1915)

1. Source port number = $(06\ 32)_H$
= 434 ...Ans.
2. Destination port number = $(0D\ 00)_H$
= 832 ...Ans.
3. Total length (header + data) = $(00\ 1E)_H$
= 30 bytes ...Ans.
4. Length of data = 30 - 8 (header)
= 22 bytes ...Ans.

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 out 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 ?

000



Application Layer

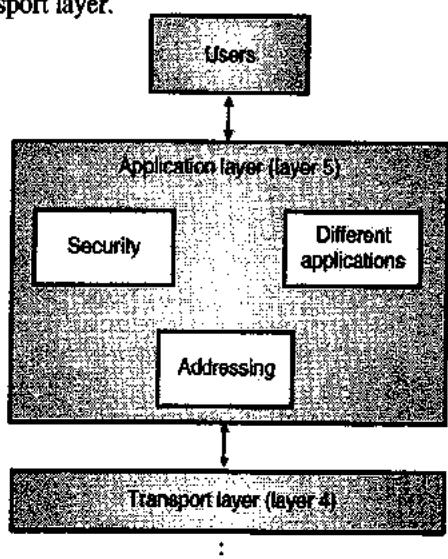
Unit VI

Syllabus :

Domain Name System (DNS), Hyper Text Transfer Protocol (HTTP), Email: SMTP, MIME, POP3, Webmail, FTP, TELNET, Dynamic Host Control Protocol (DHCP), Simple Network Management Protocol (SNMP).

7.1 Application Layer :

- The application layer is the topmost (fifth layer) of the Internet model. This is layer where all the interesting applications are found.
- People can use the Internet due to the presence of application layer.
- The layers below the application layer provide reliable transport but they do not do any real work for the users. In other words, the other four layers are created so that people can use the various application programs.
- Fig. 7.1.1 shows the position of application layer in the 5-layer Internet model.
- The application layer provides services to the users. The users can be humans or software. It enables the user to access the network.
- The application layer receives services from the transport layer.



(G-62) Fig. 7.1.1 : Position of application layer

- For the real applications in the application layer to function, there is a need of support protocols.
- The three areas or protocols required for such support are :

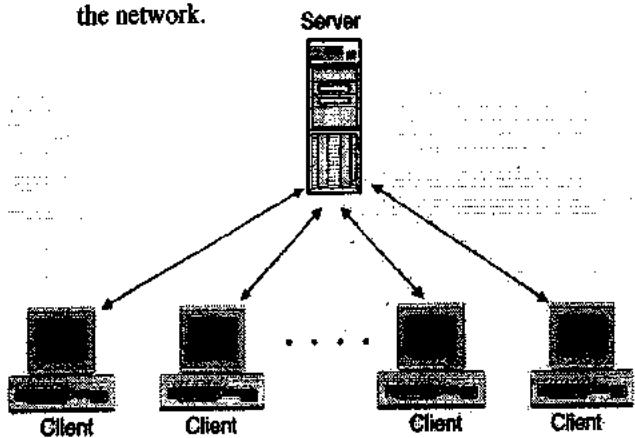
1. Network security.
 2. Domain Name Service (DNS)
 3. Network management
- Security is not a single protocol but it contains a large number of concepts and protocols used for providing privacy.
 - DNS is used to handle naming or addressing within the Internet. The third support protocol is network management.

7.1.1 Client Server Model :

- In computer networking the computers connected to the Internet are known as the **end systems**.
- The examples of end systems are as follows :
 1. Desktop computers
 2. PCs
 3. Workstations
 4. Household applications
 5. Web TVs and set top boxes
 6. Digital cameras etc.
- The end systems are also known as **hosts** because they run application programs such as Web browser program, or a Web server program etc.
- Hosts can be of two different categories as follows :
 1. Client
 2. Server
- In client-server network relationships, some computers act as server and other act as clients. A **server** is a computer, that makes the network resources available to other computers when they request it. It also provides some services to them. A **client** is the computer running a program that requests the service from a server.
- Local Area Networking (LAN) uses the client-server network relationship for its operation. You can construct a client server network by using one or more powerful computers as a servers and the remaining computers as clients. Client-server network typically uses a directory service to store information about the network and its users.



- All available network resources such as files, directories, applications and shared devices, are centrally managed and hosted by the server and then are accessed by client in a client-server network.
- Fig. 7.1.2 shows client-server network relationship. The server provides security and administration of the network.



(G-41) Fig. 7.1.2 : Client server network relationship

- In client-server networks the processing tasks are divided between clients and servers. Clients request services such as file storage and printing and servers deliver them.

Client :

The individual workstations in the network are called as the clients. A client can also be a mobile PC, PDA and so on.

Server :

The central computer which is more powerful than the clients and which allows the clients to access its software and database is called as the server.

- Server computers typically are more powerful than client computers or are optimised to function as servers.
- No user can access the resources of the servers until he has been authenticated (permitted) by the server to do so.

Communication in client-server configuration :

- Fig. 7.1.3 explains the principle of communication in the client server configuration.
- The client places a request on the server machine when he wants an access to the centralised resources.



(G-42) Fig. 7.1.3 : Client/server communication

- The server responds to this request and sends the signal accordingly to the client as shown in Fig. 7.1.3.
- The software run at the client computer is called as client program. This software configures that particular computer to act as a client.

- Similarly the software run on the server computer is called as server program. It configures that particular computer to act as a server.

Advantages of client-server network :

The advantages of client-server network are as follows :

1. The network is secure :

In client-server network's high security is because of several things.

- Shared resources are located in a centralized area and they are administered centrally.
- The servers are physically placed in secure location such as lockable separate server room.
- The operating system runs on client-server are designed to provide better security to network.
- Better security to network due to good administration.

2. Better performance :

The dedicated server computers are more expensive than standard computer workstations, but they also offer considerably better performance.

3. Centralized backup :

Backing up company's important data is much easier when it is located on a centralized server. Centralized backup is much faster too.

4. Higher reliability :

In client server network centralized dedicated server provide more reliability. It has built-in redundancy.

- Central file storage, which allows all users to work from the same of data.
- Reduces cost because of sharing of hardware and software.
- It can have dedicated servers which increase the speed of sharing resources.
- Single password allows access to all shared resources.
- Central organisation which keeps data from getting lost among computers and easy manageability of large number of users.
- The individual users don't have to manage or share resources.

Disadvantages of client-server networks :

- Professional administration is required :** Client-server networks usually need professional administration. You can hire a network administrator or you can use a company which provides professional network administration services.
- We have to use a high speed server computer with lots of memory and disk space.
- It requires a special network operating system and a number of client license.
- Expensive dedicated hardware needs to be used.

Applications of client-server configuration :

Some of the important applications are as follows :

- E-mail clients.
- Web browsers.
- FTP (file transfer) clients.

7.1.2 Addressing :

- For communication between client and server, addressing is required. When a client requests a service from the server it has to include the servers address as destination address and its own address as source address.
- When the server responds, it reverses the addresses.
- DNS is used for addressing.

7.1.3 Applications :

- Some of the important applications are :
 - Electronic mail.
 - USENET (net news).
 - World Wide Web.
 - Multimedia.
 - Remote file transfer and access.
- The most common service provided is SMTP or electronic mail. It allows the user to send a message to another user in the Internet.
- Another common service is file transfer. A user can transfer a file from its computer to the server or transfer a file from a server to its computer. This application is called FTP.
- To use the World Wide Web (WWW) we require a simple transfer protocol called HTTP.
- Multimedia allows audio and video data to be attached with the computer for the Internet users. The Internet users can listen to radio or TV or music that is streamed from a server. It is possible to talk to each other or create a teleconferencing environment.

7.1.4 Socket :

- In most applications there exists a pair of communicating processes. They send messages to each other. These messages must travel the underlying network.
- The sending process sends messages into the network through its socket and receiving process

receives messages from the network through its socket as shown in Fig. 7.1.4.

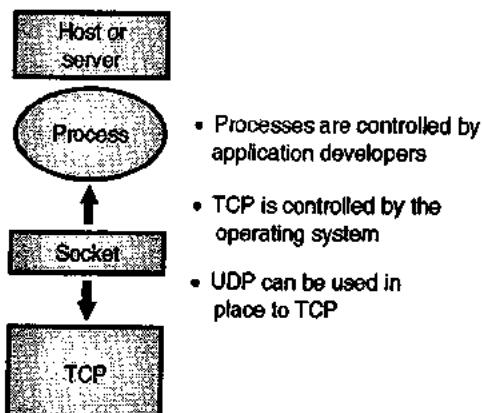
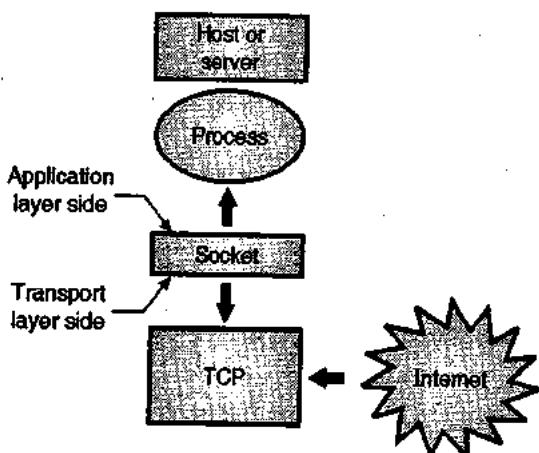
- Thus socket is defined as an interface between the application layer and the transport layer within a host.
- It is also called as the Application Programming Interface (API) between the application and the network.
- In Fig. 7.1.4 we have assumed that the transport protocol being used is TCP. But note that UDP can also be used.

7.2 Domain Name System (DNS) :

SPPU : Dec. 06, May 08, Dec. 09, May 11, Dec. 11, May 12, May 13, Dec. 13, Dec. 15, Feb. 16

University Questions

- Q. 1** Write a short notes on DNS. (Dec. 06, Dec. 09, 6 Marks)
- Q. 2** What is DNS ? Explain in detail. (May 08, 6 Marks)
- Q. 3** What is domain name system ? Explain how a resolver looks up a remote name with suitable example. (May 11, 7 Marks)
- Q. 4** What is DNS ? Explain its various resources records with one example. (Dec. 11, 8 Marks)
- Q. 5** State which transport layer protocol is used by the following protocols-HTTP, FTP, DHCP, DNS, ICMP, TFTP, IP, SMTP. (Dec. 11, 4 Marks)
- Q. 6** Comment on the importance of DNS. Explain with suitable example how query resolving process is done ? (May 12, 8 Marks)
- Q. 7** What is DNS ? Explain with suitable example how query resolving process is done ? (May 13, 8 Marks)
- Q. 8** What is DNS ? Explain in brief hierarchical structure of DNS. (Dec. 13, 8 Marks, Dec. 15, 6 Marks)
- Q. 9** What is DNS ? Explain its working with the example. (Feb. 16, 5 Marks)



(G-630) Fig. 7.1.4 : Socket

Addressing :

- For communication to take place successfully, the sender and receiver both should have addresses and they should be known to each other.
- The addressing in application program is different from that in the other layers. Each program will have its own address format. For example an e-mail address is like sachinshaha@vsnl.net where as the address to access a web page is like <http://www.google.com/>
- It is important to note that there is an alias name for the address of remote host. The application program uses an alias name instead of an IP address.
- This type of address is very convenient for the human beings to remember and use. But it is not suitable for the IP protocol.
- So the alias address has to be mapped to the IP address. For this an application program needs service of another entity.
- This entity is an application program called DNS. Note that DNS is not used directly by the user. It is used by another application programs for carrying out the mapping.

7.2.1 How does DNS Work ?

SPPU : May 06, May 11, Feb. 16

University Questions

- Q. 1** How the resolver looks up a remote names in DNS? (May 06, 9 Marks)
- Q. 2** What is domain name system? Explain how a resolver looks up a remote name with suitable example. (May 11, 7 Marks)
- Q. 3** What is DNS? Explain its working with the example. (Feb. 16, 5 Marks)

- To map a name onto an IP address, an application program calls a library procedure called the resolver. The name is passed on to the resolver as a parameter.
- The resolver sends a UDP packet to a local DNS server which looks up the name and returns the corresponding IP address to the resolver.
- The resolver then sends this address to the caller. Then the program can establish a TCP connection with the destination or sends in the UDP packets.

7.2.2 Name Space :

- The names assigned to machines should be selected carefully from the name space. There should be a complete control over the relation between the names and the IP addresses.
- The names and corresponding addresses are uniquely defined. A name space maps each address to a unique name. It can be arranged in two different ways :
 - Flat name space.
 - Hierarchical name space.

7.2.3 Flat Name Space :

- In a flat name space, a name is assigned to every address. This type of name is simply the sequence of characters. That means it does not have any structure.
- The flat name space is not suitable for large systems like Internet, because there can be ambiguity and /or duplication.

7.2.4 Hierarchical Name Space :

SPPU : Dec. 13, Dec. 15

University Questions

- Q. 1** What is DNS? Explain in brief hierarchical structure of DNS. (Dec. 13, 8 Marks; Dec. 15, 6 Marks)

- In the hierarchical name space, each name is made of many parts. The first part may correspond to the name of an institution, the second part may define the department and so on.
- The part that defines the nature of institution and name of institution is assigned by a central authority. The responsibility of deciding the rest of the name can be given to that institute itself.
- That institute can add suffix or prefix to the name for defining its host or resources.

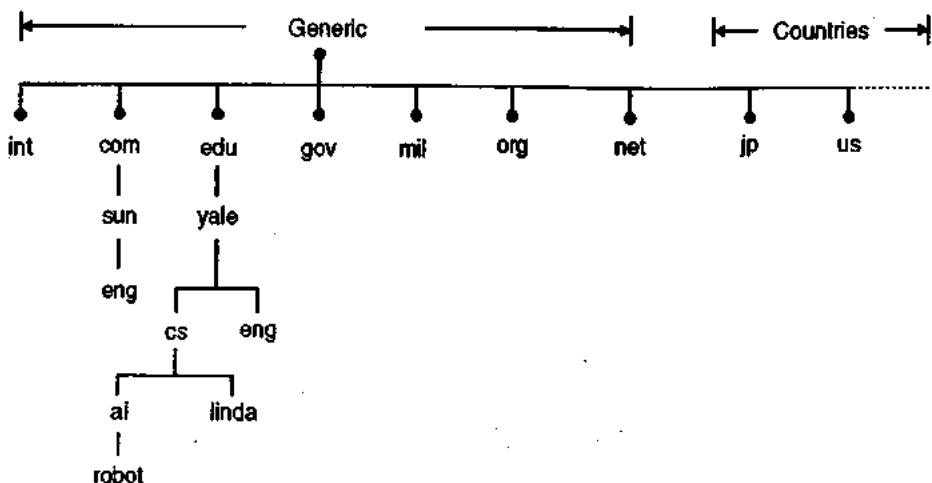
7.3 Domain Name Space :

SPPU : Dec. 12, Dec. 13, Dec. 15

University Questions

- Q. 1** What is DNS? Explain with suitable example process of delivering of requested web page on your computer? (Dec. 12, 8 Marks)
- Q. 2** What is DNS? Explain in brief hierarchical structure of DNS. (Dec. 13, 8 Marks; Dec. 15, 6 Marks)

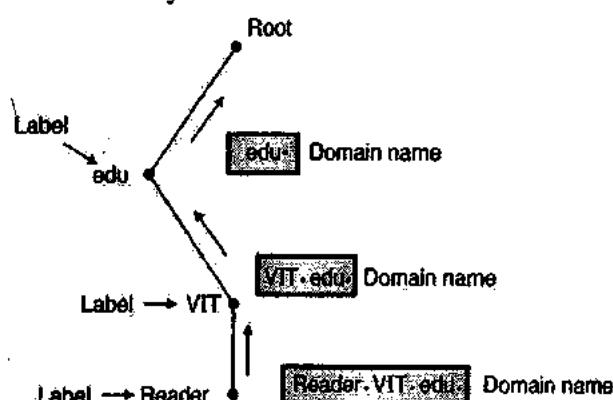
- Conceptually the Internet has been divided into hundreds of top level domains. Each domain covers many hosts.
- Each domain is divided into several subdomains and they are further partitioned and so on.
- These domains can be represented by a tree as shown in Fig. 7.3.1.
- The top level domains are of two types namely generic and countries.



(G-631) Fig. 7.3.1 : A portion of Internet domain name space

Generic domains :

- The generic domains are com (commercial), edu (educational institutions), gov (government), int (some international organizations), mil (military), net (network providers) and org (nonprofit organizations).
- The country domains include one entry for every country.
- Each domain is named by following an upward path. The components are separated by dots e.g. eng.sun.com. This is called hierarchical naming.
- Another example of hierarchical naming is shown in Fig. 7.3.2. The upward followed path has been shown by an arrow.



(G-632) Fig. 7.3.2 : Domain names, labels and hierarchical naming

Label :

- Each node in the tree has a label (or component) and it can be specified using upto 63 characters.
- If we had to remember the IP addresses of all of the Web sites we visit every day, we would all go nuts. Human beings just are not that good at remembering strings of numbers. We are good at remembering words, however, and that is where domain names come in. You probably have hundreds of domain names stored in your head. For example :

- www.yahoo.com - the world's best-known name
- www.mit.edu - a popular EDU name
- encarta.msn.com - a Web server that does not start with www
- www.bbc.co.uk - a name using four parts rather than three
- ftp.microsoft.com - an FTP server rather than a Web server

The COM, EDU and UK portions of these domain names are called the **top-level domain** or **first-level domain**. There are several hundred top-level domain names, including COM, EDU, GOV, MIL, NET, ORG and INT, as well as unique **two-letter combinations for every country**.

Within every top-level domain there is a huge list of **second-level domains**. For example, in the COM first-level domain, you have got :

- yahoo
- msn
- microsoft
- plus millions of others.

Every name in the COM top-level domain must be **unique**, but there can be duplication across domains. For example, msn.com and msn.org are completely different machines.

In the case of bbc.co.uk, it is a third-level domain. Up to 127 levels are possible, although more than four is rare.

The left-most word, such as **www** or **encarta**, is the **host name**. It specifies the name of a specific machine (with a specific IP address) in a domain. A given domain can potentially contain millions of host names as long as they are all unique within that domain.

Absolute and relative domain names :

- Domain names can be of two types : absolute or relative.
- An absolute domain name always ends with a dot (or period as it was called). For example eng. sun. com.
- But the relative domain does not end with a dot.

Are domain names case sensitive ?

No they are not case sensitive. So com and COM means the same thing.

How many characters ?

- Component names can have upto 63 characters and the full path name can at the most have 255 characters.
- Each domain controls how it allocates the domain under it. To create a new domain we have to take a permission of the domain in which it is to be included.

Domain :

- A domain can be defined as a subtree of the DNS name space as shown in Fig. 7.3.3. The name of the domain is the domain name of the node at the top of the subtree as shown in Fig. 7.3.3. e.g. com or edu.
- A domain can be divided into subdomains as shown in Fig. 7.3.3.
- Note that the naming follows organizational boundaries, not physical networks. That means even if two different departments are located in the same building, they can have distinct domains. But the computers belonging to the same department kept in two different buildings will not have different domains.

7.4 Distribution of Name Space :

- The information contained in the domain name should be stored. But this is a huge information and if we store it on one computer then the system would be highly inefficient and unreliable.
- It will be an inefficient system because the system will be heavily loaded by the requests coming from all over the world.
- It will be unreliable because failure of one computer will make the data inaccessible. If we make a distributed name space then all these problems can be overcome.

7.4.1 Hierarchy of Name Servers :

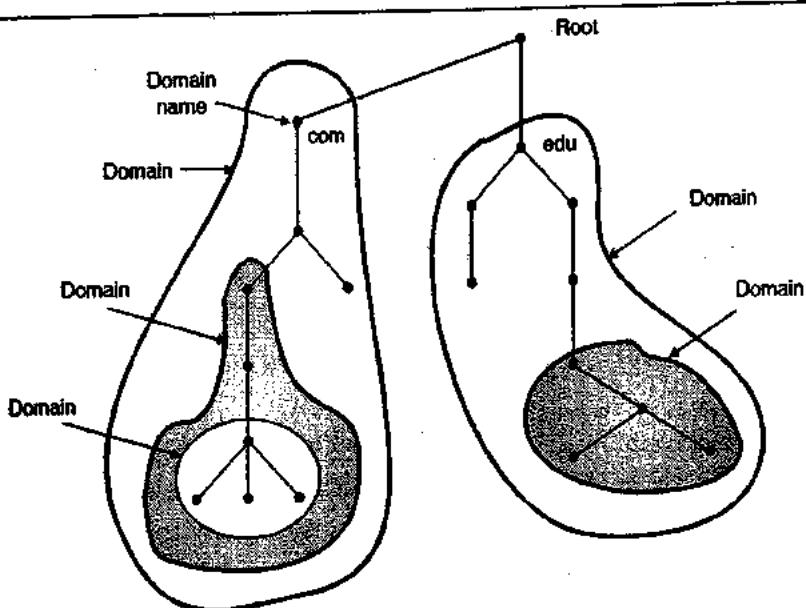
SPPU : May 09, Dec. 13

University Questions

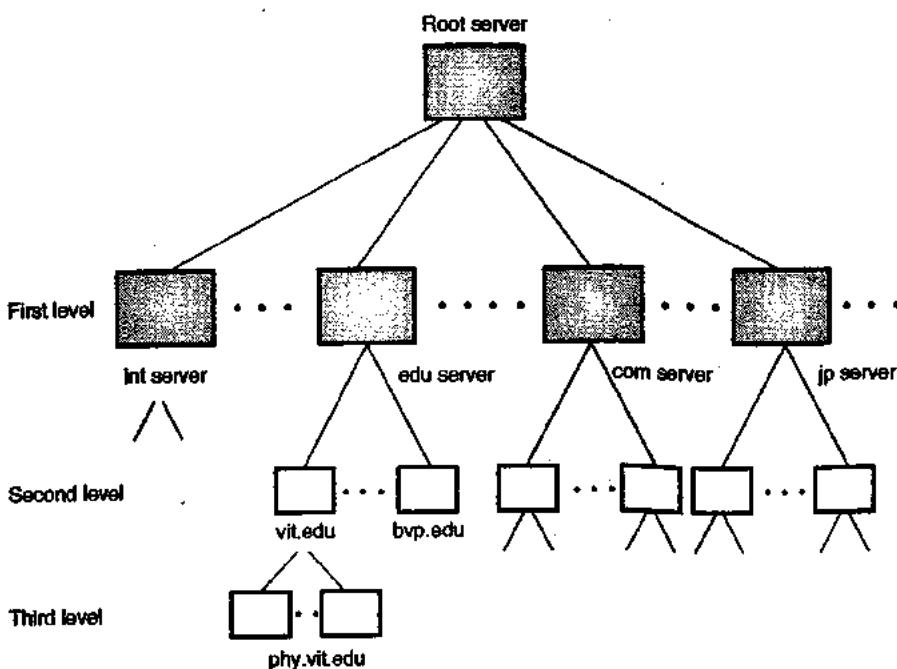
Q. 1 What is name server ? How does caching increase the efficiency of name resolution ?
 (May 09, 6 Marks)

Q. 2 What is DNS ? Explain in brief hierarchical structure of DNS.
 (Dec. 13, 8 Marks)

- Name server contains the DNS database i.e. the various names and their corresponding IP addresses.
- Theoretically a single name server could contain the entire DNS database. But practically to store such a huge information at one place is inefficient and unreliable.
- Such a server will be soon overloaded and be useless and worst thing is if it ever goes down the entire Internet will go down.
- The solution to this problem is to distribute the information among many computers called DNS servers.



(G-63)Fig. 7.3.3 : Domains

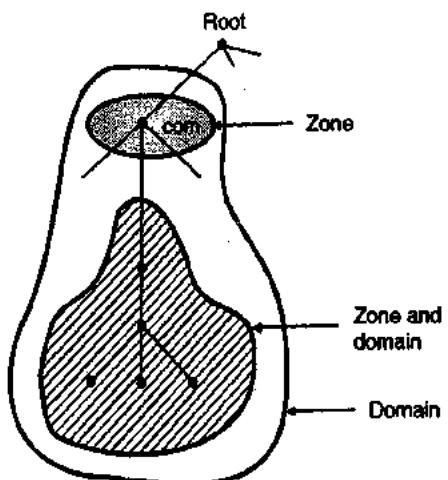


(G-634)Fig. 7.4.1 : Hierarchy of name servers

- Then we have to use a hierarchy of the Name servers as shown in Fig. 7.4.1.
- First the whole space is divided into many first level domains. The root server stands alone and can create as many first level domains as required.
- The first level domains are further divided into smaller subdomains called second level domains. They can be further divided as shown in Fig. 7.4.1.
- Each server can be responsible (authoritative) to either a large or small domain.
- Note that the hierarchy of servers is similar to the hierarchy of names.
- The whole DNS name space is divided up into non overlapping zones. The concept of zones is as explained below.

Zones :

- With a number of DNS servers being used instead of a single one, we have to define the area over which each server has an authority.
- What a server is responsible for or has authority over is called as a zone.
- If a server is appointed for a domain and the domain is not further divided into subdomains then the domain and zone will be the same as shown in Fig. 7.4.2.
- The server makes a database called a zone file. It keeps all information about every node under that zone.
- But if a server divides its domains into subdomains and delegates a part of its authority to other servers then domain and zone will be different from each other. This is shown in Fig. 7.4.2.



(G-635)Fig. 7.4.2 : Domains and zones

- The information about the nodes that belong to the subdomains is stored in the servers at the lower levels. The higher level and original server keeps some sort of reference of these lower level servers.

Root server :

- A root server is defined as a server whose zone consists of the whole DNS tree. It does not store any information about domains but delegates the authority to other servers. It only keeps the reference of these servers.
- There are more than 13 root servers and they are distributed all around the world.

Primary and secondary servers :

DNS defines two types of servers namely the primary servers and the secondary servers.

Primary server :

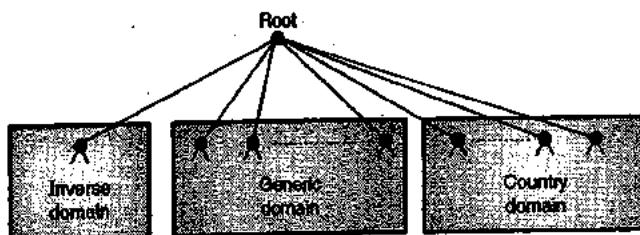
It is a server which stores a file about its zone. It is authorised to create, maintain and update the zone file. It stores the zone file on a local disk.

Secondary server :

- This server transfers complete information about a zone from another server which may be primary or secondary server. The transferred information is saved on the disc storage of the secondary server.
- The secondary server is not authorized to create or update a zone file. If its zone file is to be updated, then it is to be done by the primary server.

7.5 DNS in the Internet :

- Let us now understand how DNS is used in Internet where the domain name space (tree) is divided into three different sections as shown in Fig. 7.5.1.
 - Generic domain
 - Country domain.
 - Inverse domain.



(G-43)Fig. 7.5.1 : Use of DNS in Internet

7.5.1 Generic Domains :

- The registered hosts are defined in the generic domains according to their generic behaviour e.g. com for commercial organizations. The first level in the generic domains section allows 14 possible labels. Some of them are given in Table 7.5.1.

Table 7.5.1 : Generic domain labels

Table	Description
aero	Airline or aerospace related companies.
com	Commercial organizations.
coop	Cooperative business organizations.
edu	Educational institutions.
gov	Government institutions.
int	International organizations.
mil	Military organization.
net	Network support centers.
org	Non-profit organizations.

7.5.2 Country Domain :

- This domain section uses two character country abbreviations eg. US for united states.
- Second label in this domain can specify organization or national designations.

7.5.3 Inverse Domain :

The inverse domain is used for mapping an address to a name. This is exactly the opposite process discussed so far in which a name is mapped onto the address.

7.6 Name Address Resolution :

SPPU : May 09, May 12, May 13

University Questions

- Q. 1** What is an authoritative name server ? How can name server tell if a client wants a recursive query or not? (May 09, 6 Marks)
- Q. 2** Comment on the importance of DNS. Explain with suitable example how query resolving process is done ? (May 12, 8 Marks)
- Q. 3** What is DNS ? Explain with suitable example how query resolving process is done ? (May 13, 8 Marks)

The process of mapping a name to an address or vice versa is called as name address resolution.

Resolver :

- DNS application is based on the client server model. If a host wants to map a name to address or vice versa it calls a DNS client named as resolver.
- In other words, when the name ↔ address mapping is necessary a host calls a resolver.
- The resolver then sends a mapping request to the closest DNS server and accesses its storage.
- If this server has the requested information, it gives that information to the resolver but if it does not have the requested information, then it refers the resolver to other servers or asks other servers to provide the information.
- Thus the resolver receives the mapping from some source. It then checks for errors and if found error free delivers the mapping to the requesting process.

Mapping names to addresses :

- Generally the resolver gives a domain name to the server and requests for the corresponding IP address. The server checks the generic or country domains to get the corresponding address.
 - If the domain name is from the generic domain section then the resolver receives a domain name such as,
- xxx.yyy.zzz.edu
- The query is sent to the local DNS server for resolution by the resolver.
 - If the local server does not get the answer then, it will refer the resolver to other servers or asks them directly. The same procedure is followed for a name from country domain.

Mapping addresses to names :

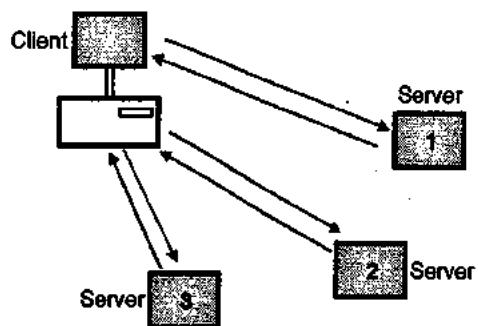
- Here, a client sends an IP address to a server and requests for its name. This type of query is called as PTR query. To answer the PTR query, the DNS uses the inverse domain.
- If the IP address is 142.36.48.118 then the resolver first inverts the address and adds two labels "in_addr" and "arpa" to it. So the domain name sent is : 118.48.36.142.in_addr.arpa.
- This is received by the local DNS and resolved.

7.6.1 Recursive Resolution :

- Sometimes a client (resolver) requests for recursive or final answer from a name server.
- If this server is authorised for the domain name, it checks its database and sends a reply.
- But if this server is not authorised it diverts this request to another server (usually the parent server) and waits for the response.
- If the parent has the authority, then it sends the answer, otherwise it diverts the query to another server.
- When the query is solved, the response is returned back to the requesting client.
- Such a query is called as recursive query and the process is called recursive resolution. It is illustrated in Fig. 7.6.1.

7.6.2 Iterative Resolution :

- This type of mapping can be done if the client does not ask for recursive answer.
- In iterative resolution, if the server has authority for the name it will send the answer. But if it does not have the authority then it returns to the client the IP address of the server that holds the answer to the query.



(G-638)Fig. 7.6.2 : Iterative resolution

- The client has to repeat the query to this new server. If this server also cannot answer the query then it sends the IP address of another server to the client.
- Now the client should send the query to this third server. This process is called as iterative resolution because client sends the same query to different servers.
- Fig. 7.6.2 illustrates the iterative resolution.

DNS examples :

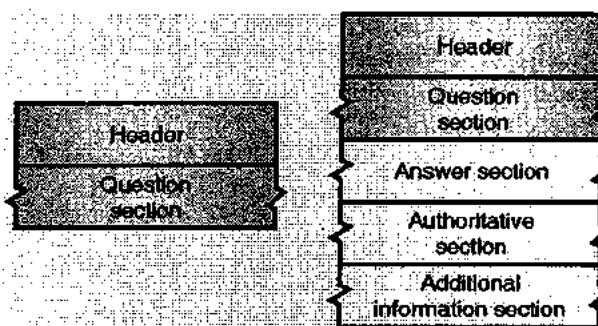
The DNS system is a **database** and no other database on the planet gets this many requests. No other database on the planet has millions of people changing it every day, either. That is what makes the DNS system so unique!

For example :

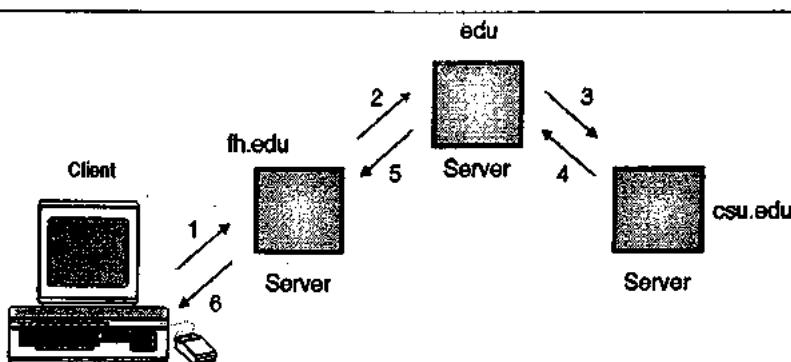
- www.yahoo.com - the world's best-known name.
- www.mit.edu - a popular EDU name.
- encarta.msn.com - a Web server that does not start with www.
- www.bbc.co.uk - a name using four parts rather than three.
- ftp.microsoft.com - an FTP server rather than a Web server.
- www.spce.ac.in - Server in India 'in' domain.
- The COM, EDU and UK portions of these domain names are called the **top-level domain** or **first-level domain**. There are several hundred top-level domain names, including COM, EDU, GOV, MIL, NET, ORG and INT, as well as unique two-letter combinations for every country.

7.6.3 The DNS Message Format :

- DNS has two types of messages as follows and both of them have the same format :
 1. Query
 2. Responses or reply
- The formats of the two DNS messages are as shown in Fig. 7.6.3.



(G-639) Fig. 7.6.3



(G-637)Fig. 7.6.1 : Recursive resolution

- Both query and reply messages have the same header format with some fields set to zero for query messages. The header is 12 byte long. The header format for both the types of messages is shown by shaded portions in Fig. 7.6.3.

7.6.4 Caching :

SPPU : May 09

University Questions

- Q.1** What is name server ? How does caching increase the efficiency of name resolution ?
(May 09, 6 Marks)

- Every time a query is asked, the server has to spend time in searching the corresponding IP address.
- If this searching time is reduced then efficiency would go up. The searching time can be reduced by using a technique called caching.
- When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client.
- If the same or other client request for the same mapping, it can check its cache memory and resolve the problem at its own level. This will certainly save a lot of time.
- But the problem with caching is that, if a server caches (stores) a mapping for a long time then the mapping may get outdated and the client will not get the latest mapping.
- This problem can be solved by adding the time to live information (TTL) to the mapping and each server is asked to keep a TTL counter for each mapping in its cache.

7.7 Electronic Mail :

- One of the most popular network services is electronic mail (e-mail).
- Simple Mail Transfer Protocol (SMTP) is the standard mechanism for electronic mail in the internet.
- The first e-mail systems simply consisted by file transfer protocols.
- But some of the limitations of this system were as follows :
 - It is difficult to send a message to a group of people.
 - Message did not have any internal structure. So its computer processing was difficult.
 - The sender never used to know if a message arrived or not.
 - It was not easy to handover one's e-mails to someone else for the purpose of managing them when one is out of town or country for some time.

- The user interface with the transmission system is poorly integrated.
- It was not possible to create and send messages containing a text, drawing, facsimile and voice together.

- So more elaborate e-mail systems were proposed. ARPANET e-mail proposals were published as RFC 821 (transmission protocol) and RFC 822 (message format).
- These are used in Internet.

7.7.1 E-mail Architecture and Services :

SPPU : May 06, Dec. 06, May 09, May 10

University Questions

- Q.1** Explain the function of Email system.
(May 06, 6 Marks)
- Q.2** Write a short notes on E-mail Architecture.
(Dec. 06, 6 Marks)
- Q.3** Explain Email architecture and services.
(May 09, May 10, 6 Marks)

- An e-mail system consists of two subsystems :
 - User agents and
 - Message transfer agents
- User agents :** They enable users to read and send e-mail.
- Message transfer agents :** They move the messages from the sender to the receiver.

Basic Functions :

- E-mail systems support five basic systems which are as follows :
 - Composition
 - Transfer
 - Reporting
 - Disposition
 - Displaying and
- 1. Composition :**
- The process of creating messages and to answer them is known as composition. The system can also provide assistance with addressing and a number of header fields attached to each message.
- 2. Transfer :**
- It is the process of moving messages from the sender to the recipient.
 - This includes establishment of a connection from sender to destination or some intermediate machine, transferring the message, and breaking the connection.
- 3. Reporting :**
- The reporting system is designed to tell the sender about whether the message was delivered or rejected or lost.
- 4. Displaying :**
- It is the process of displaying the incoming messages so that it can be read by the user. For this purpose simple conversions and formatting are required to be done.

5. Disposition :

- This is concerned with what the recipient does with the received message. Disposition is the final step in e-mail system.
- Some of the possibilities are as follows :
 1. Throw after reading
 2. Throw before reading
 3. Save messages
 4. Forward messages
 5. Process messages in some other way.

Advanced features of E-mail systems :

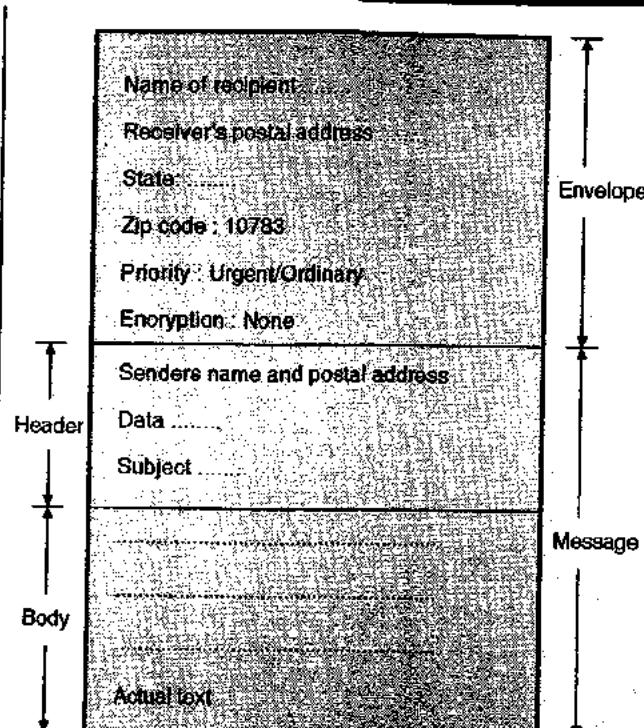
- Some of the advanced features included in addition to the basic functions are as follows :
 1. Forwarding an e-mail to a person away from his computer.
 2. Creating and destroying mailboxes to store incoming e-mail.
 3. Inspecting contents of mailbox, insert and delete messages from the mailboxes.
 4. Sending a message to a large group of people using the idea of mail list.
 5. To provide the facility of registered e-mail.
 6. Automatic notification of undelivered e-mails.
 7. Carbon copies.
 8. High priority e-mail (setting the priority of e-mails).
 9. Secret (encrypted e-mail).
 10. Alternative recipient. This allows automatic forwarding of an e-mail to an alternate recipient if the main recipient is not available.

E-mail Envelope :

- In the modern e-mail systems, there is a distinction made between the e-mail and its contents.
- An e-mail envelope contains the message, destination address, priority, security level etc.
- The message transport agents such as SMTP use this envelope for routing.

Message :

- The actual message inside the envelope is made of two parts :
 1. Header and 2. Body
- Header carries the control information while body contains the message contents.
- Envelopes and messages are shown in Fig. 7.7.1.



(G-64) Fig. 7.7.1 : Envelope and message

7.7.2 Message Formats :

SPPU : May 07

University Questions

Q. 1 Explain different message formats in email.

(May 07; 9 Marks)

Let us now discuss the e-mail message formats.

RFC 822 :

- All the e-mail messages consist of an envelope, a few header fields, a blank line and then the message body.
- Each header field logically consists of a single line of ASCII text which consists of the field name, a colon and a field.
- Normally the user agent builds a message and passes it to the message transfer agent which uses some header fields for construction of an envelope.
- Table 7.7.1 shows the principle header fields related to the message transport. Let us discuss them one by one.

Table 7.7.1 : RFC 822 header fields related to message transport

Header name	Meaning
To :	E-mail address of primary recipients.
Cc :	E-mail address of secondary recipients (Carbon copy).
Bcc :	E-mail address for blind carbon copies.
From :	Originator of the message.
Sender :	E-mail address of the person sending the message.
Received :	Line added by each transfer agent along the route.
Return – Path :	Can be used to identify the path back to the sender.

1. The To : field :

This field gives the DNS address of the primary recipient. It is allowed to have multiple recipients.

2. The Cc : field :

This field gives the addresses of any secondary recipients. Cc stands for carbon copy. Whatever message and attachments are sent to the primary recipient the same are sent to the secondary recipient as well.

3. The Bcc : field :

- The long form of Bcc is blind carbon copy. This field is like Cc field, except that this is deleted from all the copies sent to the primary and secondary recipients.
- Thus a sender can send copies to third parties without primary and secondary recipients knowing about it.

4. From : and Sender : fields :

- These fields tell about who wrote the message and who actually sent the message respectively because the person who creates the message and the person who sends it can be different.
- The From : Field is necessary but the Sender : field can be omitted, if it is same as the From : field.
- These fields are required when the message cannot be delivered and is to be returned to the sender.

5. Received : field :

- A line containing Received : is added by each message transfer agent along the way. This line carries the agent's identity, date and time at which the message was received.
- It also contains some other information that can be used to find bugs in the routing system.

6. The Return-Path : field :

- This field is added by the final message transfer agent and it is intended to tell how to get back to the sender.
- This information can be obtained from all the received : headers.

Other header fields :

- In addition to the fields of Table 7.7.2, RFC 822 messages may contain many other header fields. These are used by either the user agents or human recipients some of them are shown in Table 7.7.2.

Table 7.7.2 : Some fields in RFC 822 message header

Header	Meaning
Date :	The date and time of the message.
Reply-To :	E-mail address to which the reply is to be sent.
Message-Id :	Message identifying number.
In-Reply-To :	Message-Id of the message to which this is a reply.

Header	Meaning
References :	Other relevant message identifying numbers.
Keywords :	Keywords chosen by user.
Subject :	Summary of the message for the one line display.

- The RFC 822 allows the users to invent new headers for their own private use but it is essential that these headers start with the string X-. For example X-Event of the week.

Message body :

- The message body comes after the header. The users can include anything that they want to send, in the message body.
- It is possible to terminate the messages with ASCII cartoons, quotations, political statements etc.

7.8 MIME – Multipurpose Internet Mail Extensions :

SPPU : Dec. 09, Feb. 16

University Questions

- Q. 1** Write short notes on MIME. (Dec. 09, 9 Marks)
Q. 2 What is the use of MIME ? Explain MIME header in detail. (Feb. 16, 5 Marks)

- In the early days, the e-mail used to consist of only the text messages in English and expressed in ASCII.
- RS 822 was sufficient for this environment. But in the worldwide internet environment, this approach is not adequate.
- Some problems are encountered in sending and receiving the following types of messages.
 - Messages in certain languages that have accents such as French or Germans.
 - Messages which do not contain text e.g. audio and video.
 - Messages in the languages which do not have alphabets (e.g. Chinese and Japanese).
 - Messages which contain some non-Latin alphabets such as Russian or Hebrew.
- The solution to these problems was MIME i.e. Multipurpose Internet Mail Extensions. It was proposed in the standard RFC 1341 and then updated in RFC 1521.

7.8.1 Principle of MIME :

SPPU : May 11, Feb. 16

University Questions

- Q. 1** When web pages are sent out, they are prefixed by MIME headers, why ? (May 11, 7 Marks)
Q. 2 What is the use of MIME ? Explain MIME header in detail. (Feb. 16, 5 Marks)

- MIME uses the same RFC 822 format but it adds structure to the message body (In RFC 822 there is no structure to the message body). In addition to this, MIME defines encoding rules for non ASCII messages. It is possible to send MIME messages using the existing mail programs and protocols.



- The sending and receiving programs need to be changed to achieve this, which users can do themselves.

New message headers :

Five new message headers are defined for MIME. They are listed in Table 7.8.1.

1. MIME-Version :

It tells the user agent that this message is a MIME message and it also specifies the version of MIME being used.

Table 7.8.1 : New headers in MIME

Sl. No.	Header Name	Meaning
1.	MIME – Version :	Indicates the MIME version
2.	Content – Description :	Tells what is in the message
3.	Content – Id :	Identifier
4.	Content – Transfer – Encoding :	How is the body wrapped for transmission
5.	Content – Type :	Type of the message

2. Content-Description : This header tells what the message is. It is in the form of ASCII string. This header is needed because the recipient will know whether it is worth decoding and reading the message.

3. Content-Id : This field identifies the contents. Its format is same as the format of standard Message- Id header.

4. Content-Transfer-Encoding :

- This field tells how the body is wrapped for transmission through a network. The network can object to most characters except for the letters, numbers and punctuation marks.

- Five schemes are provided for this purpose in addition to an escape to new schemes. These schemes are as follows :

(a) The first scheme simply uses ASCII text. Each ASCII character uses 7-bits and can be carried directly if each line contains at the most 1000 characters.

(b) The second scheme is similar to the first scheme except for one change. Instead of 7-bit characters, now 8-bit characters are used. The maximum line length remains unchanged.

(c) Third is the messages using binary encoding. The problems with these messages are that they do not always use all the 8 bits and do not stick to the 1000 line per character limit. There is no guarantee that these messages arrive error free.

(d) The fourth type is encoded binary messages using base 64 encoding which is also called as ASCII armour.

- The fifth type is the messages with a special type of encoding called quoted-printable encoding.

5. Content-Type :

- This is last header in Table 7.8.1 and it is used to specify the type of the message body. RFC 1521 defines seven types with each one having one or more subtypes.
- The type and subtype are separated by a slash such as,

Content – Type : Video / mpeg.

The subtype must be given in the header. Table 7.8.2 gives the initial list of types and subtypes specified in RFC 1521.

Table 7.8.2 : The MIME types and subtypes in RFC 1521

Type	Subtype	Description
Text	Plain	Text in the unformatted way
	Richtext	Text includes simple formatting commands
Image	Gif	Still pictures in GIF format
	Jpeg	Still pictures in JPEG format
Audio	Basic	Audio or sound content
Video	Mpeg	Movie (video) in MPEG format
Applications	Octet-stream	Byte sequence in uninterpreted form
	Post script	A printable document in Post script
Message	Rfc 822	A MIME RFC 822 message
	Partial	Split message for transmission
	External body	Message itself should be fetched over the net
Multipart	Mixed	There are independent parts in the specified order
	Alternative	Same message in different formats
	Parallel	Parts must be viewed simultaneously
	Digest	Each part is a complete RFC 822 message

- Note that many new types have been added to the basic list of Table 7.8.2 and the addition is still being made. Let us discuss the content types listed in Table 7.8.2.

(a) Text :

- The text type is for straight text. There are two subtypes namely plain and richtext.

- The text/plain combination represents the original messages without any encoding or further processing.
- The text/richtext allows simple formatting in the text. It allows the text with boldface, italics, small and large point sizes, indentation, subscripts, page layout etc.

(b) Image :

- This MIME type is used for transmitting still pictures. There are many formats used for storing and transmitting images with or without compression.
- The two subtypes are GIF and JPEG.

(c) Audio and Video :

The audio type is for sound and video is for moving pictures. The video does not include any soundtrack. Only one video format defined is MPEG which is designed by the Moving Picture Experts Group (MPEG).

(d) Applications :

- This type is used for formats which require external processing and which is not covered by any other type.
- The octet stream is a sequence of uninterpreted bytes. When it is received a user agent should display it and suggest the user to copy it in a file for further processing.
- The other subtype is post script. It corresponds to the post script language produced by Adobe systems which is used for describing printed pages.

(e) Message :

- This type allows one message to be fully encapsulated inside the other message. This is useful in order to forward e-mails.
- The partial subtype allows to break an encapsulated message into pieces and send them separately.
- The external body subtype can be used for very long messages such as video films.

(f) Multipart :

- This is the last type of multipart. It allows a message to contain multiple parts in the same message. The beginning and end of each part is clearly demarcated within a message.

- There are four subtypes. The mixed subtype allows each part to be different. In the alternative subtype each part should contain the same message expressed in a different medium or encoding.
- The alternative subtype can be used for multiple languages as well.
- The parallel subtype is used for viewing all parts simultaneously e.g. audio and video parts of a movie.
- The fourth subtype is digest. It is used when many messages are packed together to form a composite message.

7.9 Message Transfer Agent : SMTP :

SPPU : May 07, Dec. 11

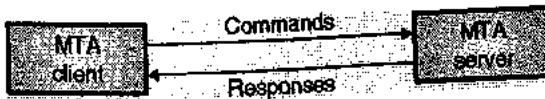
University Questions

- Q.1** Write short notes on : SMTP (May 07, 6 Marks)
Q.2 State which transport layer protocol is used by the following protocols: HTTP, FTP, DHCP, DNS, ICMP, TFTP, IP, SMTP. (Dec. 11, 4 Marks)

- The actual mail transfer is carried out through the message transfer agent. A system should have the client MTA in order to send a mail and it should have a server MTA in order to receive one.
- SMTP is the protocol which defines MTA client and server in the Internet.
- As shown in Fig. 7.9.1, the SMTP is used twice, once between the sender and sender's mail server and then between the two mail servers.
- The job of SMTP is simply to define how commands and responses be sent back and forth. Each network can choose its software package for implementation.

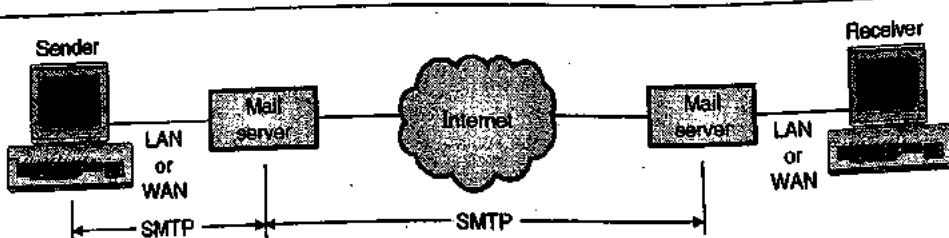
7.9.1 Commands and Responses :

- As shown in Fig. 7.9.2, SMTP the transfer of messages between MTA client and MTA server takes place using the command and response principle.



(G-642)Fig. 7.9.2 : Commands and responses in SMTP

- Each command or response is terminated by a two character end of line token. The two characters used are carriage return and line feed.



(G-641)Fig. 7.9.1 : SMTP range



7.9.2 SMTP (Simple Mail Transfer Protocol)

Operation : SPPU : Dec. 06, May 11

University Questions

- Q. 1 Explain the role of SMTP and POP protocol in E-mail message transfer. (Dec. 06, 9 Marks)
- Q. 2 Explain FTP protocol. Can SMTP be used to retrieve mail from mail server to the client. (May 11, 6 Marks)

- In internet the source machine establishes a connection to port 25 of the destination machine so as to deliver an e-mail.
- An e-mail daemon which speaks SMTP is listening to this port.
- This daemon is supposed to perform the following tasks :
 1. Accept the incoming connections, and copy messages from them into appropriate mailboxes.
 2. Return an error message to the sender, if a message is not delivered.
- SMTP is a simple ASCII protocol.
- Once a TCP connection between a sender and port 25 of the receiver is established, the sending machine operates as a client and the receiving machine acts as a server.
- The client then waits for the server to take initiative in communication.
- The server sends a line of text which declares its identity and announces its willingness/unwillingness to receive mail. If the server is not prepared, the client will release the connection, wait for some time and try again later.
- But if the server is willing to accept e-mail, then the client announces the sender of e-mail and its recipient.
- If such a recipient exists at the destination, then the server tells the client to send the message. The client, then sends the message and the server sends back its acknowledgement.
- No checksums are generally required because TCP provides a reliable byte stream. If there are any more e-mail, then they can be sent now.
- After exchanging all the e-mail, the connection is released.
- SMTP uses numerical codes. The lines sent by the client are marked C:; and those sent by the server are marked S:;
- Some of the commands, useful for communication are : HELO, RCTP, DATA, QUIT etc.
- RCTP represents recipient. If only one command is used then the message is being sent to only one recipient. If the command is used many times, then it indicates that the message is sent to more than one recipients.
- In such a case each message is individually acknowledged or rejected.

- The syntax of four character commands for the clients are rigidly specified but the syntax for the replies are not that rigid.
- The SMTP protocol is well defined by RFC 821 but some problems are still present.

Problems in SMTP :

Some of the problems in SMTP are as follows :

1. Some older versions of SMTP are not capable of handling messages longer than 64 kB.
2. If client and server have different time-outs, then one of them may give up when the other is still busy. This will terminate the connection unnecessarily.
3. In rate situations, infinite mailstorms can be triggered.

Extended SMTP (ESMTP) :

Some of these problems can be solved by using the extended SMTP (ESMTP) which is defined in RFC 1425.

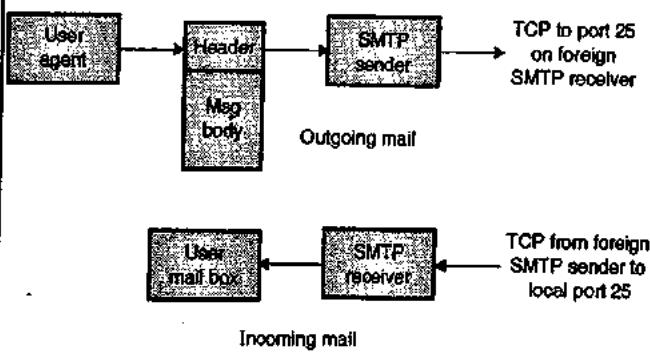
7.9.3 Components of E-mail System :

The three main components of internet mail system are :

1. User Agent (UA)
2. SMTP sender
3. SMTP receiver

They are shown in Fig. 7.9.3.

- The mail is created by a user agent program in response to user input. Each created message consists of a header which includes the recipient's E-mail address and other information and the message body containing the message to be sent.
- These messages are lined up to form a queue and provided as input to an SMTP sender program.
- The SMTP sender takes messages from the queue and transmits them to the proper destination host via SMTP connection over one or more TCP connections to port 25.
- The SMTP protocol is used to transfer a message from the SMTP sender to SMTP receiver and it uses TCP connection for the same.
- The SMTP receiver accepts each arriving message and stores it in the user mail box. If the mail is to be forwarded then the SMTP receiver copies it to the outgoing mail queue.



(G-643) Fig. 7.9.3 : SMTP mail flow

7.9.4 SMTP Commands :

- The operation of SMTP consists of a series of commands and responses exchanged between the SMTP sender and receiver.
- The SMTP sender establishes the TCP connection to the receiver. After establishing the connection, the SMTP sender sends commands over the connections to the receiver.
- The SMTP receiver generates exactly one reply from the SMTP receiver.
- Table 7.9.1 shows the SMTP commands. Each command consists of a single line of text which begins with a four letter command code followed in some cases by an argument field.
- Most replies are a single line. However multiline replies also are possible.

Table 7.9.1 : SMTP commands

Name	Description
HELO	Send identification of the sender.
MAIL	Identifies originator of mail.
RCPT	Identifies recipient of mail.
DATA	Transfer message text.
RSET	Abort the current mail transaction.
NOOP	No operation.
QUIT	Close TCP connection.
SEND	Send mail to terminal.
SOML	Send mail to the terminal if possible, otherwise to mailbox.
SAML	Send mail to terminal and mail box.
VRFY	Confirm user name.
EXPN	Return membership of mailing list.
HELP	Send system-specific documentation.
TURN	Reverse role of sender and receiver.

7.9.5 SMTP Operation :

The basic SMTP operation occurs in three phases :

- Connection setup
- Exchange of one or more command-response pairs
- Connection termination

1. Connection setup :

- The sender opens (i.e. creates) a TCP connection with the receiver.
- Once the connection is established, the receiver identifies itself with "220 Service Ready".
- The sender identifies itself with HELO command.
- The receiver accepts the sender's identification with "250 OK".

2. Mail transfer :

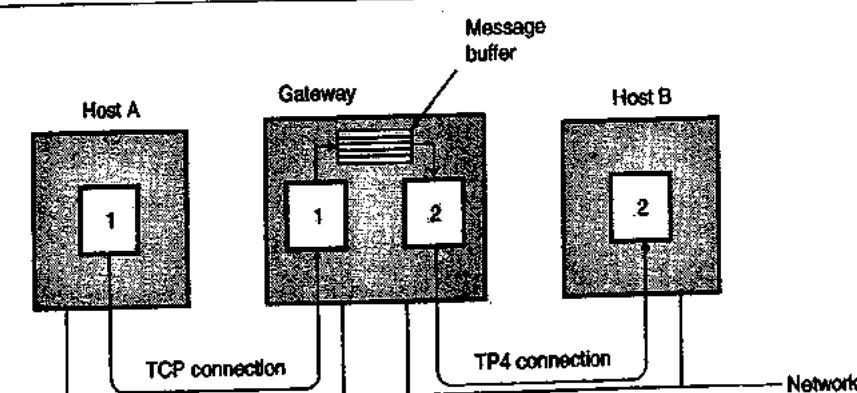
- Once the connection has been established, the SMTP sender may send one or more messages to SMTP receiver.
- There are three logical phases to transfer a message :
 - A MAIL command identifies the originator of message.
 - One or more RCPT commands identify the recipient for this message.
 - A DATA command transfers the message text.

3. Connection closing :

- The SMTP sender closes the connection in two steps. First the sender sends a QUIT command and waits for a reply.
- Second step is to initiate a TCP close operation for the TCP connection.
- The receiver initiates its TCP close after sending its reply to the QUIT command.

7.10 E-mail Gateways :

- The E-mail using SMTP can work properly if both the sender and the receiver are connected to the Internet and can support TCP connections between them. But there can be many machines which are not on the Internet still want to send and receive e-mail.
- This is made possible by using the application layer e-mail gateways, as shown in Fig. 7.10.1.



(G-644) Fig. 7.10.1 : E-mail gateway

- In Fig. 7.10.1, host A speaks only TCP/IP and RFC 822 whereas host B speaks only OSI TP4 and X.400. So without the e-mail gateway they cannot exchange e-mails. But e-mail gateway allows them to exchange e-mails.
- Host A first establishes a TCP connection to the gateway. Then it uses SMTP and transfer message (1) to the gateway message buffer.
- Then the gateway daemon establishes a TP4 connection (OSI equivalent of TCP) with the destination host B, and message (2) is transferred using the OSI equivalent of SMTP.
- A gateway process is supposed to extract incoming messages from one queue and deposit them in the other.

Problems :

- The first problem is that the internet addresses are totally different from the X.400 addresses so an elaborate mapping between them is required.
- The envelopes and header fields of one system are different from those of the other.
- The body parts are incompatible. For simple unstructured text messages in ASCII, gatewaying is a good solution. But it is not suitable for sending a more complex message than that.

7.11 Message Access Agent : POP and IMAP :

- The SMTP is used in the first and second stages of mail delivery. But SMTP is not used in the third stage, because SMTP is a push protocol which is meant for pushing the message from client to server.
- The third stage needs a **pull** protocol because the client has to pull messages from the server. The bulk data gets transferred from the server to client. Therefore third stage uses a message access agent which is a pull protocol.
- The two message access agents available are :
 - Post office protocol, version 3 (POP 3).
 - Internet mail access protocol (IMAP 4).

7.11.1 POP 3 :

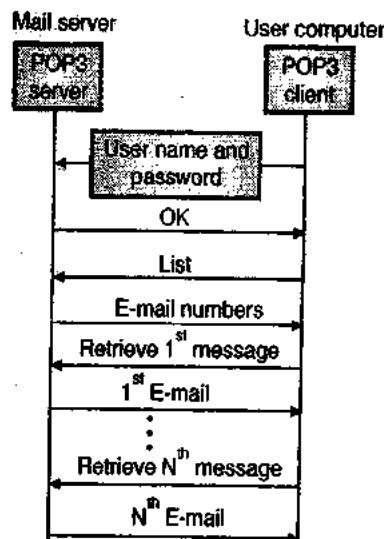
SPPU : Dec. 15

University Questions

Q.1 Explain POP3

(Dec. 15, 3 Marks)

- The POP 3 consists of client POP3 software and server POP 3 software. Out of these, the client POP3 software is installed on the receiving computer whereas the mail server gets the server POP 3 software installed on it.
- When the user wants to download email from the mailbox on the email server, the events take place in the following sequence. Refer Fig. 7.11.2.
 - The client (user) establishes a connection with the server on TCP port 110.
 - The client then sends its user name and password to the server in order to access the mailbox.
 - The user is then allowed to list and get the mail messages one by one.
- This is called as downloading. It is illustrated in Fig. 7.11.2.



(G-67) Fig. 7.11.2 : Downloading in POP 3

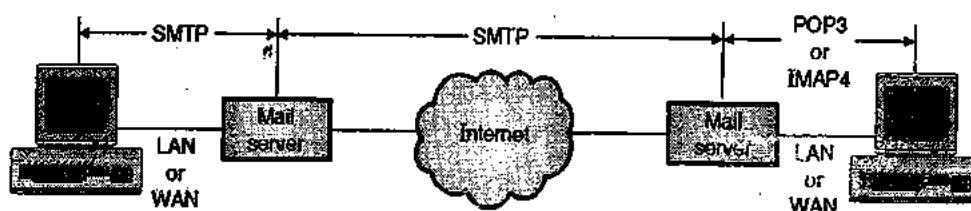
Modes of POP 3 :

POP3 has two modes of operation :

1. Delete mode and 2. Keep mode.

Delete mode : In this mode the mail is deleted from the mailbox after each retrieval. This mode is used when the user is working on his permanent computer because it is then possible for him to save and rearrange the received mail after reading it.

Keep mode : If operated in this mode, the mail remains in the mailbox after retrieval. This mode is used when the user accesses mail away from the primary computer. The read mail can be organized later.



(G-65) Fig. 7.11.1 : Use of POP 3 or IMAP 4

Disadvantages of POP 3 :

1. POP 3 does not allow organization of email on the server.
2. The user can not create different folders on the server. It can create them only on his own computer.
3. The user can not partially check the contents of E mail before downloading.

7.11.2 IMAP 4 : SPPU : May 09, May 10, Dec.15**University Questions**

- Q. 1** Why do we need POP3 and IMAP 4 for electronic mail? (May 09, 6 Marks)
Q. 2 Write short notes on IMAP 4. (May 10, 9 Marks)
Q. 3 Explain IMAP 4. (Dec. 15, 3 Marks)

- Internet Mail Access Protocol Version 4 (IMAP 4) is another mail access protocol which is very similar to POP 3 but has more features.
- This makes IMAP 4 more powerful but more complex as compared to POP3.
- IMAP is more sophisticated than POP 3 and it is defined in RFC 1064.
- IMAP is ideal for a user having multiple computers such as a laptop on the road, PC at home and a workstation in office.
- IMAP maintains a central repository which can be accessed from any machine. So IMAP does not copy e-mail to the user's personal machine.
- An important feature of IMAP is its ability to address mail not by arrival number but by using attributes. That means the mailbox is like a relational database system than a linear sequence of messages.

Extra features of IMAP4 :

1. It is possible for the user to check the header before down loading.
2. It is possible for the user to search for the contents of E mail before downloading.
3. It is possible to partially download E mail.
4. It is possible for the user to create, rename or delete mailboxes on the mail server.
5. It is possible for the user to create a hierarchy of mailboxes in a folder for storing e-mails.

7.11.3 Comparison of IMAP and POP 3 :

SPPU : Dec. 07, Dec. 08

University Questions

- Q. 1** List the similarities and differences between POP 3 and IMAP. From ISP point of view which protocol would be better and why? (Dec. 07, Dec. 08, 6 Marks)

Sr. No.	Parameter	POP 3	IMAP
1.	Protocol is defined at	RFC 1939	RFC 2060
2.	TCP port used	110	143
3.	e-mail is stored at	User's PC	Server

Sr. No.	Parameter	POP 3	IMAP
4.	e-mail is read	Off line	On line
5.	Time required to connect	Small	Long
6.	Use of server resources	Minimal	Extensive
7.	Multiple mail boxes	Not possible	Possible
8.	Who backs up mailboxes	User	ISP
9.	For mobile users	Not good	Good
10.	User control over download	Little	Great
11.	Partial message downloads	No	Yes
12.	Simplicity in implementation	Yes	No
13.	Support	Wide spread	Increasing

7.12 Web Based Mail :

- Some websites provide the e-mail service to any user who accesses the site. The examples are hotmail and yahoo.
- The idea is simple. Mail transfer from sender's browser to his mail server is done using HTTP.
- The message transfer from the sending mail server to the receiving mail server also takes place using SMTP.
- But in the third phase POP 3 or IMAP 4 is not used. Instead HTTP is used. That means HTTP is used for transfer of message from receiving server to destination computer.
- When the receiver wants to retrieve his e-mail, he sends a message to that website (hotmail or yahoo).
- The website sends a form to the recipient in which the log-in name and password are to be filled in.
- If the log-in name and password match, the e-mail is transferred from the website to receiver's browser in HTML format.

7.13 File Transfer Protocol (FTP) :

SPPU : Dec. 07, Dec. 08, May 09, Dec. 09, May 10, May 11, Dec. 11, May 15, May 16

University Questions

- Q. 1** FTP service is liable because it uses two ports, port 20 and port 21. Give your comments to justify or to nullify the statement. (Dec. 07, 8 Marks)
- Q. 2** Explain the working of FTP protocol in detail. (Dec. 08, 8 Marks)
- Q. 3** Does FTP and TFTP perform error recovery. If so, describe the basics of how this occurs? (May 09, May 10, 6 Marks)

- Q. 4** How FTP works ? Explain. (Dec 09, 9 Marks)
Q. 5 Explain FTP protocol. Can SMTP be used to retrieve mail from mail server to the client. (May 11, 6 Marks)
Q. 6 State which transport layer protocol is used by the following protocols : HTTP, FTP, DHCP, DNS, ICMP, TFTP, IP, SMTP. (Dec 11, 4 Marks)
Q. 7 Explain FTP in detail. (May 16, 7 Marks)
Q. 8 What is FTP ? What are the three FTP transmission modes ? (May 16, 4 Marks)

- A standard mechanism provided by the Internet which helps in copying a file from one host to the other is known as the File Transfer Program (FTP).
- Some of the problems in transferring files from one system to the other are as follows :
 1. Two systems may use different file name conventions.
 2. Two systems may represent text and data in different ways.
 3. The directory structures of the two systems may be different.
- FTP provides a simple solution to all these problems.
- The basic model of FTP is shown in Fig. 7.13.1.
- FTP establishes two types of connections between the client and server. One of them is used for data transfer and the other is for the control information.
- The fact that FTP separates control and data makes it very efficient.
- The control connection uses simple rules of communication. Only one line of command or a line of response is transferred at a time.
- But the data connection uses more complex rules due to the variety of data types being transferred.
- FTP uses port 21 for the control connection and port 20 for the data connection. Both these are well known TCP ports.
- As shown in Fig. 7.13.1 the client is made of three blocks namely :
 1. User interface
 2. Control process and
 3. Data transfer process.

- The server has two blocks : the control process and data transfer process.
- The control connection connects the control processes while data connection connects the data transfer processes as shown in Fig. 7.13.1.
- The control connection is kept alive during the entire interactive FTP session. The data connection is first opened, file is transferred and data connection is closed. This is done for transferring each file.

Control connection :

- This connection is created in the same way as the other application programs described earlier.
- Control connection remains alive during the entire process.
- The IP uses minimize delay type service because this is an interactive connection between a user and a server.

Data connection :

- Data connection uses the port 20 at the server site. This connection is opened when data to be transferred is ready and it is closed when transfer of data is over.
- The data connection does not remain open continuously like control connection. It is opened and closed many times as per requirement.

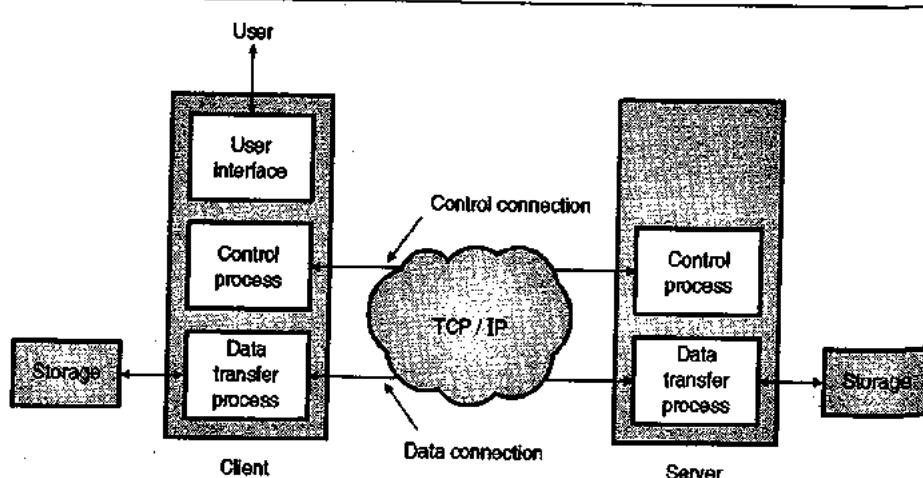
7.13.1 Communication in FTP :

SPPU : Dec 06, May 07, May 13

University Questions

- Q. 1** Compare the FTP and TFTP. List the 5 commands of each. (Dec 06, May 07, 9 Marks)
Q. 2 Compare file transfer using FTP and HTTP methods. (May 13, 6 Marks)

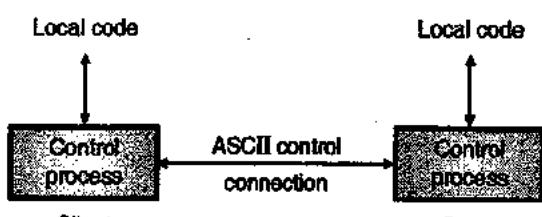
- FTP operates in client – server environment. The two computers involved in communication may be different in terms of the operating systems, character sets, file structures and file formats etc.
- FTP can make them compatible. The approaches for communication over control connection and data connection are different from each other.



(G-648)Fig. 7.13.1 : Basic model of FTP

1. Communication over control connection :

- Refer Fig. 7.13.2 to understand the FTP's approach for the communication over the control connection.
- Similar to SMTP, FTP uses a set of ASCII characters to communicate across the control connection.
- Communication is achieved through a process of commands and response. One command is sent at a time. Each command or response is only of one short line.
- So it is not necessary to think about file format or file structure. Each line is ended with a two character token. The two characters used in the token are carriage return and line feed.



(G-649)Fig. 7.13.2 : Communication over control connection

2. Communication over data connection :

- The purpose of implementing a data connection is to transfer a file. For this the client has to define the following :
 - Type of file being transferred.
 - Structure of data in the file.
 - Mode of transmission.
- Before the transmission over data connection, the communication over control connection is performed.
- Refer Fig. 7.13.2(a) to understand communication over data connection. The problem of heterogeneity is solved by defining three attributes of communication : file type, data structure and transmission mode. Let us discuss them one by one.

7.13.2 File Types :

- FTP can use one of the following file types for transfer of data over the data connection :
 - ASCII file
 - EBCDIC file
 - Image file.
- ASCII file is a text file, EBCDIC file can be transferred if both ends use EBCDIC encoding.
- Image file is the default format for transferring the binary files.
- With ASCII or EBCDIC files one more attribute must be added for defining the printability of the file. This attribute is nonprint or TELNET.

7.13.3 Data Structure :

- FTP can use one of the following data structures :
 - File structure (default)
 - Record structure and
 - Page structure.
- File has no structure. It is simply a continuous stream of bytes.
- In the record structure the file is divided into records. This data structure is suitable only for the text files.
- In page structure, a file is divided into pages which can be stored or accessed randomly or sequentially.

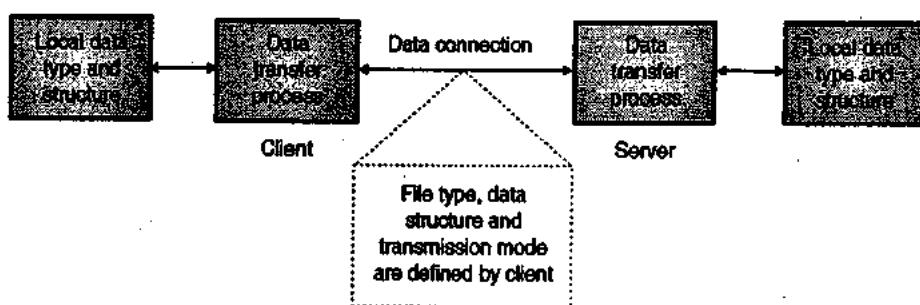
7.13.4 Transmission Mode :

SPPU : May 16

University Questions

Q. 1 What is FTP? What are the three FTP transmission modes? (May 16, 4 Marks)

- FTP uses one of the following modes to transfer a file :
 - Stream mode
 - Block mode and
 - Compressed mode.

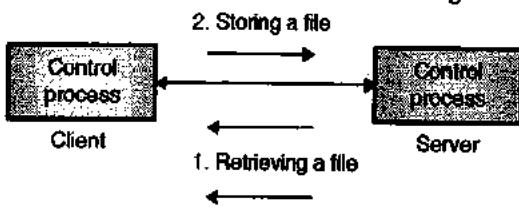


(G-650)Fig. 7.13.2(a) : Communication over the data connection

- Stream mode :** In this mode the data is delivered from FTP to TCP in the form of continuous stream of bytes. TCP chops this data into segments of appropriate size stream mode is the default mode of transmission.
- Block mode :** In this mode, data delivery from FTP to TCP takes place in the form of data blocks. Each such block is preceded by a 3 byte header.
- Compressed mode :** For big files the data can be compressed. Generally a run length encoding is used for compression.

7.13.5 File Transfer :

- File transfer takes place over the data connection and the commands are sent over the control connection. The commands supervise the data transfer.
- But file transfer in FTP means one of the following :
 - Retrieving a file :** Server copies a file onto a client.
 - Storing of a file :** A file can be copied from client to the server.
 - A server sends a list of directory or file names to the client. FTP treats such a list of directory also as a file.
- The file transfer has been illustrated in Fig. 7.13.3.



(G-651)Fig. 7.13.3 : File transfer

7.13.6 FTP Commands :

SPPU : Dec. 06, May 07, May 13

University Questions

- Q. 1** Compare the FTP and TFTP. List the 5 commands of each. (Dec. 06, May 07, 9 Marks)
- Q. 2** Compare file transfer using FTP and HTTP methods. (May 13, 8 Marks)

- The following commands are used for copying files using FTP.

Table 7.13.1 : FTP commands to transfer files

Command	Explanation
Get	Copy a file from remote host to local host
M get	Copy multiple files from the remote host to local host
Put	Copy a file from local host to remote host
M put	Copy multiple files from the local host to remote host

- FTP commands used to connect to a remote host are as shown in Table 7.13.2.

Table 7.13.2 : FTP commands to connect to a remote host

Command	Explanation
Open	Select the remote host and initiate login session
User	Identify the remote user ID
Pass	Authenticate the user
Site	Send the information to the remote host.

- FTP commands used to end an FTP session are as shown in Table 7.13.3.

Table 7.13.3 : FTP command to terminate session

Command	Explanation
Quit	Disconnect from the remote host and terminate FTP.
Close	Disconnect from the remote host but leave FTP client running.

7.13.7 Anonymous FTP :

SPPU : Feb. 16

University Questions

- Q. 1** When I asked my company admin for some software he asked me to use 'anonymous FTP' and download it ? What is it ? Outline a problem scenario using it. (Feb. 16, 3 Marks)

- A user needs to have an account (or username) alongwith a password on the remote server if he wants to use FTP.
- Some sites have a set of files available for public access to enable anonymous FTP.
- A user does not need to have an account or password to access these files. Instead the user can use **anonymous** as the user name and **guest** as the password.

7.14 TFTP :

SPPU : May 09, May 10, Dec. 11

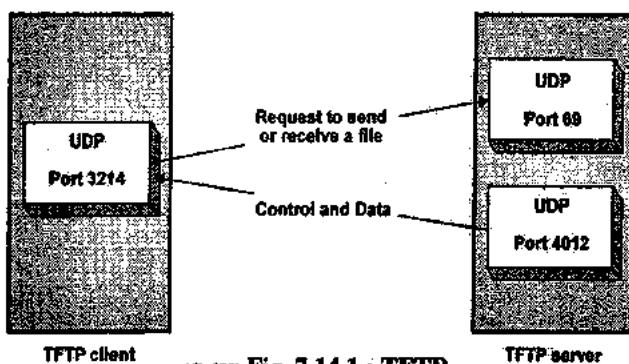
University Questions

- Q. 1** Does FTP and TFTP perform error recovery. If so, describe the basics of how this occurs ? (May 09, May 10, 6 Marks)
- Q. 2** State which transport layer protocol is used by the following protocols: HTTP, FTP, DHCP, DNS, ICMP, TFTP, IP, SMTP. (Dec. 11, 4 Marks)

- The Trivial File Transfer Protocol (TFTP) is a minimal protocol for transferring files without authentication and without any separation of control information and data as in FTP.
- TFTP is frequently used by devices without permanent storage for copying an initial memory image (bootstrap) from a remote server when the devices are powered on. Due to the lack of any security features, the use of TFTP is generally restricted. TFTP uses the unreliable transport protocol UDP for the transportation of data.



- Each TFTP message is carried in a separate UDP datagram. The first two bytes of a TFTP message specify the type of message, which can be a request to download a file, request to upload a file, a data message, or an acknowledgement or error message.
- At the beginning of a TFTP session a TFTP client sends a request to upload or download a file from a UDP port to the (well-known) UDP port 69 of an TFTP server.
- When the request is received the TFTP server picks a UDP port of its own and uses this port to communicate with the TFTP client. Thus, both client and server communicate using ephemeral ports as shown in Fig. 7.14.1.



(G-652) Fig. 7.14.1 : TFTP

- Since UDP does not recover lost or corrupted data, TFTP is supposed to maintain the integrity of the data exchange.
- TFTP transfers data in blocks of 512 bytes. A 2 byte long sequence number is assigned to each block and is transmitted in a separate UDP datagram.
- A block must be acknowledged before the next block can be sent. When an acknowledgment is not received before a timer expires, the block is retransmitted. When the receiver receives a block that is less than 512 bytes long, it assumes that the end of file has been reached.

7.14.1 Comparison of FTP and TFTP :

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

University Questions

- Q. 1** Compare FTP and TFTP. (May 06, May 11, 3 Marks)
- Q. 2** Compare the FTP and TFTP. List the 5 commands of each. (Dec. 06, May 07, 9 Marks)

Sr. No.	Parameter	FTP	TFTP
5.	Ports	21 – control, 20 – data	Port 3214; 69, 4012
6.	Data transfer	Reliable	Unreliable

7.15 World Wide Web (WWW) :

SPPU : Dec. 09, May 10

University Questions

- Q. 1** What is WWW ? How it works ? What is the difference between static and dynamic web pages ? (Dec. 09, 9 Marks)
- Q. 2** Write short notes on : WWW. (May 10, 9 Marks)

- People have become aware of the power of Internet through WWW. HTTP is a file transfer protocol which is specifically designed to facilitate access to the WWW.
- The World Wide Web is an architectural framework for accessing documents which are spread out over a number of machines over Internet.
- It has a colourful graphical interface which is easy for the beginners to use.
- It provides information on almost every subject. The web (also known as WWW) began in 1989 at CERN the European center for nuclear research.
- The web was designed basically to connect scientists stationed all over the world.
- The web is basically a client-server system. The web pages are written in the languages HTML and Java.
- The growth of the World-Wide Web (WWW or simply Web) today is simply phenomenal. Each day, thousands of more people join the Internet (above 100 million users at recent estimates).
- Easy retrieval of electronic information along with the multimedia capabilities of Web browsers (like Mosaic or Netscape) are the factors responsible for this explosion.
- This topic provides some basic information behind some of this technology used in accessing the World-Wide Web.

Difference between Web and Internet :

The Web and the Internet are not the same thing. The Web is a collection of standard protocols or instructions, sent back and forth over the Internet to gain access to information. The Internet, on the other hand, is a "network of networks" -- a more physical entity.

7.15.1 Web from the Users Side :

- The user (client) looks at the web as a collection of vast worldwide collection of documents called **pages** in short.
- Links or pointers :** Each page may contain links or pointers to it, related pages, anywhere in the world. A user can follow a link by clicking on it.

Sr. No.	Parameter	FTP	TFTP
1.	Operation	Transferring files	Transferring files
2.	Authentication	Yes	NO
3.	Control and data	Separated	Not separated
4.	Protocol	TCP	UDP

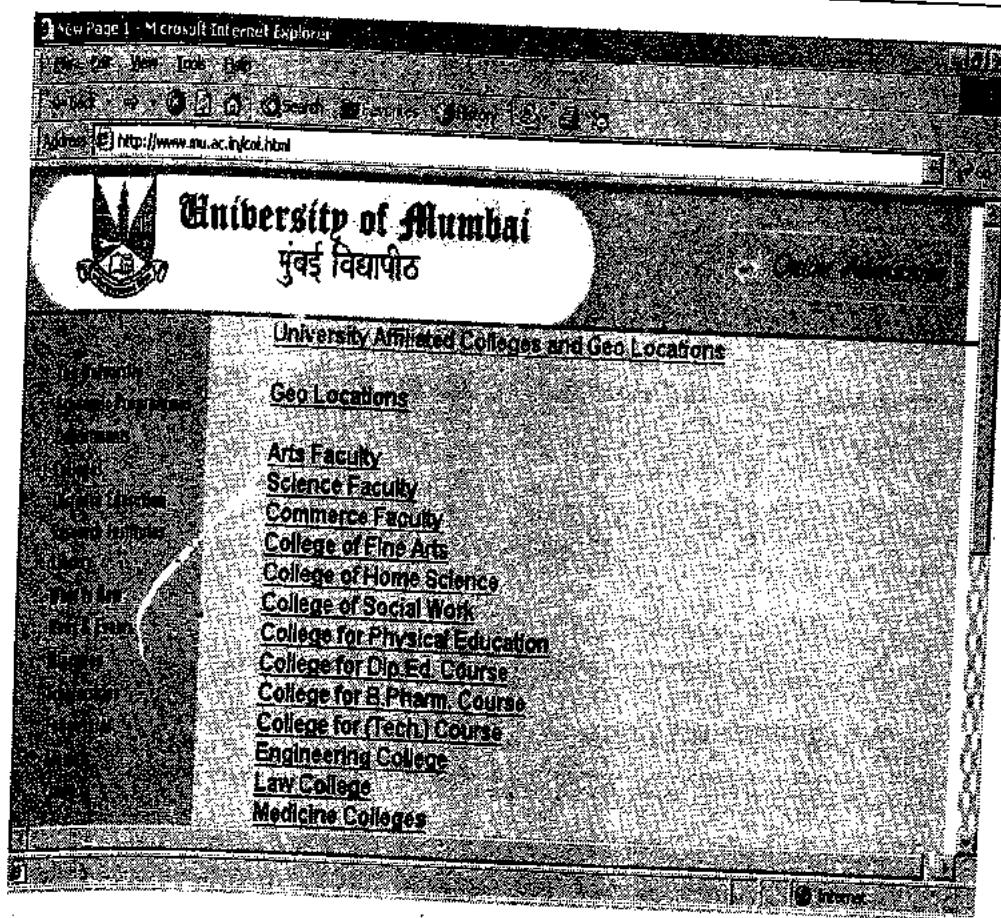


- This will take him to the pages pointed by the links. This process can be repeated indefinitely.
- **Hypertext** : Pages which point to the other pages are said to use hypertext.
- **Browser** : The program used for viewing pages is called as a browser.
- The job of a browser is to fetch the page requested by the user, interprets the text and formatting commands which it contains, display the page with proper format on the screen.
- An example of a web page is shown in Fig. 7.15.1.
- A web page starts with a title and contains the following :
 1. Some information
 2. Strings of text, linked to other pages
 3. E-mail address of the page's maintainer.
- **Hyperlinks** : Strings of text that are links to other pages are called hyperlinks. They are high lightened by underlining, using special colour or both.
- In order to follow a link, the user has to place the cursor on the high lightened area using the mouse or arrow keys and select it by clicking the mouse or pressing the ENTER key.
- The browsers can be of two types, namely the graphical browsers and nongraphical browsers. But

- the graphical browsers are more popular. Voice based browsers are also being developed.
- Most browsers have a large number of buttons and features which make the navigation on web easier. There can be a button to back to the previous page or a button for going forward to the next page.
- Some browsers can provide a facility of having a button or menu item to set a bookmark on a given page and another one to display the list of bookmarks. This makes it possible to revisit any of them with a single click on mouse.
- It is also possible to save pages or print them. Lot of options are available to control the screen layout and setting various preferences of the users.
- The web pages can also contain line drawings, icons, maps, photographs etc and they can be linked (if required) to another page.

Hypermedia :

- All pages may not be viewable in the conventional way because some pages may contain audio tracks, video clips or both.
- If the hypertext pages are mixed with other media, the result of such a mixing is called as hypermedia.
- Some browsers are capable of displaying all kinds of hypermedia but others cannot do so.



(G-653) Fig. 7.15.1 : A Web page



- Many web pages contain large images that take a long time to load. When the images are being loaded, the user does not have anything to see.
- To solve this problem, some browsers first fetch and display the text and then get the images. The user can read the text when images are getting loaded. Another strategy can be to provide an option to disable the automatic fetching and displaying of images.
- One more alternative opted by some page writers is to display the full image in a coarse resolution and then to fill up the details gradually.
- Some web pages display forms requesting the user to fill up information. This is meant for searching a database for a user supplied item or ordering a product etc.
- Some web pages contain maps which allow the users to click on them to get the zooming facility or get information about the clicked geographical area.
- For hosting a web browser a machine should be directly connected to the Internet or at least have a SLIP or PPP connection to a router or other machine which is directly connected to Internet.
- This is because of the manner in which the browser fetches a page. To fetch a page it has to establish a

TCP connection to the machine from where the page is to be fetched.

7.15.2 Web from the Servers Side :

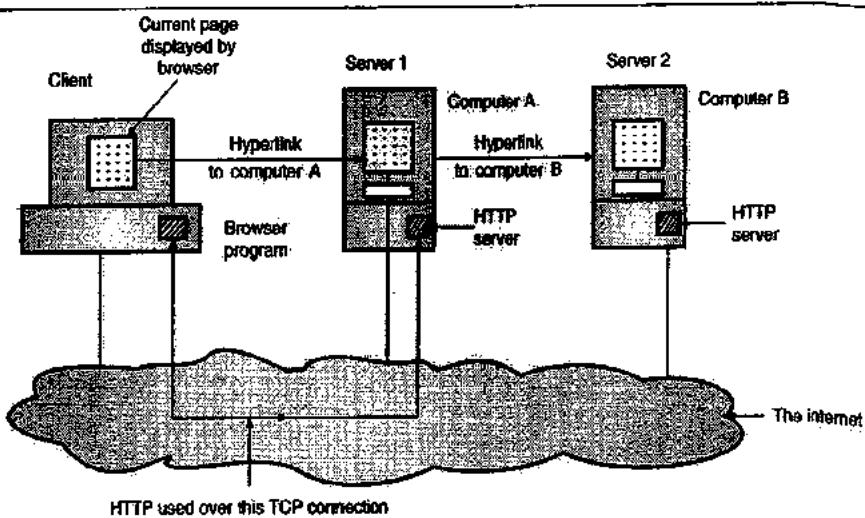
- Every website has a server process. It is listening to TCP port 80 on which incoming clients (browsers) are connected.
- Once a connection is established, the client sends a request and the server sends a reply for that. Then the connection is released.
- The protocol used for defining the legal request and replies is called HTTP.
- Fig. 7.15.2 shows various parts of the web model.

7.15.3 WWW Architecture :

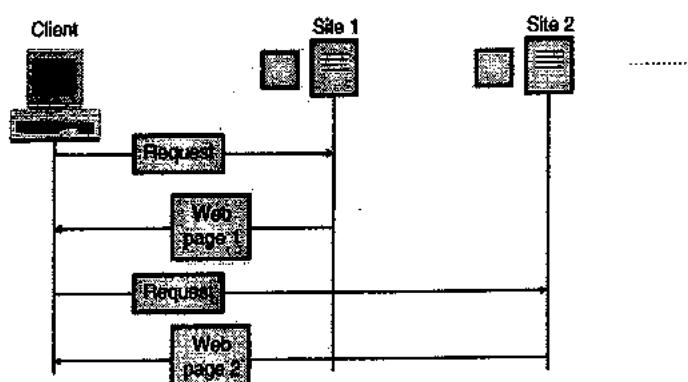
SPPU : Dec. 09, Dec. 12

University Questions

- Q.1 What is WWW ? How it works ? What is the difference between static and dynamic web pages ?
 (Dec. 09, 9 Marks)
- Q.2 What is DNS ? Explain with suitable example process of delivering of requested web page on your computer ?
 (Dec. 12, 8 Marks)



(G-654) Fig. 7.15.2 : Web model



(G-655) Fig. 7.15.3 : WWW architecture

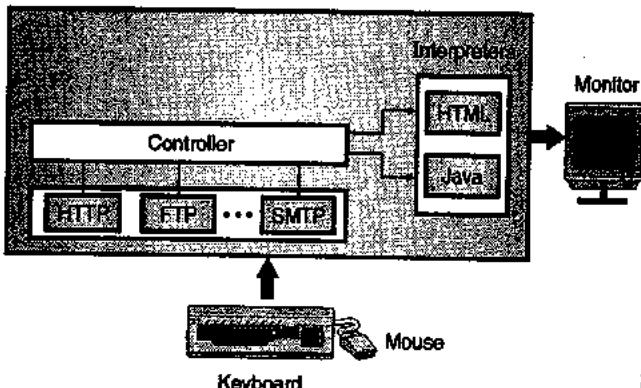


- The WWW is a distributed client/server service. A client (user) uses a browser to access a service using a server. But the service provided is distributed over a number of separate locations called as sites.
- Fig. 7.15.3 shows the architecture of WWW.
- As shown in Fig. 7.15.3, there are number of sites and each site holds a number of web pages. These pages can be retrieved and viewed by using browsers.
- The client sends a request through its browser to get a web document from a particular site.
- This request contains the site address and web page address (called URL) along with some other information.
- The server at the requested website finds the document and sends it to the client.

7.16 Browser (Client) :

- Even though a number of browsers are available around, the browser architecture is nearly the same for all of them.
- Each browser consists of the following parts :
 - A controller
 - Client programs
 - Interpreters.
- Fig. 7.16.1 shows the general architecture of a browser.
- The controller receives input from the keyboard or mouse. It then uses the client programs like HTTP, FTP etc to access the document.
- After accessing the document, the controller makes use of an interpreter such as HTML or Java (depending on type of document) and displays the accessed document on the screen.

Browser



(G-665) Fig. 7.16.1 : Browser architecture

7.16.1 Server :

- All the information is stored in the form of web pages at the server. Whenever a client requests for one the corresponding document is sent to the client.

7.16.2 Uniform Resource Locator (URL) :

- The client accessing a web page needs an address. The HTTP uses the URL to facilitate the access of any document distributed over the world. The URL specifies any information on Internet by using four thing as shown in Fig. 7.16.2(a). They are as follows :
- | | |
|-----------------------|------------------|
| 1. Method or protocol | 2. Host computer |
| 3. Port | 4. Path. |



(G-666) Fig. 7.16.2(a) : URL

- Method is the protocol used such as FTP, HTTP which helps retrieving the desired information. Host is the computer where the required information is located. The name of the computer begins with www but this is not mandatory.
- URL can optionally contain the server's port number. If the port is to be included then it should be inserted between host and path and it should be separated by a colon, as shown in Fig. 7.16.2(a).
- Path is the name of the file where the information is located. The port and path fields are separated from each other by a slash.
- Version : The latest version of HTTP is 1.1 but the versions 0.9 and 1 are also used.
- The example of URL is shown in Fig. 7.16.2(b). Note that the port is not included.



(G-1969) Fig. 7.16.2(b) : Example of URL

7.16.3 Cookies : User-Server Interaction :

- We know that the HTTP servers are stateless. The disadvantage of being stateless is that the server cannot identify the client. The meaning of statelessness is that the client server relationship gets over as soon as their communication terminates.
- But the advantage of statelessness is that the server design is simplified to a great extent and it permits the engineers to develop high performance web servers which can handle thousands of TCP connections at a time.
- But many a times it is necessary for a web site to identify users. In such cases HTTP uses cookies.
- Cookies are defined in RFC 2109 and they allow sites to keep track of users.
- Cookies are not used by all the sites but some of the prominent sites that use cookies are : Yahoo, Amazon etc.



Components of cookie technology :

- Following are the four components of the cookie technology.
 - A cookie header line in HTTP response message.
 - A cookie header line in the HTTP request message.
 - A cookie file kept on the user's end system and managed by user's browser.
 - A back end database at web site.

Operating principle :

- If a new user X contacts a site (that uses cookies) for the first time, then that web site creates a unique identification number for this new user and then creates an entry in its back end data base. This entry is associated with the identification number of user X.
 - The server will then respond to X's browser by including the header set-cookies : header, in the HTTP response number of user X.
- For example the header line can be :

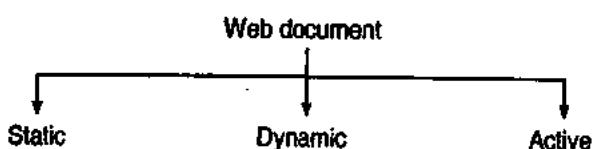
Set-cookie : 1 2 3 4 5 6 7

Where, 1 2 3 4 5 6 7 is the identification number.

- When X's browser receives the HTTP response message, it reads the set cookie : header.
- The browser then appends a line to the special cookie file which is managed by the browser. This line will include the hostname of the server and the identification number 1 2 3 4 5 6 7.
- Next time when X visits this same site again, his browser will include the same identification number in each of his HTTP request.
- Thus it is now possible for the web site to track X's activities.
- It is then possible to know the areas of interest of X, which pages does he visit and at what time etc.
- Cookies simplify the internet shopping to a great extent but they remain highly controversial because they are thought as invasion in users privacy.
- It is possible to use cookies to gather personal information about X across a large number of websites.

7.17 Web Documents :

- The web documents can be classified into three categories as shown in Fig. 7.17.1.



(G-66) Fig. 7.17.1 : Categories of web documents

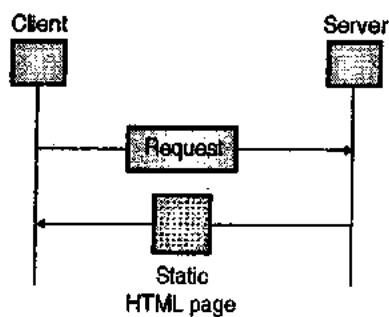
7.17.1 Static Documents :

SPPU : Dec. 09

University Questions

- Q.1 What is WWW ? How it works ? What is the difference between static and dynamic web pages ?
(Dec. 09, 9 Marks)

- The contents of static documents are fixed. These contents are created and stored in a server. If required the client can get a copy of static document.
- The contents of the static document are determined when it is created. These contents cannot be changed when the static document is being used.
- It is possible to change the contents of static document at the server but the user cannot change them. The user can display the static document by using a browser as shown in Fig. 7.17.2.



(G-66) Fig. 7.17.2 : Static document

7.17.2 HTML (Hypertext Markup Language) :

SPPU : May 11

University Questions

- Q.1 How do you make an image clickable in HTML ? Give an example.
(May 11, 6 Marks)

- The web pages are created by using a language called HTML. It uses certain marks to format the text. For example if a part of text is required to be "boldface" then we can use the beginning and ending bold face tags (marks) in the text as shown below :
 - - Beginning of boldface
 - - End of boldface.
- Here and are the instructions for the browser. The browser will make the part of the text between these tags bold. HTML lets the user to use only ASCII characters for the main text as well as for formatting instructions.
- So every computer can receive the whole document as an ASCII document. The formatting instructions are used by the browser to format the data.

7.17.3 Dynamic Document :

SPPU : Dec. 09

University Questions

- Q.1 What is WWW ? How it works ? What is the difference between static and dynamic web pages ?
(Dec. 09, 9 Marks)

- The dynamic documents are not present in a predefined format, like static documents. A dynamic document is created by a web server on the request for the document from a browser.



- Refer Fig. 7.17.3 to understand how a dynamic document is created and passed on to the client.
- First the client sends a request to the web server. After receiving this request, the web server will execute an application program to create a dynamic document.
- The server returns the dynamic document as a response of the request to the client.
- The contents of a dynamic document will be different corresponding to every request. A simple example of a dynamic document is to get time and data from the server.
- A server follows the steps given below to handle dynamic documents :
 1. The server checks the URL in order to find if it has defined a dynamic document.
 2. If the URL has defined the dynamic document, then the server executes the program.
 3. The output of this program is the dynamic document. It is returned back to the client.

7.17.4 Common Gateway Interface (CGI) :

- CGI is the name of a technology which creates the dynamic documents and handles them too.
- CGI is in fact a set of standards. It defines the way in which a dynamic document should be written, the way in which input data be supplied to the program and how the output result be used.

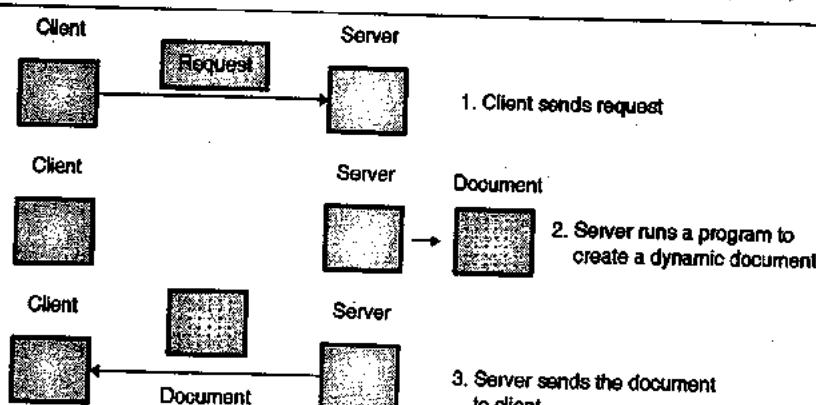
- Note that CGI is not a new language. It allows the user to use the existing languages such as C, C++, Perl etc. However CGI defines rules and terms which are to be followed by the programmers.
- The word **common** in CGI shows that this standard defines some rules which are commonly applicable to any language or platform.
- The word **gateway** indicates that a CGI program is gateway for accessing other resources such as databases and graphic packages.
- Lastly the word **interface** in CGI indicates the presence of a set of terms, calls and variables which can be used in any CGI program.

CGI Program :

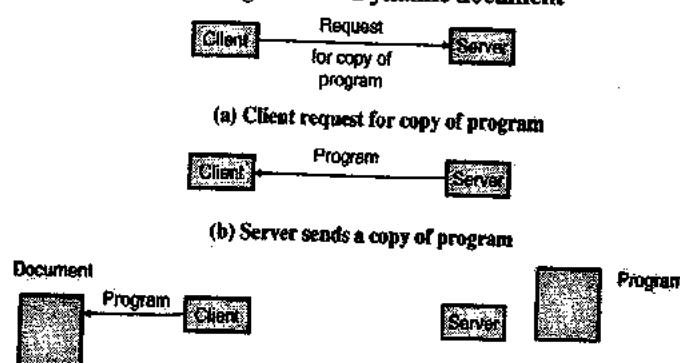
It is a code which is written in one of the languages that supports CGI (such as C, C++, etc.).

7.17.5 Active Documents :

- Active document can be defined as the program, that is needed to be run at the client side.
- The examples of active documents are the programs creating animated graphics on the screen or the ones which help interaction with the user.
- Refer Fig. 7.17.4 to understand this concept. It shows that whenever a browser requests for an active document, the server will send a copy of document in the form of byte code. The active document will then be run at the browser (client) site.



(G-670) Fig. 7.17.3 : Dynamic document



(G-671) Fig. 7.17.4 : Active document

- The server stores the active document in the form of a binary code. The active document is stored on the server but it is not run on the server.
- The client receives the document and stores it, and can run it as many times as required without repeating the request.
- The server sends the active document to the client in the binary form. So it is possible to compress it at the server's site and then decompress it at the client's site.
- This will save the bandwidth as well as the transmission time.

Steps in creation of an active document :

Refer Fig. 7.17.4 to understand the creation, compilation and execution of an active document.

- At the server, a program is written in source code and stored in a file.
- Then the program is compiled and binary code is created and stored in a file at the server's site.
- A client (browser) requests for a copy of program as shown in Fig. 7.17.4(a). This program is transported from the server to the client in the compressed form.
- The client converts the received program from binary code into executable code using its own software.
- The client runs the program to create the desired result which can include animation or interaction with the user.

7.18 HTTP (Hypertext Transfer Protocol) :

SPPU : Dec. 11

University Questions

- Q. 1** State which transport layer protocol is used by the following protocols: HTTP, FTP, DHCP, DNS, ICMP, TFTP, IP, SMTP. (Dec. 11, 4 Marks)

- The main function of HTTP is to access data on WWW. This protocol can access the data in various forms such as plaintext, hypertext, audio, video etc.,
- The function of HTTP is equivalent to a combination of FTP and SMTP. It uses services of TCP. It uses only one TCP connection (port 80). There is no separate control connection like the one in FTP. Only the data transfer takes place between the client and the server so there is only one connection and it is the data connection.
- The data transfer in HTTP is similar to SMTP. The format of the messages is controlled by MIME like headers.

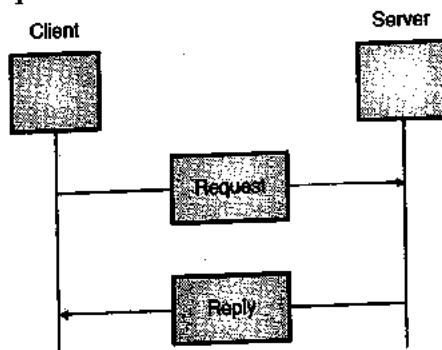
7.18.1 Principle of HTTP Operation :

SPPU : May 13

University Questions

- Q. 1** Compare file transfer using FTP and HTTP methods. (May 13, 8 Marks)

- The principle of HTTP is simple. A client sends a request. The server sends a response. The request and response messages carry data in the form of a letter with a MIME like format.
- Fig. 7.18.1 shows the HTTP transactions between client and server.
- The client initializes the transaction by sending a request message and the server responds by sending a response.



(G-65) Fig. 7.18.1 : HTTP transaction

7.18.2 The Web and HTTP :

SPPU : May 13

University Questions

- Q. 1** Compare file transfer using FTP and HTTP methods. (May 13, 8 Marks)

- HTTP is the Web's application layer protocol. It is the heart of the Web. It has been defined in [RFC 1945] and [RFC 2616].
- HTTP is implemented in two programs :
 - A client's program.
 - A server's program.
- These programs are executed on different systems and talk to each other by exchanging HTTP messages.
- HTTP defines how Web clients such as browsers request Web pages from Web servers and how servers transfer Web pages to clients.
- HTTP uses TCP as its underlying transport protocol (rather than using UDP).
- The HTTP client first initiates a TCP connection with the server. After establishing a connection, the browser and the server process access TCP through their socket interface.
- TCP provides a reliable data transfer service to HTTP. That means each HTTP request message, transmitted by a client will eventually arrive intact at the server.
- Similarly each HTTP response message transmitted by the server will eventually arrive intact at the client, due to the reliable TCP connection.
- Due to this kind of layered architecture HTTP need not have to worry about the lost data or about the details of how TCP deals with the loss and retransmission of data. It is managed by TCP.

**Statelessness :**

- In HTTP, the server sends the files requested to the client without storing any state information about the client.
- So it may happen that the same client may ask the same information repeatedly to the server and the server would not even understand it. So it will keep resending those files.
- As the HTTP servers does not maintain any information about the state of client it is called as a stateless protocol.

7.18.3 Non-persistent and Persistent Connection :

SPPU : Dec. 11, Feb. 16

University Questions

- Q. 1** What is the difference between persistent and non-persistent HTTP? Also explain HTTP message format. (Dec. 11, 5 Marks, Feb. 16, 4 Marks)

- HTTP is capable of using both non-persistent and persistent connections. HTTP uses persistent connection in its default mode. But HTTP clients and servers can be configured to use the non-persistent connection as well.

1. Non-persistent connections :

- Let us discuss the step-by-step procedure followed for transferring a web page from server to client for a non-persistent connection.
- Imagine that the web page consists of a base HTML file and many JPEG images and that all these objects reside on the same server.
- Let the URL for the base HTML file be as follows :
http://www.vit.edu/itdept/home.index

- Then the sequence of events is as follows :

1. The HTTP client process initiates a TCP connection to the server www.vit.edu on port number 80, which is the default port number for HTTP.
2. The HTTP client, sends an HTTP request message to the server via its socket associated with the TCP connection. This request message is of the following format :

Path name/itdept/home.index.

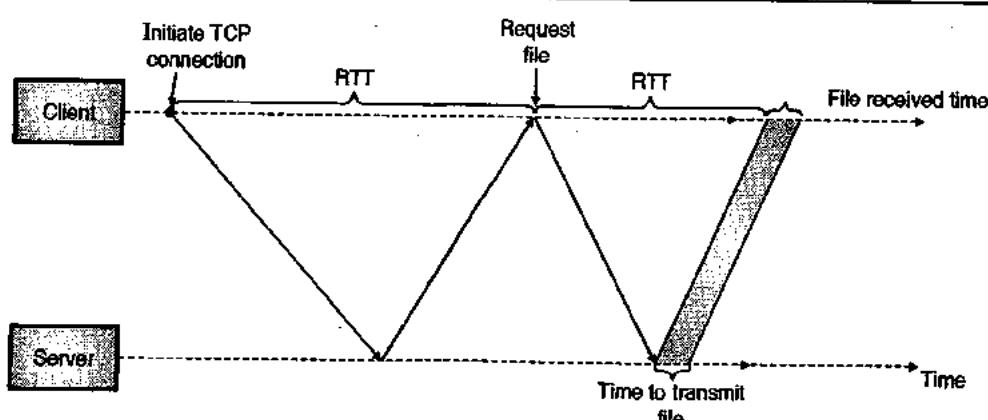
3. The HTTP server process receives the request message via its socket associated with the connection. It then retrieves the object.
/itdept/home.index
from its storage. It then encapsulates this retrieved object in an HTTP response message and sends the response message to the client via its socket.
4. The HTTP server process tells TCP to close the TCP connection.
5. As soon as the HTTP client receives the response message, the TCP connection is terminated.
6. The response message indicates that the encapsulated object is an HTML file. The client takes out the file from the response message and examines the HTML file. The client will find references to all the JPEG objects.
7. The client follows the first four steps for each JPEG object.
- As the browser receives the web page, it displays the page. Different browsers can display the same web page differently. However HTTP is not concerned about this. Its specifications define only the communication between the HTTP client program and HTTP server program.
- The steps discussed earlier were for the non-persistent connection where each TCP connection is closed after the server sends the object. That means the TCP connection does not persist for other objects.
- Each TCP connection transports one request message and one response message.

Round-Trip Time (RTT) :

The RTT is defined as the time taken by a small packet to travel from client to server and then back to the client.

The components of RTT are :

1. Packet propagation delays
 2. Packet queuing delays
 3. Packet processing delays.
- Now consider the sequence of events taking place when a user clicks on a hyperlink. These events are illustrated in Fig. 7.18.2.



(G-658) Fig. 7.18.2



1. The browser initiates a TCP connection between the browser and web server. This process makes use of a **three way handshake**.

In the three way handshake, the client sends a small TCP segment to the web server. The server acknowledges and responds with another small TCP segment. Finally the client acknowledges back to the server.

2. After completing the first two parts of the three way handshake the client sends the HTTP request message to the server.
3. In response the server sends the HTML file to the client. The total response time as shown in Fig. 7.18.2 is equal to 2RTT plus the time taken by the server to transmit the file.

Disadvantages of non-persistent connections :

1. It is necessary to establish and maintain a new connection for each requested object.
2. For each connection TCP buffers need to be allocated and TCP variables need to be kept in both the client and server.
3. There is a delay of 2RTTs associated with the transfer of each object.

Persistent connection :

- The disadvantages of non-persistent connections can be overcome if persistent connection is used.
- With the persistent connection, the server leaves the TCP connection open after sending a response. All the requests and responses between the same client and server can be sent over the same connection.
- Hence the entire web page can be sent over a single persistent connection. It is also possible to send the multiple web pages residing on the same server to the same client over a single persistent TCP connection.
- The TCP connection is closed only after the time out interval by the HTTP server.

Types of persistent connections :

- The two versions of persistent connections are as follows :
 1. Without pipelining
 2. With pipelining.

1. **Without pipelining** : For this version, the client has to issue a new request only when it receives the previous response. The delay of only one RTT is experienced by the client in order to request and receive each object. This is an improvement over the non-persistent connection which experiences a delay of 2RTT. This delay can be reduced by using pipelining.

Another disadvantage of no pipelining is that the TCP connection becomes idle i.e. does nothing while it waits for another request after the server had sent an object.

2. **With pipelining** : This mode reduces the delay further. The default mode of HTTP uses persistent connection. With pipelining the HTTP client will issue a request as soon as it encounters a reference.

This allows the HTTP to make back to back requests. It can make a new request before receiving the response. When the server receives back to back requests, it sends the objects back to back.

With pipelining only one RTT will be expended for all the referenced objects. Another advantage is that the pipelined TCP connection remains idle for a very short time.

7.18.4 HTTP Messages :

- The HTTP messages are of two types :
 1. Request message
 2. Response message.
- The format of both these messages is almost the same.

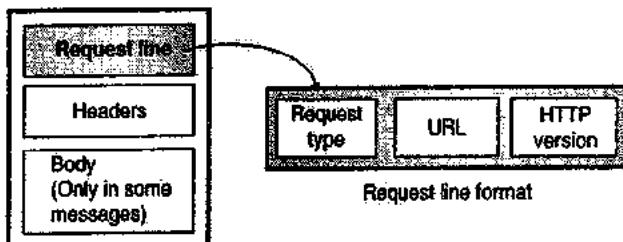
7.18.5 Request Message :

SPPU : Dec. 11, Feb. 16

University Questions

Q. 1 What is the difference between persistent and non-persistent HTTP ? Also explain HTTP message format (Dec. 11, 8 Marks, Feb. 16, 4 Marks)

- Fig. 7.18.3(a) shows the format of the request message. It consists of a request line, headers and sometimes a body.



(G-65) Fig. 7.18.3(a) : HTTP request message

1. Request line :

- The request line is used for defining the request type, resource (URL) and HTTP version as shown in Fig. 7.18.3(a).
- **Request type** : Several request types are defined.
- **Uniform Resource Locator (URL)** : The client accessing a web page needs an address. The HTTP uses the URL to facilitate the access of any document distributed over the world. The URL defines four thing as shown in Fig. 7.18.3(b). They are as follows :
 1. Method
 2. Host computer
 3. Port
 4. Path.



(G-66) Fig. 7.18.3(b) : URL

- Method is the protocol used such as FTP, HTTP. Host is the computer where the required information is located. The name of the computer begins with www but this is not mandatory.
- URL can optionally contain the server's port number. If the port is included then it should be inserted between host and path and it should be separated by a colon.

- Path is the name of the file where the information is located.
- Version : The latest version of HTTP is 1.1 but the versions 0.9 and 1 are also used.
- The example of URL is shown in Fig. 7.18.3(c).

http : // www.w4.org / hypertext / WWW / Project.html.
 Method Host Path

(G-1969) Fig. 7.18.3(c) : Example of URL

7.18.6 Methods (Request Type) : SPPU : May 12

University Questions

Q.1 State and explain any three HTTP methods.

(May 12, 8 Marks)

- This is one of the fields in the request line format. It defines different types of messages referred to as request types or methods.
- The request method is a command or request issued by the client to the server.
- Following are some of the important methods (request types).

1. GET :

The client uses this method for retrieving a document from the server. The address from where this document is to be obtained is defined in the URL.

2. HEAD :

The client uses this method in order to obtain some information about a document but not the document itself.

3. POST :

This method is used when the client wants to provide some information to the server.

4. PUT :

This is used by the client for providing a new or replacement document to be stored on the server.

5. PATCH :

This method is similar to PUT. But there is one change. The patch request contains a list of differences which should be implemented in the existing file.

6. COPY :

This method is used to copy a file to another location.

7. MOVE :

This method is used for moving a file to another location.

8. DELETE :

It is used for removing a document on the server.

9. LINK :

It is used for creating a link or a link from a document to another location. The location of the file is specified in the URL request line and the location of destination is specified in the entity header.

10. UNLINK :

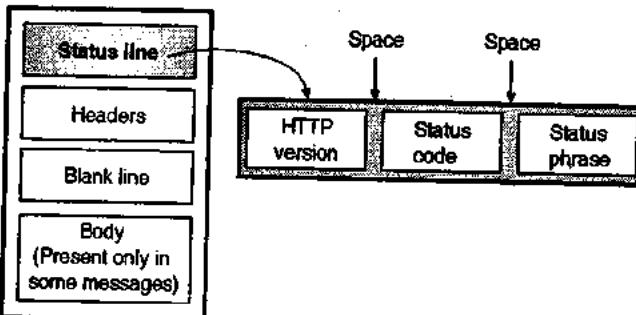
It is used for deleting the links created by the LINK method.

11. OPTION :

It is used by the client to ask the server about various options that are available.

7.18.7 Response Message :

- Fig. 7.18.4(a) shows the format of the response message. A response message is made of a status line, a header and sometimes a body.



(a) Response message

(b) Status line format

(G-662) Fig. 7.18.4

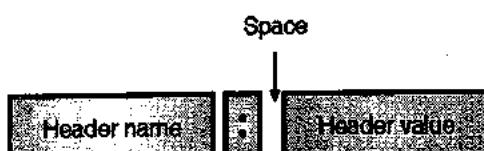
Status line :

The status line is used for defining the status of the response message. As shown in Fig. 7.18.4(b) it consists of HTTP version, status code and status phrases with spaces in between.

- **HTTP Version :** This field indicates the version of HTTP being used. This field is same as the HTTP version field used in the request line.
- **Status Code :** It is a three digit field which is similar to those in FTP and SMTP protocols.
- **Status Phrase :** It is used for explaining the status code in the text form.

7.18.8 Headers :

- Headers in the response message are used for exchanging additional information between the client and server.
- The header can be a one liner or multiple lines. The format of a header line is shown in Fig. 7.18.5 which shows that it consists of a header name, a colon, a space and a header value.



(G-63) Fig. 7.18.5 : Header format

- A header line can be of one of the following four types :
 1. General header
 2. Request header
 3. Response header and
 4. Entity header.
 - A request message can contain only general, request and entity headers but a response message can contain only general response and entity headers.
 - The comparison of request message and response message is shown in Fig. 7.18.6. The common headers and different headers have been indicated clearly.
1. **General header** : It is meant to provide general information about the message. It is present in request message as well as response message as shown in Fig. 7.18.6.
 2. **Request header** : It can be present only in the request message. The client's configuration and the client's preferred file format are specified using the request header.
 3. **Response header** : It can be present only in the response message. The server's configuration can be specified using the response header.
 4. **Entity header** : The information about the body of the document is provided by the entity header. It can be present in the request message as well as the response message as shown in Fig. 7.18.6.

7.18.9 Comparison of HTTP and SMTP :

SPPU : May 06, Dec. 12

University Questions	
Q. 1	Compare HTTP and SMTP. (May 06, 6 Marks)
Q. 2	Compare file transfer using SMTP and HTTP methods. (Dec. 12, 8 Marks)

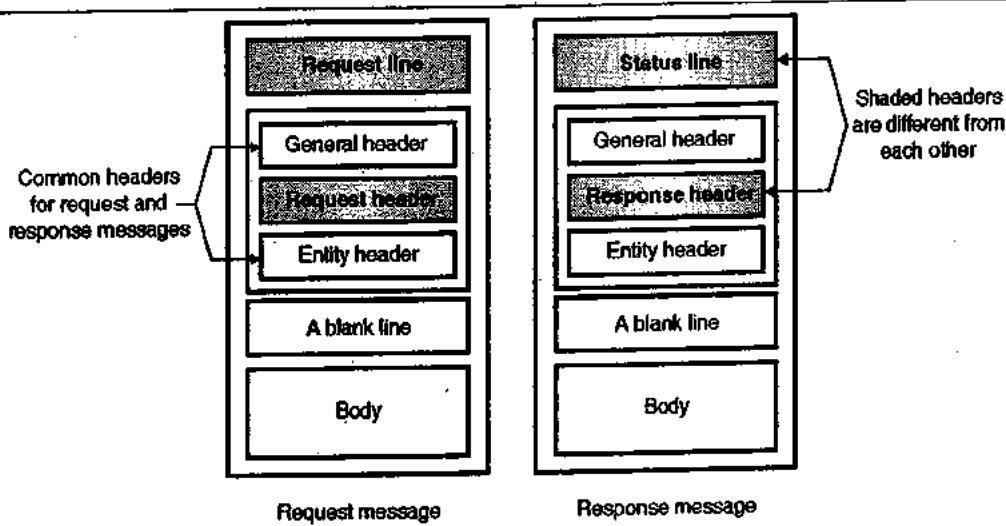
Sr. No.	SMTP	HTTP
1.	Message is transferred from client to server or the other way round.	Message transfer is from client to server or the other way round.
2.	Uses TCP.	Uses TCP.
3.	Uses port 25 for transmission.	Uses port 80 for transmission.
4.	SMTP messages are to be read by humans.	HTTP messages are to be read and understood by the HTTP servers and HTTP clients.
5.	These messages are first stored and then forwarded.	These messages are immediately delivered.

7.19 Proxy Server :

SPPU : May 12, Dec. 13, May 15

University Questions	
Q. 1	Explain in brief functionality of DHCP server, Proxy server, Mail server. (May 12, 8 Marks)
Q. 2	Explain functionality of Proxy server. (Dec. 13, May 15, 2 Marks)

- All the servers cannot speak HTTP some of them use the FTP, Gopher or some other protocols.
- A large information is available on FTP and Gopher servers so it should be made available to web users.
- To do so, one solution can be to have a browser which can use the HTTP as well as FTP, Gopher and other protocols. But this makes the browser unnecessarily large.



(G-64) Fig. 7.18.6 : Comparison of request message and response message



- The other solution to this problem is proxy server, shown in Fig. 7.19.1.
- Proxy server is basically a gateway which communicates using HTTP to the browser FTP, Gopher or some other protocol for communicating to the server.
- It receives HTTP requests from a browser, converts them in FTP or Gopher requests and sends them to the FTP/Gopher server as shown in Fig. 7.19.1.
- Proxy server can be a program running on the same machine working as a browser or it can be a separate machine.
- The users can configure their browsers with proxies for those protocols which the browser does not use for communication.
- The other important feature of a proxy server is caching. A caching proxy server collects and stores all the pages which pass through it.
- When a user asks for a page, the proxy server will first see if it has the page stored with it. If the page is there then it will see if the page is upto date.
- If the page is updated then, it passes the page to the user otherwise it will fetch a new copy of the page.
- A proxy server can be put inside a firewall. The user can access the web but he is not allowed the full Internet access.
- In such situation the user talks to the proxy server and the server communicates with obtains different sites and obtains pages on behalf of the user.

7.20 Performance Enhancement :

- The users of world wide web are increasing in an exponential manner therefore, the servers, routers and lines are frequently overloaded and the user has to wait for a longer time.
- To reduce this endless delay researchers have developed various techniques for improving the performance. Some of these techniques are :
 - caching
 - server replication
 - content delivery network.

7.20.1 Content Delivery Networks :

- Companies called CDNs (content delivery networks) talk to content providers such as music sites, newspapers etc. and offer to deliver them to end users by charging fees.
- After signing the contract the content owner gives the CDN the contents of its website for preprocessing and distribution.
- After this, the CDN talks to large number of ISPs and offers to pay them if they grant a permission to place a remotely managed server having valuable contents on their LANs.
- The contents replicated at various sites worldwide, the performance is likely to improve to a great extent.

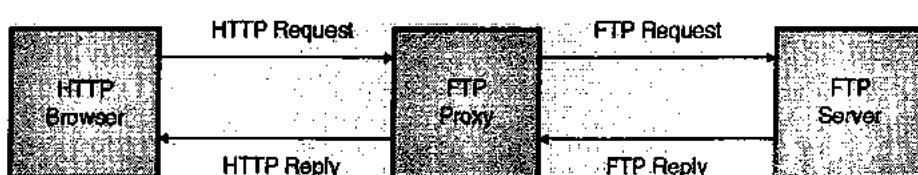
7.20.2 DNS Records (Resource Records) :

SPPU : May 10, Dec. 11

University Questions

- Q. 1** Explain in detail principle DNS resource record types. (May 10, 8 Marks)
- Q. 2** What is DNS ? Explain its various resources records with one example. (Dec. 11, 8 Marks)

- The DNS servers which implement the DNS distributed database together, store resource records (RR), including RR that provide hostname-to-IP-address mapping.
- Each DNS reply message carries one or more resource records with it.
- A resource record is a four tuple which contains the following fields :
 - Name
 - Value
 - Type
 - TTL
- TTL is the time to live resource record. It determines the time for which the source record is to be kept in a cache.
- The meaning of Name and Value will be dependent on Type as explained below.



(G-65) Fig. 7.19.1 : Proxy server



1. If Type = A :

For type A, the Name is a hostname and value is the IP address of the hostname. Thus type A record provides the standard hostname to IP address mapping.

2. If Type = NS :

For type NS, the Name is a domain and value is the hostname of an authoritative DNS server. This server knows how to obtain the IP address for hosts in the domain. This record is used for routing DNS queries further along in the query chain.

3. If Type = CNAME :

For type CNAME, the value is a canonical hostname for the alias hostname Name.

4. If Type = MX :

For type MX, the value is the canonical name of the mail server that has an alias name.

If DNS server is authoritative for a particular hostname, then the DNS server will keep a type A record for the hostname.

But if the DNS server is not authoritative for a hostname, then the server will keep a type NS record for the domain that includes the hostname. It will also keep a type A record to provide the IP address of the DNS server in the value field of the NS record.

7.21 P2P File Sharing :

- P2P means process to process file sharing.
- The P2P file sharing is the most important Internet application because the highest amount of Internet traffic, corresponds to the P2P file sharing.
- Modern P2P file sharing system shares MP3 (3 to 8 M bytes), videos (10 to 1,000 M bytes), images, software documents etc.
- In this section, we will discuss the protocols and networking issues in P2P file sharing.
- Before going into details of P2P file sharing system, let us take an example. Suppose Rahul uses the P2P file sharing application for MP3 downloading. He runs the P2P file sharing software on his home PC (peer). He uses an ADSL connection to access the Internet. He shuts down his PC every night and does not have a hostname. So everytime he connects to the Internet the ISP will assign a new IP address to his PC.
- Suppose that Rahul is connected to the Internet and searching for the MP3 for a particular song of a particular artist.
- As soon as he goes into search, the P2P application displays a list of those peers who are currently connected to the Internet and have a copy of that song, for sharing.
- Each one of them is an ordinary PC owned by an ordinary Internet user like Rahul.
- Rahul then requests the required MP3 file from one of the peers say Preeti's PC. Then a direct TCP connection gets established between Rahul and

Preeti's PC and the MP3 file is sent from Preeti's PC to Rahul's PC.

- If Preeti disconnects her PC from the Internet in the middle of this download, then Rahul's P2P file sharing software may attempt the remaining part of the MP3 file from the other peer.
- Also when the download from Preeti to Rahul is going on, some other user can download some other song from Rahul's PC.
- Thus the P2P file sharing allows direct sharing of information without any independent server getting involved. However P2P file sharing operates on the client server principle. The requesting person acts as a client and the requested user acts as the server. The file is sent using the file transfer protocol (FTP).
- In P2P file sharing system, typically a large number of users are connected to Internet and each user has objects such as MP3, videos, software and images for sharing.

7.22 Remote Login : TELNET and SSH :

- The Internet and TCP/IP suite have been designed primarily to provide service to its users. The requirements of different users will be of different types and with increase in the number of users, the number of diversified demands will also be very large. It is practically impossible to write a specific client - server program for each demand.
- Therefore a general purpose client - server program should be developed which will help a user to access any application on a remote computer. That means a user will be allowed to log into a remote computer.
- Two of such general purpose client - server programs which allow remote login are : TELNET and SSH.

7.22.1 TELNET :

SPPU : May 08

University Questions

Q. 1 Write short notes on TELNET. (May 08, 6 Marks)

- The long form of TELNET is TTerminal NETwork. It was proposed by ISO as a standard TCP/IP protocol for a virtual terminal service.
- TELNET enables a user to establish a connection to a remote system.

Concepts related to TELNET :

- Some of the important concepts related to TELNET are as follows :
 1. Time sharing environment.
 2. Login : Local or Remote.
 3. Network Virtual Terminal.



Time sharing Environment :

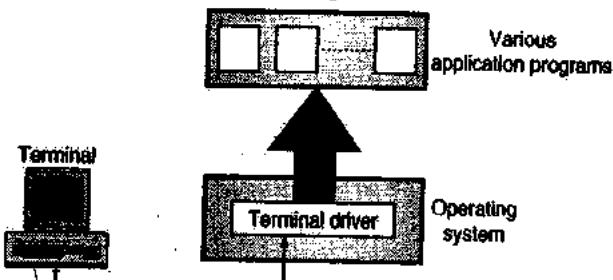
- TELNET was designed during those days when almost all the operating systems were operating on the time - sharing principle.
- In the time sharing environment there is a large central computer which supports all the users.
- All the processing is done by the central computer, and each user feels that it is a dedicated computer. The users can access all the common system resources, use all the programs or switch from one program to the other.

Login :

- In a system based on time sharing, every user must have an identification and a password for his authentication. Whenever a user wants to access the system he will log into the system with his user id and password. The system will check the password to allow only the authorised users to access the resources.
- The logic can be one of the following two types :
 1. Local login.
 2. Remote login.

1. Local login :

- The user login into a local time sharing system is called as local login. Fig. 7.22.1 illustrates the principle of local login.



(G-1793) Fig. 7.22.1 : Local login

- The local login takes place in a step - by - step manner as follows :
 1. The user types at the keyboard of a terminal.

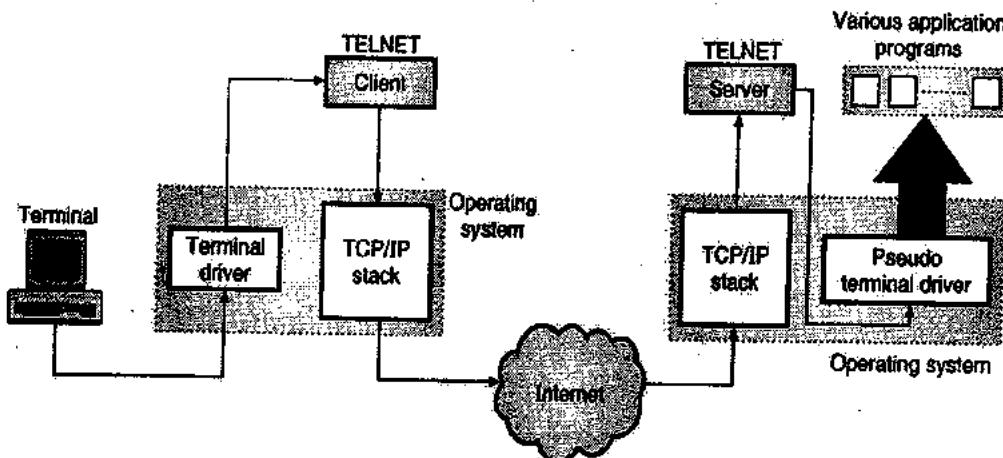
2. The terminal driver accepts these keystrokes.
3. It converts the keystrokes to characters.
4. It passes the characters to operating system.
5. The O.S. understands the combination of characters.
6. It allows access of intended application to the user.

2. Remote Login :

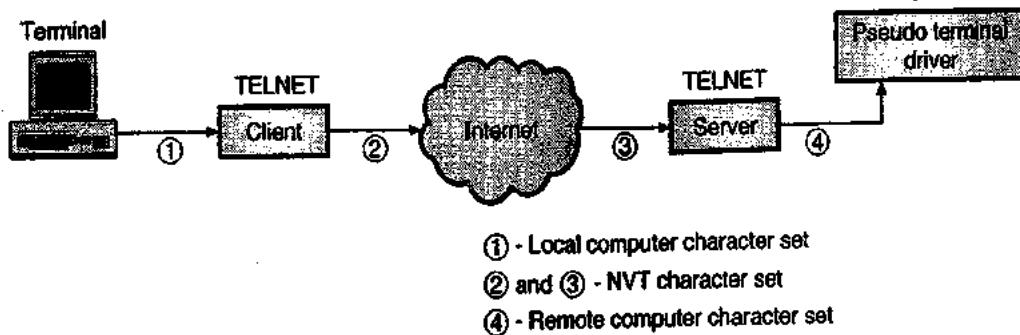
The user will have to go for the remote login process when he wants to access an application program residing on a remote computer. He can do it using the TELNET client and server programs. Fig. 7.22.2 illustrates the principle of remote login.

Remote login takes place in a step-by-step manner as follows :

1. The user types at the keyboard of a terminal.
2. The terminal driver at local O.S. accepts the characters but sends them to TELNET client without interpreting them.
3. TELNET client converts them into NVT characters. NVT is Network Virtual Terminal. This is a universal character set.
4. NVT characters are delivered to TCP/IP stack (local).
5. The NVT characters travel on the Internet and reach the TCP/IP stack of the remote machine.
6. The NVT characters are applied to the TELNET server which converts them appropriately so that the remote computer can understand them.
7. These characters are applied to a software called pseudo terminal driver.
8. The O.S. at the remote machine then passes the character to the intended application.



(G-1794) Fig. 7.22.2 : Principle of remote login



(G-1795) Fig. 7.22.3 : Concept of NVT

7.22.2 Network Virtual Terminal (NVT) :

- NVT.character set is a universal interface defined by TELNET in order to ensure that a user can access any remote computer in this world.
- Fig. 7.22.3 illustrates the concept of NVT.
- The local computer character set is used for the communication between the user terminal and TELNET client.
- Then between the TELNET client and TELNET server the communication takes place using the NVT character set.
- And finally the remote computer character set is used for the communication between the TELNET server and the pseudo terminal driver as shown in Fig. 7.22.3.
- NVT has two sets of characters. One set is for the data and the other set is for control. Both have 8 bit characters.

7.22.3 Security Problems of TELNET :

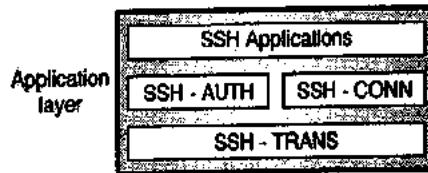
- TELNET is not a very secured system. It needs username and password for logging in. But it is not enough.
- A snooper software would be enough to capture the login name and password even if they are encrypted.

7.22.4 Secure Shell (SSH) :

- Secure Shell or SSH is another popular remote login application program. The underlying transport program for SSH is TCP. This is similar to TELNET.
- However SSH has two advantages over TELNET :
 1. It is more secured than TELNET.
 2. It provides more services.
- There are two versions of SSH namely SSH₁ and SSH₂, out of which SSH₂ is being used. We will discuss SSH₂ in this section. Note that these two versions are not compatible to each other.

SSH Components :

- This is a proposed application layer protocol and as shown in Fig. 7.22.4, it has four components.



(G-1796) Fig. 7.22.4 : SSH components

- The four SSH components are :



1. SSH - TRANS :

- The long form is SSH – Transport Layer Protocol. TCP is not a secured protocol, therefore SSH makes use of a protocol which creates a secured channel on top of TCP.
- This new secured channel is an independent protocol called SSH – TRANS.
- When SSH is used, the client and server will first establish an unsecured TCP connection and then develop a secured layer over this by exchanging various security parameters.
- The SSH – TRANS protocol provides the following services :
 1. Confidentiality of the messages.
 2. Data integrity of the exchanged messages.
 3. Authentication of the server.
 4. Message compression.

2. SSH - AUTH :

- The second component of SSH is the SSH – AUTH i.e. SSH – Authentication protocol.
- This protocol is used to authenticate the client for the server after establishing a secure channel between client and the server.

3. SSH - CONN :

- The third component of SSH is SSH – CONN i.e. SSH connection protocol.
- This piece of software is called for by the SSH once a secure connections has been established and authentication done.



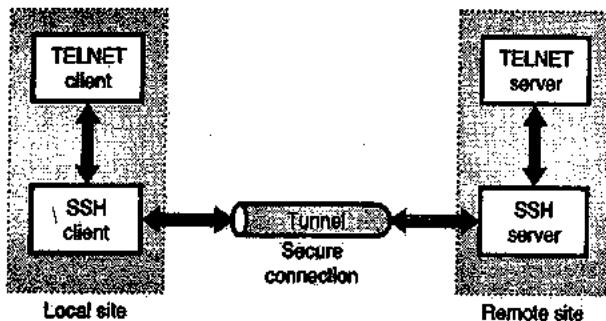
- SSH – CONN performs the multiplexing as one of its services. It allows the client to create multiple logical channel over the secure channel established between the client and the server.

4. SSH – Applications :

- As soon as the connection establishment, authentication etc. is complete, the SSH connection can be used by multiple applications.
- Each application can create its own logical channel and make use of secure SSH connection. In addition to the remote login, the other applications that make use of SSH are : file transfer application. That is called as secure file transfer.

7.22.5 Port Forwarding :

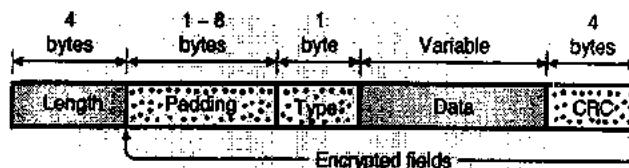
- Port forwarding is one of the services provided by the SSH – protocol. The port forwarding mechanism can be used to access application programs which do not provide any security. e.g. TELNET or SMTP.
- Such application programs can use the secure channel created by SSH to create a tunnel to carry the messages as shown in Fig. 7.22.5. Therefore this mechanism is also called as SSH Tunneling.
- We can apply the port forwarding concept to change the insecure connection between TELNET client and TELNET server into a secure connection, as shown in Fig. 7.22.5.



(G-1797) Fig. 7.22.5 : Port forwarding

7.22.6 SSH Packet Format :

- The SSH packet format is as shown in Fig. 7.22.6.



(G-1798) Fig. 7.22.6 : SSH packet format

- Description of various fields are as follows :

1. Length :

This is a 4-byte long field which defines the length of the SSH packet which includes the type, the data and the CRC fields but does not include the length and the padding fields.

2. Padding :

This is a variable length field. Its length can vary from 1-byte to 8-bytes. Padding field will make the attack on security more difficult.

3. Type :

This is a 1-byte field which is used to specify the type of packet used by the SSH protocol.

4. Data :

This is a variable length field. We can obtain the length of the data field by deducting the 5-bytes from the value of the length field.

5. CRC :

This 4-bytes long field is used for error detection purpose.

7.23 Host Configuration : DHCP :

SPPU : Dec. 11

University Questions

Q. 1 State which transport layer protocol is used by the following protocols: HTTP, FTP, DHCP, DNS, ICMP, TFTP, IP, SMTP. (Dec. 11, 4 Marks)

- DHCP (Dynamic host configuration protocol) is the first client server application program that used after a host is booted.
- Thus it works as a bootstrap when the host is booted and is to be connected to the Internet, but does not know its IP address.
- A computer that makes use of the TCP/IP suite must know its IP address. Alongwith its IP address it must also know the following information :
 - Subnet mask of the computer
 - IP address of the router, so that it can communicate with other networks.
 - IP address of the name server so that it can use the names instead of addresses.
- All this information can be saved in a configuration file and accessed by computer when booting takes place. This is known as host configuration process.

7.23.1 Previously used Protocols :

- Now a days DHCP has become the formal protocol for host configuration. But the two protocols which were used earlier for the same purpose were RARP and BOOTP.
- RARP is Reverse Address Resolution Protocol and BOOTP stands for Bootstrap protocol.

7.23.2 Need for Dynamic Configuration :

- BOOTP was designed for a working environment in which each host has a permanent network connection.
- A manager creates a BOOTP configuration file in which a set of BOOTP parameters for each host has been specified.
- The file does not change sometimes for weeks because the configuration usually remains stable.



- Due to the availability of wireless networking and portable computers such as laptops and notebooks, it has become possible to move a computer from one location to another quickly and easily.
 - BOOTP is not suitable for such situations because its configuration information cannot be changed quickly. BOOTP only provides a static mapping from a host identifier to parameters for the host.
 - Moreover a manager has to access a set of parameters for each host, and then store the information in a BOOTP server configuration file - BOOTP cannot dynamically assign values to individual machines.
 - Actually, a manager must assign an IP address to each host, and must configure the server in such a way that it understands the mapping from host identifier to IP address.
 - Static parameter assignment (done by BOOTP) works well if computers remain at fixed locations and a manager has enough IP addresses so that each computer is assigned with a unique IP address.
 - However, if computers move frequently or the number of physical computers is higher than the number of available IP host addresses, static assignment is not suitable practically.
 - To understand how to manage, when the number of computers can be higher than the number of available IP addresses, consider a LAN in a college laboratory with only 24 address and number of hosts upto 254.
 - Let the laboratory has only 30 seats and the time table schedules labs at ten different times during the week to accommodate upto 300 students.
 - Let each student carry a personal notebook computer that they use in the lab. At any given time, the net can accommodate only upto 30 active computers.
 - However, because the network address can accommodate upto 254 hosts, a manager cannot assign a unique address to each computer.
 - Thus, although the number of simultaneous user has been limited by the physical connections the number of potential computers that can use the facility is high.
 - This system is inadequate if it requires a manager to change the server's configuration file before adding a new computer to the network and begin to communicate; an automated mechanism is needed.
- Thus DHCP allows the use of computers that run server software as well as computers that run client software.
 - When a computer that runs client software is shifted to a new network, it can use DHCP to obtain configuration information automatically.
 - DHCP assigns a permanent address to a nonmobile computer that run server software. This address will not change when the computer reboots.
 - To accommodate both type of computers, DHCP makes use of a client server approach.
 - When a computer boots, it will broadcasts a DHCP Request. In response a server sends a DHCP Replay. An administrator can configure a DHCP server to have two types of addresses.
 - First is the permanent address that are assigned to server computers, and second type is a pool of addresses which can be assigned on the basis of demand, when a computer boots and sends a request to DHCP. The DHCP find the configuration information by accessing its database If the database contains a specific entry for the computer then the server returns the information from the entry. However if there is no such entry exists for the computer, then the server chooses the next IP address from the pool and assigns it to the computer.

What is DHCP ?

- DHCP, as the name suggests, is a protocol used for dynamically configuring the hosts on a network, such as workstations, personal computers and printers.
- DHCP can help in assigning various types of information such as routing information, directory-services information and default web server and mail servers.
- However, the most important and commonly used information for which DHCP is used is the IP address and subnet mask information.
- DHCP was primarily designed for managing the network and the clients automatically. With DHCP, it is not necessary to configure the network and client information manually for individual hosts.
- In addition, DHCP can coexist with statically configured hosts with fixed IP addresses. DHCP can also carry out the allocation of certain configuration information to a host on a permanent basis.

This protocol provides a four point information (IP address, subnet mask, IP address of router, IP address of name server) to a diskless computer or to a computer which is booted for the first time.

It is a client / server protocol which is backward compatible to the BOOTP.

7.23.3 DHCP :

- The Dynamic Host Configuration Protocol (DHCP) was developed by IETF in order to make the configuration automatic. Thus DHCP does not require an administrator to add an entry for each computer, to the database that a server uses.
- Instead, in DHCP a mechanism is provided for any computer to join a new network and obtain an IP address automatically with no manual intervention. This is known a plug and play networking.

7.23.4 Advantages of DHCP :

The use of DHCP on a network offers the following advantages :

1. It sets free the network administrator from the duties of setting up the configuration information, such as the IP address, the subnet mask, and the routing tables, manually. The DHCP simplifies network administration by doing these tasks automatically.
2. Avoids this and the sometimes the same IP address is assigned to two different hosts. The DHCP avoids this and the consequent malfunctioning of both the hosts from happening.
3. If the DHCP was not used, then the movement of computers from one network to another requires must be reconfigured. With DHCP, you can move the computers to different subnets or networks without the need to reconfigure them. In such situations, DHCP takes care of IP address assignment and other configuration details.
4. Mobile computers, such as laptops and palmtops, can easily get connected to different networks. They don't require reconfiguration any more as they get their configuration information from the DHCP server.
5. DHCP allocates IP addresses from a pool of IP addresses. In addition, when a computer gets disconnected, its released IP address is returned to the resource pool. Therefore, the possibility of having unused IP addresses are minimized.

7.23.5 Components of DHCP :

The use of DHCP on a network requires the following three components :

1. **DHCP server** : It assigns the IP address and other information to the clients when they request for the information.
2. **DHCP client** : It communicates with the DHCP server to get the desired information regarding its configuration. This communication can take place when the computer starts. The user of the DHCP client can also initiate a DHCP client request to the DHCP server to renew its information.

3. **DHCP relay agent** : It is used to relay (forward) client requests to the DHCP server. This is required when the DHCP server is yet to assign the client an IP address. Without an IP address, a client cannot use IP routing on its own. A DHCP relay agent helps the client to communicate with the DHCP server when the client does not have an IP address.

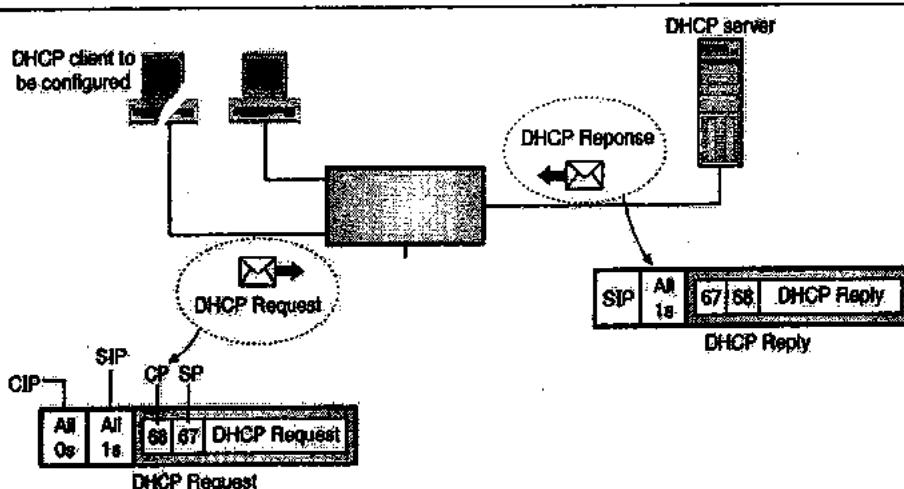
- When a client starts, it has an IP address of 0.0.0.0. It sends a broadcast message containing its MAC address and the computer name.
- In response the DHCP server sends an offer message that contains the MAC address of the client, the IP address offered to that client, the lease period for which the IP address will remain valid and its own IP address.
- The lease period is the time duration for which a client can use the IP address that has been assigned to it by the DHCP server.
- You can configure a DHCP server to set the lease time. When the client receives the IP address, it accepts the offer and then broadcasts the message that it has accepted the offer.

7.23.6 DHCP Operation :

- We will discuss the DHCP operation under two different operating conditions :
 1. DHCP client and server on the same network.
 2. DHCP client and server on different networks.

Operation on the same network :

- This situation is not a very common one. But sometimes the DHCP client and server happen to be on the same network as shown in Fig. 7.23.1.
- The operation takes place as follows :
 1. The DHCP server sends a passive open command on port 67 of UDP and waits for clients response.



(G-1789) Fig. 7.23.1 : Operation of DHCP when client and server are on the same network

2. The DHCP client sends an active open command on port 68 of UDP. This message is encapsulated in the UDP datagram with port 67 as destination port and port 68 as the source port. The UDP datagram is then encapsulated in an IP datagram. Note that the client at this time does not know its own IP address (i.e. the source address) and the server's IP address (destination address). Therefore the client uses an all zero address as source address and an all one address as destination address.
3. The server responds to this message by sending either a broadcast or a unicast message using port 67. It uses port 68 as the destination port. Broadcast address is used only for those system which do not allow the bypassing of ARP.

7.23.7 DHCP Operation on Different Networks :

- In this situation the DHCP client and server are on two entirely different networks, as shown in Fig. 7.23.2.
- In this situation a problem arises due to the broadcast nature of DHCP request. The client does not know the IP address of the server. Hence the DHCP request is a broadcast type (all 1s IP address). Any server does not allow the broadcast request to pass through it. So this request cannot reach the DHCP server.
- In order to solve this problem we can configure one of the hosts or router to operate as a relay agent as shown in Fig. 7.23.2. The relay agent knows the unicast address of the DHCP server.
- The relay will look for the broadcast request on port 67.
- As soon as it receives the broadcast request message, it encapsulates this message in a unicast datagram and sends it to the DHCP server.
- Such a unicast message is allowed to pass through by any router. Thus the request message reaches the DHCP server.

- The DHCP server sends its reply to the relay agent which in turn sends it to the DHCP client.

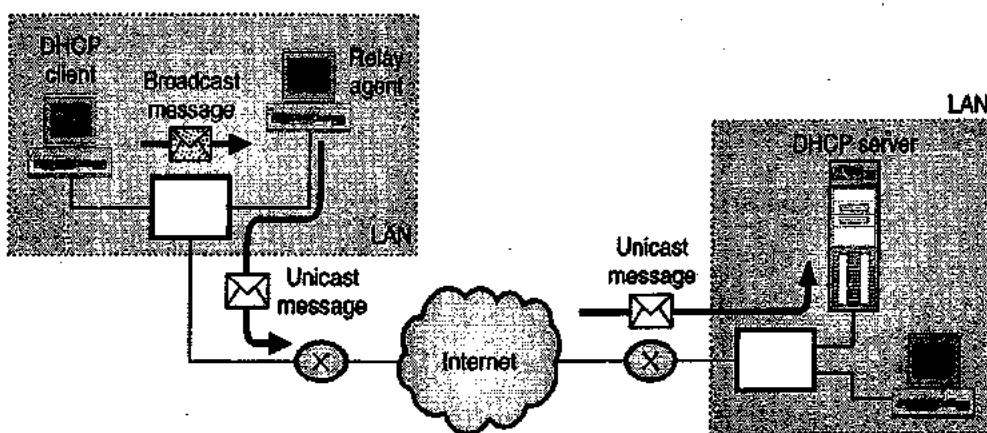
Note : In Fig. 7.23.2 only the message between the relay agent and client is of broadcast type. All the other messages are unicast types.

7.23.8 Error Control :

- DHCP can use either UDP (as discussed) or TFTP. Note that UDP does not provide any error control. Then what should be done if a request is lost or damaged ? OR if the reply is damaged ?
- As UDP does not provide any error control, the DHCP should provide it. Two strategies could be used to achieve the goal of error control :
 1. Ask UDP to use checksum. The UDP has an option of using the checksum.
 2. Ask DHCP client to use timers alongwith the retransmission policy if DHCP request or reply gets damaged or lost.

7.23.9 Optimizations in DHCP :

- The DHCP protocol has following steps :
- The first step is that a computer broadcasts a DHCP discover message in order to find DHCP server, and the other step is that the computer selects one of the available DHCP servers that responds to its message and sends a request to that server.
- To avoid a situation in which a computer follows both steps each time it boots or each time it needs to extend the lease, DHCP uses caching.
- When a computer discovers a DHCP server, the computer saves the address of that server in a cache on permanent storage (e.g. a disk file).
- Similarly, once an IP address has been allotted to it the computer saves the IP address in a cache. When a computer reboots, it uses the cached information to revalidate its former address. Doing so saves time and reduces network traffic.



(G-1790) Fig. 7.23.2 : DHCP operation when client and server are on different networks



7.23.10 DHCP Message Format :

- As Fig. 7.23.3 illustrates, DHCP uses the BOOTP message format, but modifies the contents and meanings of some fields.

OP	HTYPE	HLEN	HOPS
TRANSACTION ID			
SECONDS		FLAGS	
CLIENT IP ADDRESS			
YOUR IP ADDRESS			
GATEWAY IP ADDRESS			
ROUTER IP ADDRESS			
CLIENT HARDWARE ADDRESS (16 BYTES)			
SERVER NAME (64 BYTES)			
BOOT FILE NAME (128 BYTES)			
OPTIONS (VARIABLE LENGTH)			

Fig. 7.23.3 : The format of a DHCP message

- As shown in Fig. 7.23.3 majority of the fields in a DHCP message are same as the two fields in a BOOTP message. This is because, the two protocols are compatible. In fact a DHCP server can be programmed to answer BOOTP requests.
- Let us discuss each field and its function.

1. OP (Operation code) :

This is an 8-bit field which defines the type of DHCP packet. If it is 1 then request and if it is 2 then reply type.

2. HTYPE (Hardware type) :

This is an 8-bit field which defines the type of physical network. For example if the value of this field is 1 then it represents the Ethernet.

3. HLEN (Hardware Length) :

This is an 8-bit field which defines the length of the physical address (in terms of number of bytes). For Ethernet the value of this field is 6 (Ethernet has a 6-byte physical address).

4. HOPS (Hop count) :

The contents of this 8-bit field will define the maximum number of hops the packet can travel.

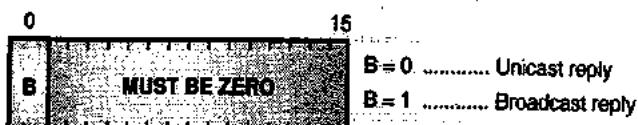
5. Transaction ID :

This is a 32-bit or 4-byte long field which carries an integer. The client sets the transaction identification number and uses it to match a request and its corresponding reply. The value of transaction ID field in the server's reply message is same as that written in the client's request.

6. Flags :

This is a 16-bit field as shown in Fig. 7.23.4 Only the leftmost bit is being used actually and all the other 15-bits are set to zero. The leftmost bit (B) specifies the type of reply from the server as follows :

- | | |
|-------|--------------------------------|
| B = 0 | ...Unicast reply from server |
| B = 1 | ...Broadcast reply from server |



(G-see) Fig. 7.23.4 : 16-bit FLAGS field format of DHCP

- The request message of DHCP contains the client's hardware address therefore, a DHCP server normally sends its responses to the client using hardware unicast.
- A client sets the high-order bit in the FLAGS field to request that the server respond using hardware broadcast instead of hardware unicast.
- A client might prefer to get broadcast response, because when a client communicates with a DHCP server, it does not yet have an IP address.
- If a datagram arrives via hardware unicast and the destination address does not match the computer's address IP then the message could be discarded.
- However, IP is required to accept and handle any datagram sent to the IP broadcast address. To ensure that the IP software accepts and delivers DHCP messages which arrive before the client gets its IP address a DHCP client can request the server to send responses using IP broadcast.

7. Client IP address :

This is a 32-bit or 4-byte field which contains the IP address of the client. This field will have a 0 value if the client does not have this information.

8. Your IP address :

This is a 32-bit or 4-byte field which contains the IP address of the client. This IP address is written by the server in the reply message generated in response to the request message of the client.

9. Server IP address :

This is a 32-bit or 4-byte field which contains the IP address of the server. This IP address is written by the server in the reply message generated in response to the client's request message.

10. Gateway IP address :

This 4-byte field contains the IP address of the router. The server writes this IP address in the reply message to the client.

11. Client hardware address :

This 16 byte field contains the physical address of the client. This address is supplied explicitly by the client in its request message.

12. Server name :

This is a 64-byte long field. It is an optional field. The server fills up this field in its reply message. If the server does not want to fill this field with any valid data then it will fill up this field with all zeros.



13. Boot file name :

This field is 128 byte long and it is an optional field. This field consists of the full pathname of the boot file. This path is useful for the client to retrieve other booting information. But being an optional field, the server may decide not to fill any data in it. Then it will fill this field with all zeros.

14. DHCP options and message type :

- It is important to note that the DHCP does not add any new fixed fields to the BOOTP message format. It also does not change the meaning of most fields. For example, the OP field in a DHCP message contains the same values as the OP field in a BOOTP message.
- The message is either a boot request (1) or a boot reply (2). To encode information such as the lease duration, DHCP uses options. For example, Fig. 7.23.5 illustrates the DHCP message type option used to specify which DHCP message is being sent.
- The options field has the same format as the VENDOR SPECIFIC AREA, and DHCP honors all the vendor specific information items defined for BOOTP.
- Similar to BOOTP, each option consists of an eight bit code field and an eight bit long field followed by octets of data that comprise the option.
- As shown in Fig. 7.23.5, the option used to specify a DHCP message type consists of exactly three bytes. The first byte contains the code 53, the second byte contains the length 1, and the third one contains a value used to identify one of the possible DHCP messages.

0	8	16	23
CODE (53)	LENGTH (1)	TYPE (1 - 7)	
<hr/>			
Type field	Corresponding DHCP message type		
1	DHCPDISCOVER		
2	DHCPOFFER		
3	DHCPRREQUEST		
4	DHCPDECLINE		
5	DHCPACK		
6	DHCPNACK		
7	DHCPRRELEASE		

Fig. 7.23.5 : The format of a DHCP message type option used to specify the DHCP message being sent

7.24 Configuration :

DHCP is capable of providing static and dynamic address allocation.

7.24.1 Static Address Allocation :

- In the static address allocation capacity, the database of DHCP server would bind the physical addresses to the IP addresses.

7.24.2 Dynamic Address Allocation :

- DHCP has another database in which a pool of available IP addresses is present. This database is used by DHCP when a client requests for a temporary IP address. In response to such a request the DHCP allots an unused IP address from the pool to the requesting client for a negotiable period of time.
- The dynamic IP address allocation is required when a host moves from one network to the other or when the host is frequently getting connected or disconnected to the same network.
- The dynamic IP address is assigned temporary for a short duration. The DHCP server issues a lease for a specific period of time.
- The client has to renew the lease as soon as it expires or stop using the assigned IP address.

7.24.3 Transition States :

- In the dynamic address allocation mode, the DHCP client acts as a state machine. Depending on the received message it will make transitions from one state to the other.
- The transition diagram with important states has been shown in Fig. 7.24.1.

7.24.3.1 Address Acquisition States :

- When the DHCP is being used to obtain an IP address, a client is in one of six states. The state transition diagram in Fig. 7.24.1 shows events and messages that force a client to change state.
- When a client first boots, it enters the INITIALIZE state. In order to get an IP address, the client first contacts all DHCP servers in the local net.
- To do so, the client broadcasts a DHCPDISCOVER message and enters into the SELECT state.
- Because DHCP is an extension of BOOTP, the client sends the DHCPDISCOVER message in a UDP datagram with the destination port set to the BOOTP port (i.e., port 67). All DHCP servers which are connected to the local net receive the message, and those servers that have been programmed to respond to that particular client send a DHCPOFFER message. Thus, a client may receive zero response or multiple responses.
- When the client is in state SELECT, it collects DHCPOFFER responses from DHCP servers. Each offer contains configuration information for the client alongwith an IP address that the server is offering to lease to the client.
- The client must choose one of the responses (e.g., the first to arrive), and negotiate with the server for a lease. To do so, the client sends a DHCP REQUEST message to the server, and enters the REQUEST state.



- To acknowledge the request has been received and to start the lease, the server responds by sending a DHCPACK. When of the acknowledgement is received the client moves to the BOUND state, where the client proceeds to use the address.
- To use DHCP, a host becomes a client by broadcasting a message to all servers on the local network. The host then collects lease offers from servers, selects one of the offers, and acknowledges the acceptance with the server.

7.24.3.2 Early Lease Termination :

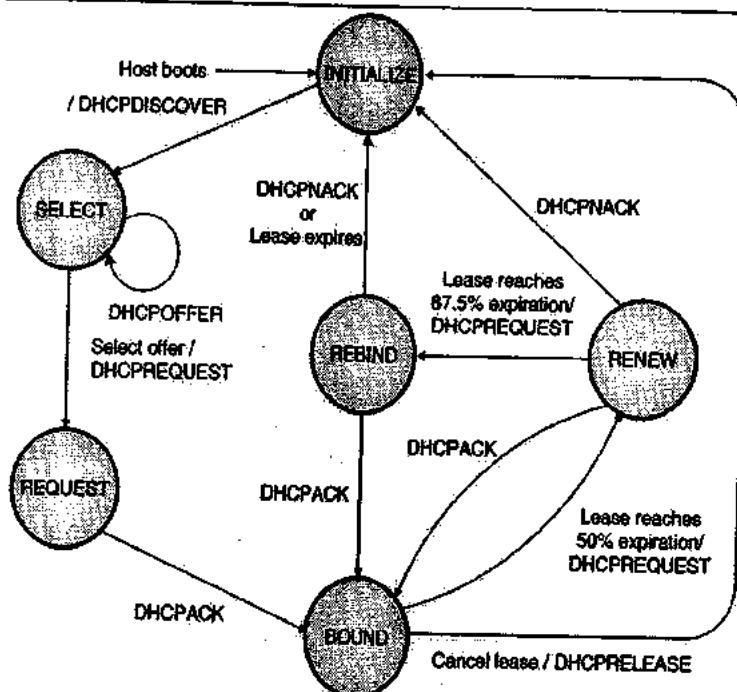
- We think of the BOUND state as the normal state of operation; a client generally remains in the BOUND state when it is using the IP address allotted to it.
- If a client has secondary storage (e.g., a local disk), the client can store the IP address on it and request for the same address when it restarts again.
- In some cases, however, a client in the BOUND state may discover that it does not need an IP address anymore. For example, suppose a user attaches a portable computer to a network, uses DHCP to acquire an IP address and then uses TCP/IP to read electronic mail.
- The user may not know how long reading mail will require, or the portable computer may allow the server to choose a lease period.
- In any case, the minimum lease period specified by DHCP is of one hour. If after obtaining an IP address, the user discovers that no e-mail messages are waiting to be read, the user may choose to

shutdown the portable computer and move to another location.

- If the clients does not needs a lease anymore, DHCP allows a client to terminate a lease and does not force the lease to expire.
- Early termination is especially important if only a small number of IP addresses are available at the server as compared to the number of computers that attach to the network. If each client terminates its lease as soon as the IP address is no longer needed, the server will be able to assign the address to another client.
- To terminate a lease early, a client sends a DHCPRELEASE message to the server. once an address is released the client is not allowed to use that address further.
- Thus, after transmitting the release message, the client must not send any other datagrams that use the address.
- As seen in the state transition diagram of Fig. 7.24.1 a host that sends a DHCPRELEASE leaves the BOUND state, and must start at the INITIALIZE a host state again before it can use IP.

7.24.3.3 Lease Renewal States :

- We have seen that when a client acquires an address, it moves to the BOUND state. After entering the BOUND state, the client sets three timers that control lease renewal, rebinding and expiration.
- A DHCP server can specify precise values for the timers when it allocates an address to the client; if the server does not specify timer values, the client uses the default values.



(G-582) Fig. 7.24.1 : State diagram of DHCP

- The default value for the first timer is one-half of the total lease time. When the first timer expires, the client must attempt to renew its lease. To request a renewal, the client sends a DHCPREQUEST message to the server from which it had obtained the lease.
- The client then moves to the RENEW state and waits for a response. The DHCPREQUEST contains the IP address which the client is currently using, and asks the server to extend the lease time to use the same address.
- Similar to the initial lease negotiation, a client can request its preferred period for the extension, but the actual lease time allotment is controlled entirely by the server.
- A server can respond to a client's renewal request in one of two ways: it can instruct the client to stop using the address or it can allow the client to continue use.
- If it allows the client to continue then, the server sends a DHCPACK, which causes the client to return to the BOUND state and continue using the same IP address.
- The DHCPACK can also contain new values for the client's timers. If a server does not allow the client to continue using the same address then, the server sends a DHCPNACK (negative acknowledgement), which causes the client to stop using the address immediately and return to the INITIALIZE state.
- After sending a DHCPREQUEST message that requests an extension on its lease, a client remains in state RENEW and waits for a response from the server.
- If it does not receive any response then the server that granted the lease is either down or unreachable. To handle this situation, DHCP relies on a second timer, which was set when the client entered the BOUND state.
- The second timer expires after 87.5% of the lease period, and makes the client to move from state RENEW to state REBIND. When making the transition, the client assumes the old DHCP server is not available anymore and starts broadcasting a DHCPREQUEST message to any server on the local net.
- Any server configured to provide service to the client can respond positively (i.e. to extend the lease), or negatively (i.e. to deny further use of the same IP address). If it receives a positive response, the client returns to the BOUND state, and resets the two timers.
- If it receives a negative response, the client must move to the INITIALIZE state, must immediately stop using the IP address, and must acquire a new IP address before it can continue to use IP.
- After moving to the REBIND state, a client should have asked the original server and all servers on the local net for a lease extension. sometimes a client

does not receive any response from any server before its third timer, expires, the lease expires.

The client must stop using the IP address, must move back to the INITIALIZE state, and begin acquiring a new address.

7.24.4 DHCP Architecture :

- DHCP offer a host with an Internet Protocol (IP) address along with other Internet configuration factor exclusive of any need for pre-configuration by the user.
- These innovative protocols get better on the usual Internet architecture, where the system administrator must allocate or modify each IP address independently. The manual process is costly, hard, error-prone and time-consuming.
- DHCP decrease the cost of organization of networks by reducing the need for the administrator to allocate or modify IP addresses again and again.
- Dynamic IP addresses are selected from a collection of unused IP addresses, and are automatically allocated to a host for temporary or permanent use.
- DHCP also recover that IP address for use by other clients when it is no longer required or when the time period for its use is up.
- The packet format design for DHCP and BOOTP are the same, even if BOOTP packets are fixed length and DHCP packets are variable length. The DHCP packet length is negotiate between the client and the server.
- DHCP is a technology that allow numerous valuable features :
 1. Network configuration automatically, once client machines are powered ON in a network that supports DHCP, the clients obtain IP addresses, subnet masks, the DNS domain, DNS servers, NIS+ domain, NIS+ servers, default routers, Time zones, time servers, and all the other information necessary to function without any requirement for individual configuration by an administrator.
 2. Automatic IP address administration together with assignment, reconfiguration, and renumbering of IP addresses. Since all TCP/IP parameters are handling centrally, and the DHCP service manages the task and use again of IP addresses automatically, minimal administrator participation is necessary.
 3. Easy system administration during the centralized location of network configuration information. The TCP/IP configuration information can be accumulating in a central place, in its place of being distributed between all the clients in the network.
 4. A network can be renumbered just and rapidly using somewhat short IP address on leases.

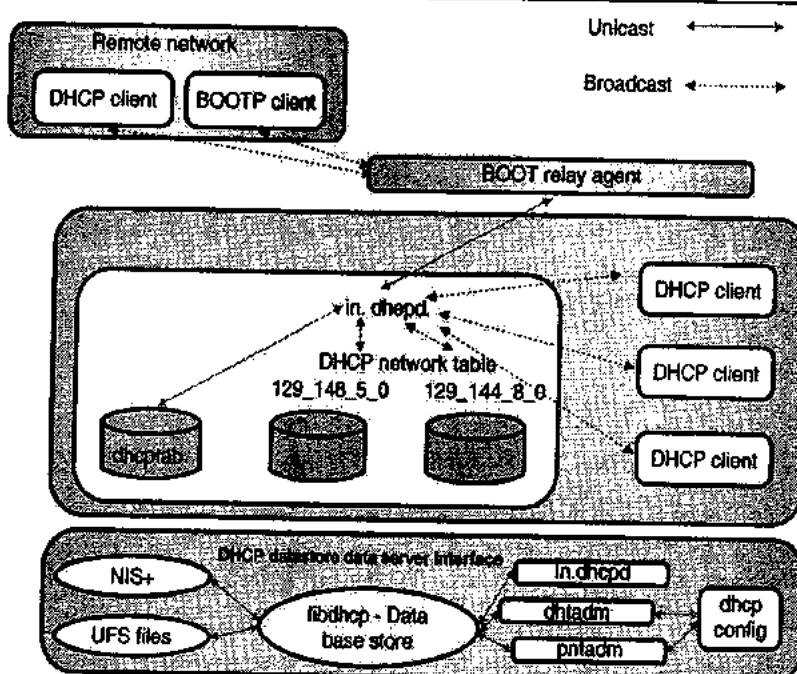


- DHCP can use accessible BOOTP relay function as DHCP is base on the BOOTP. This allows network administrators to set their routers to forward BOOTP/DHCP traffic to remote BOOTP/DHCP servers.
- Consequently network restriction, servers are no longer required on every network segment, as was true of the in rarpd and bootparams configuration services.
- The command of bootstraps that configures local and remote networks. Local networks are the server is directly connected. Remote networks the servers are not directly connected, but are access through BOOTP relay agents.
- An available client on remote networks needs the configuration of a BOOTP relay agent on the client's network.
- BOOTP relay agent functionality is available with routers and switches. Fig. 7.24.2 shows an overview of DHCP and BOOTP as DHCP Architectural Diagram.
- In figure, Unicast can represent by thick bi-directional link while broadcast can represent by dotted bi-directional link.
- There are various module are available in DHCP architecture as shown in Fig. 7.24.2.

7.24.5 The DHCP Client :

- The DHCP protocol has two functions consider to the client. It sends enough information to clients to establish end to end connection for network communications, and it supplies other parameters needed by system- and application-level software.

- It can perform some operation such as, the DHCP protocol supplies an IP address valid for the network attached to the client's hardware interface.
- The right to use of IP address is given to the client for a period of time, called a lease. This differs from the traditional static configuration. If the client wants to use the IP address for a period of time longer than the original lease, it must periodically negotiate a lease extension with the server through DHCP.
- When the client no longer needs the IP address, the user of the machine can relinquish its lease, returning it to the pool of available IP addresses. Otherwise, the IP address is reclaimed automatically when its lease expires.
- In addition sends and receives all the DHCP protocol packets when talking to the server with some steps :
 1. Constructs and sends packets
 2. Listens for responses from servers
 3. Caches the configuration information received
 4. Releases or renews leases
 5. Configures the interfaces with sufficient information to enable communications with the network through the interface
- This is where the responsibilities of the agent end. The daemon knows nothing of any higher-level services that the client might be running.
- Another operation is that, delivering application and system-level information we used `dhcpcinfo(1)`.
- The `dhcpcinfo` command takes a command line argument with a specified parameter, interrogates the agent as to the value of that parameter, and echoes the result to its standard output as a text.



(G-1621) Fig. 7.24.2 : DHCP Architecture



- The `dhcpcinfo` command allows other command line options to make ineffective this default behavior. One of these options allows an interface name to be explicitly specified. In that case, the values returned are those delivered by DHCP for that interface.

7.24.6 DHCP Server :

SPPU : May 12, Dec. 13, May 15

University Questions

- Q.1 Explain in brief functionality of DHCP server, Proxy server, Mail server. (May 12, 8 Marks)
- Q.2 Explain functionality of DHCP server. (Dec. 13, May 15, 2 Marks)

- The DHCP server runs the IP address space of networks directly connected to that server. To extend into other networks, DHCP servers or BOOTP relay agents must be set up on those networks.
- A DHCP server can act as a primary or a secondary server. To be a primary server, it must have a range of IP addresses for which it is responsible.
- When a DHCP server is added to a network that already has a primary DHCP server, the new server can be configured to provide primary and secondary service, or secondary service only.
- If the server is configured for both services, both servers can perform the duties of a primary server, (they can give out IP addresses) as long as each is primarily responsible for a different IP range.
- Each server can act as a secondary server for the other, by confirming existing configurations supplied by a primary server when the primary server is unable to respond to requests for confirmation. Every primary server automatically acts as a secondary server.
- A DHCP server's range of IP addresses is specified during the installation and configuration of the software on the server.
- As a primary DHCP server, the server can give out an IP address to a client requesting a new configuration from the range of IP addresses for which it is responsible.
- When a client asks for confirmation of its existing configuration, the server responsible for that client's IP address confirms the configuration.
- Acting as a secondary server, it can confirm configurations that were supplied by another DHCP server on the network.
- To provide secondary service, the DHCP server confirms configurations that were supplied by another DHCP server on the network. It does this when the primary server responsible for those IP addresses cannot respond. After a waiting period, the secondary server responds in its place.

- DHCP servers can be configured as secondary only. If you decide you want to configure a DHCP server as a secondary server only, you can do this through the `dhcpconfig` program, by choosing to configure the server without a range of IP addresses that it can give out to clients requesting a new configuration. In this configuration, the DHCP servers should be using NIS+ for their data storage.

- DHCP service is enabled and configured on the machine on which it is run with the `dhcpconfig` utility. This utility allows you to set startup options, configure the DHCP service database type and location, and initialize the `dhcptab` and `dhcp_network` tables for any locally attached or remote networks.
- When `dhcpconfig` is invoked, it presents a menu offering the option of configuring the DHCP service, configuring a BOOTP relay agent, removing the DHCP configuration or relay service configuration, or exiting. When the administrator selects one of the menu options, he or she is presented with a series of questions to collect the required information. Then `dhcpconfig` performs the appropriate steps to turn on the selected functions.
- Multiple DHCP servers on the same network operate much more efficiently if they share DHCP databases through NIS+. Sharing allows DHCP servers to communicate through a common datastore, increasing redundancy and balancing load among cooperating servers.
- When a new DHCP client is added to the network, the client broadcasts a message intended to locate all available DHCP and/or BOOTP servers within reach.
- Any DHCP server that receives the message first checks to see if any IP addresses are available for assignment.
- If they are, the server verifies that a potential IP address is not already in use. If it is not, the server offers the IP address and other configuration information to the client.
- If the IP address is in use, the server marks this IP address as unusable, notifies the network administrator of its status, and selects another IP address.
- The client selects an IP address offered to it based on its own criteria, and broadcasts a message that identifies its selection.

Server Databases :

- The DHCP/BOOTP server uses two types of databases: the `dhcptab` database and the `dhcp_network` databases.



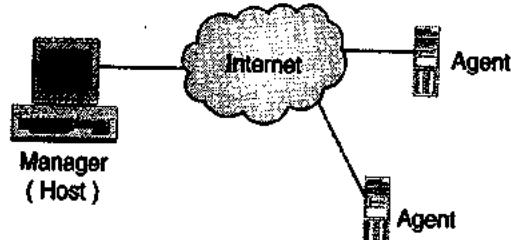
- The dhcptab database contains macros defined using a termcap-like syntax. This syntax permits network administrators to define groups of DHCP configuration parameters to be returned to clients. There are currently 77 predefined parameters.
 - A DHCP/BOOTP server returns hostname, network broadcast address, network subnet mask, or IP Maximum Transfer Unit (MTU), if this information is requested by a client attached to the same network as the server.
 - This information does not have to be explicitly configured in the dhcptab. The dhcpcmd command manages the dhcptab service configuration table.
 - If there are two servers sharing a distributed dhcptab table, the administrator can configure the DHCP parameters in the table so the servers back each other up, provided that they are in the same NIS+ domain.
 - However, each should be primarily responsible for a different range of IP addresses. Each network might require a BOOTP relay agent as well, so its clients can reach the server on the other network.
 - The dhcp_network databases contain client identifier-to-IP address mappings. These databases are named after the network they support.
 - There is one dhcp_network database for each network that offers DHCP/BOOTP services.
 - The dhcp_network databases are located dynamically by the server and consulted during runtime.
 - A client request received from a network for which no dhcp_network database exists is ignored.
 - The dhcp_network database maps a DHCP client's client identifier to an IP address and the configuration parameter associated with that IP address.
 - This database is located by the DHCP server at runtime by generating dhcp_network database name by using the IP network address and subnet mask for the network where the DHCP request originated.
 - The in.dhcpd daemon has two run modes, DHCP server (with optional BOOTP compatibility mode) and BOOTP relay agent mode (see in.dhcpd(1M)).
- 7.24.7 BOOTP Relay Agents :**
- Multiple networks, and the use of netmasks to identify them, complicate the functioning of TCP/IP-based networks.
 - For instance, broadcasting using IP cannot take place through the gateways that link networks. So clients on one network cannot broadcast DHCP or BOOTP requests to servers on other networks.
 - A BOOTP relay agent must direct the initial requests through the gateway to the server, then return the replies from the server to the clients.
 - The in.dhcpd daemon can be run as a BOOTP relay agent. If you specify BOOTP relay agent mode, the option argument specifies a comma-separated list of IP addresses or the hostnames of DHCP or BOOTP servers to which the relay agent must forward BOOTP requests.
 - When the daemon is started in this mode, any DHCP databases are ignored, and the daemon acts as a BOOTP relay agent. A BOOTP relay agent listens to UDP port 68, and forwards BOOTP request packets received on this port to the destinations specified on the command line.
 - The relay agent can run on any machine that has knowledge of local routers, so it does not have to be an Internet gateway machine.
 - After you install the BOOTP relay agent, entries must be added to the distributed DHCP databases so the DHCP servers can service clients sending requests through the BOOTP relay agent.

7.25 Simple Network Management Protocol (SNMP) :

- SNMP provides the framework which is necessary for management of devices in an internet (any internet). It uses TCP/IP suite for the same.
- SNMP can be used to monitor and maintain an internet with the help of some fundamental operations.

7.25.1 Concept :

- SNMP is based on the concept of manager and agent. A manager is usually a host and agents are usually routers. The host controls and monitors the routers.
- Fig. 7.25.1 demonstrates the SNMP concept.



(G-1531) Fig. 7.25.1 : SNMP concept

- SNMP is an application-level protocol. It is designed in such a way that it can monitor devices made by different manufacturers, used in different physical networks.
- SNMP can work successfully in a heterogeneous internet made up of LANs and WANs that are interconnected by different types of routers.

7.25.2 Managers and Agents :

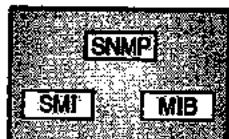
- A manager is actually a management station that runs the SNMP client program. An agent is actually a managed station which is a router or a host that runs the SNMP server program. The manager and agent simply interact with each other to achieve the management objective.
- The agent maintains a database which has its performance information. The manager can access these values in the database.



- The manager can also force the agent (router) to perform certain tasks. For example the manager can reboot the router remotely at any time by sending a packet to force a 0 value in the reboot counter of the router. (A router reboots itself when the contents of reboot counter go to zero).
- An agent can get involved in the management process by sending a trap (warning) message to the manager if it (agent) notices something wrong around it.
- Thus the SNMP manages on the basis of the following three basic ideas :
 - A manager controls an agent by asking for information about behaviour of the agent.
 - A manager can force an agent to perform certain actions.
 - An agent can send warning messages (trap) to manager to report anything unusual around itself.

7.25.3 Management Components :

- SNMP uses two other protocols to perform its management tasks :
 - Structure of Management Information (SMI)
 - Management Information Base (MIB)
- So management on the Internet is performed through the simultaneous use of three protocols : SNMP, SMI and MIB. Fig. 7.25.2 shows the components of network management on Internet.



(G-1533) Fig. 7.25.2 : Components of network management on the Internet

- These three protocols interact with each other in the following manner.
- Role of SNMP :**
 - SNMP plays very specific roles in network management. Some of them are as follows :
 - To define the format of the packet sent from manager to agent and vice versa.
 - To interpret the results and create statistics by making use of other management software.
 - To read and exchange the status (values) of objects (variables) in SNMP packets.

2. Role of SMI :

- The role of SMI is as follows :
 - To define the general rules which can be used for naming objects, defining object types. These rules are required for using SNMP.
 - To show how to encode objects and values.

Note : SMI does not define the number of objects that are to be managed by an entity. It also does not name the objects to be managed or define the relationship between objects and their values.

3. Role of MIB :

- The role of MIB is as follows :
 - To define the number of objects and name them for each entity to be managed. This is to be done according to the rules defined by SMI.
 - To associate a name to each numbered object.

7.25.4 Structure of Management Information (SMI) :

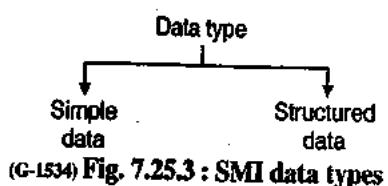
- The SMI version 2 (SMIV2) is an important ingredient of network management. It has the following functions to perform :
 - It has to name objects.
 - It needs to decide the type of data that an object can store.
 - It has to instruct about encoding the data to be transmitted over the network.
- SMI performs the role of providing a guideline to SNMP. It stresses upon three attributes to handle an object. They are :
 - Name
 - Type
 - Encoding method.

Name :

- SMI feels that each managed object such as a router, a value, a variable in a router etc. must have a name and the name should be unique one.
- SMI makes use of an object identifier to name objects globally. An object identifier works on the basis of a hierarchical identifier which in turn makes use of the tree structure.
- The tree structure starts with an unnamed root. We can use a sequence of integers separated by dots in order to uniquely define each object. This type of representation is used in SNMP.

Type :

- The second attribute of an object is related to what type of data is being stored in it. The fundamental Abstract Syntax Notation 1 (ASN. 1) definitions and some new ones are being used, to define the data type.
- As shown in Fig. 7.25.3 data types in SMI can be classified into two types namely :
 - Simple data
 - Structured data



1. Simple data type :

- The simple data types basically are atomic data types. A few of them have been taken directly from ASN.1 but some of them have been added by SMI.
- Table 7.25.1 shows the most important simple data types. First five have been taken from ASN.1 and the next seven have been added by SMI.

Table 7.25.1 : Basic data types of the SMI

Data type	Description
Integer	32-bit integer as defined in ASN.1.
Integer 32	32-bit integer with a value between -2^{31} to $2^{31} - 1$.
Unsigned 32	Unsigned 32 bit integer from 0 to $2^{32} - 1$.
Octet string	ASN.1 format byte string.
Object identifier	ASN.1 format.
IP address	32 bit Internet address.
Counter 32	32 bit counter which increases from 0 to $2^{32} - 1$.
Counter 64	64 bit counter
Gauge 32	32 bit integer in the range $2^{32} - 1$ to 0.
Time ticks	Time, measured in $1/100^{\text{th}}$ of a second since some event.
Opaque	Uninterpreted ASN.1 string, needed for backward compatibility.

Structured type data :

- The new structured data types can be prepared by combining the simple and structured data types.
- The two structured data types defined by SMI are as follows :
 - Sequence
 - Sequence of

1. Sequence :

This data type can be obtained by combining simple data types which may or may not be of the same type.

2. Sequence of :

This data type can be obtained by combining simple data types which are of the same type.

Encoding method :

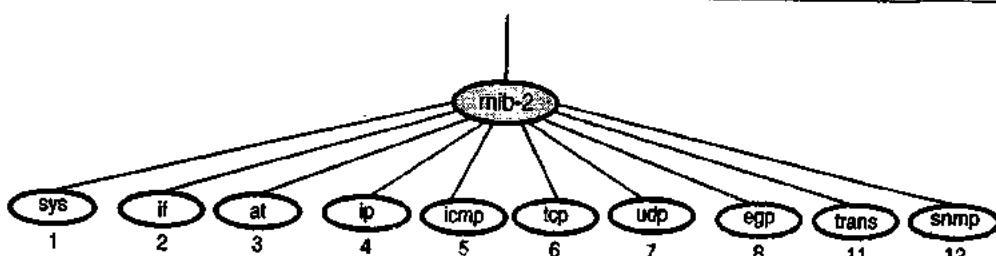
- SMI uses **Basic Encoding Rule (BER)** as a standard in order to encode data before sending it over the network.
- According to BER each data symbol should be encoded in triplet format : 1. Tag 2. Length and 3. Value.

7.25.5 Management Information Base (MIB) :

- The second ingredient used in network management is the management information base version 2 (**MIBv2**).
- Each agent has his own MIB2. It is a collection of all the objects which a manager is capable of managing successfully.
- The MIB2 objects are classified into ten categories or groups. All these groups come under mib-2 object in the object identifier tree as shown in Fig. 7.25.4.

7.25.6 Simple Network Management Protocol (SNMP) :

- This is the actual SNMP protocol itself. It defines how information is exchanged between SNMP agents and network management stations.
- The SNMP protocol operations define the various SNMP messages and how they are created and used. SNMP transport mappings describe how SNMP can be used over various underlying internet works, such as TCP/IP, IPX and others.
- It is simply an application program that has a client on the manager and a server on the agent. SNMP allows a manager to perform following three important tasks :
 - Retrieve any information from an agent database (i.e. retrieve variables defined by the agent).
 - Store/update the value in an agent database.
 - Receive alerts from agents in case of problems.
- To achieve these objectives, SNMP defines five message types, as shown in Table 7.25.2. Note that all these messages are exchanged as simple UDP packets between the manager and the agent.



(G-1535) Fig. 7.25.4 : MIB2 objects in the object identifier

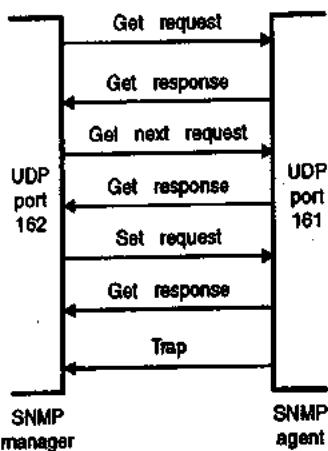


- Since these messages are simple request-response pairs, they do not require any connection/session to be established. Therefore, TCP is not required in this case.

Table 7.25.2 : SNMP messages

Message	Description
GetRequest	The manager (client) sends this message to the agent (server) to request for the value of an agent variable.
GetNextRequest	If the agent variables are in the form of a table, the manager cannot use the GetRequest message, as it does not know where the current table pointer is located. This message is used in such cases.
GetResponse	The agent replies to a manager's GetRequest or GetNextRequest messages using this message. This message contains the values of the variables requested for by the manager.
SetRequest	The manager can ask the agent to store a particular value in an agent variable using this message.
Trap	The agent can report an error or any such event to the manager using this message.

Fig. 7.25.5 shows five SNMP messages.



(G.723) Fig. 7.25.5 : Five SNMP messages

Review Questions

- Q. 1 Briefly discuss of the following terms, emphasis more on implementation details :
 (a) DNS (b) Mail server
- Q. 2 When web pages are sent out, they are prefixed by MIME headers ? Why ?
- Q. 3 What is domain name system ? How does it work ? Explain resolution process.
- Q. 4 What is mailing list ? Explain with suitable block diagram.
- Q. 5 Describe a typical resolution process in DNS.
- Q. 6 Write short notes on : Domain name resolution.
- Q. 7 Explain how file transfer protocol clients servers are configured. Discuss the various FTP and telnet commands.
- Q. 8 Why do HTTP, FTP, SMTP, POP3 and IMAP run on top of TCP rather than UDP ?

Ans. :

All these protocols require a reliable end to end connection oriented service which they can get only from TCP and not from UDP. For more details on how TCP is used in FTP refer section 5.13.

Q. 9 Write a short note on TFTP.

Q. 10 What is the difference between FTP and TFTP ?

7.26 University Questions and Answers :

- Q. 1 Explain functionality of file server, web server.

(May 2015, 4 Marks)

Ans. :

Types of servers :

The commonly used servers are of following types :

1. File servers
2. Print servers
3. Application servers
4. Message servers
5. Database servers

Windows NT server support all of these capabilities and can by itself serve in all of these capacities simultaneously on a small network. On large networks however a number of servers are required to increase the access speed.

File servers :

Some of the important features of file servers are as follows :

- These servers provide the services such as storing, retrieving and moving the data.
- A user can read, write, exchange and manage the files with the help of file servers.
- A file can be stored in three different ways namely online, offline and nearline storage.



Solved University Question Papers of August 2017 & Dec. 2017

August 2017

Chapter 1 : Physical Layer

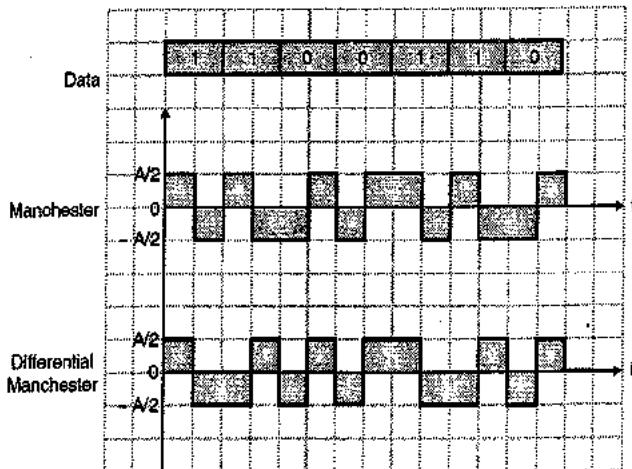
Q. 1(a) What are the design issues of layers ? Explain it.
(Section 1.15) (5 Marks)

Q. 1(b) What are the different network devices ? Explain difference between switch and hub.
(Sections 1.29 and 1.36.6) (5 Marks)

Q. 2(b)OR What is line encoding ? Give the Manchester line code and differential Manchester code for the bit sequence : 1100110. (5 Marks)

Ans. :

For definition of line coding refer section 1.37.



(G-2274) Fig. 1

Chapter 2 : Logical Link Control

Q. 3(a) What is need of framing ? What are the different techniques of framing ? Explain any two.
(Sections 2.4, 2.4.1, 2.4.2 and 2.4.3)
(5 Marks)

Q. 3(b) The data word 1101011011 is to be sent using generator polynomial $X^4 + X + 1$. Use CRC to compute the code word at the sender side.
(Ex. 2.6.12) (5 Marks)

Q. 4(a)OR Explain Go back N sliding window protocol with example. (Section 2.9.2) (5 Marks)

Q. 4(b)OR Explain bit oriented protocol for communication over point to point and multipoint link.
(Section 2.11) (5 Marks)

Chapter 3 : Medium Access Control

Q. 2(a)OR What are the transmission techniques used by 802.11 to send a MAC frame from one station to another ? Explain two of them.
(Sections 3.29.2, 3.29.3 and 3.30.1)

(5 Marks)

Q. 5(a) Draw and explain frame format of 802.16 standard.
(Section 3.44.2) (5 Marks)

Q. 5(b) Consider building a CSMA / CD network running at 1 Gbps over a 1 km cable with no repeaters. The signal speed in the cable is 200000 km/sec. What is the minimum frame size ? (Ex. 3.19.2) (5 Marks)

Q. 6(a)OR State the difference between static and dynamic channel allocation. Give two examples for each. (Sections 3.2.1 and 3.2.2)
(5 Marks)

Q. 6(b)OR Explain working of CSMA/CA with the help of flow diagram. (Section 3.5.3) (5 Marks)



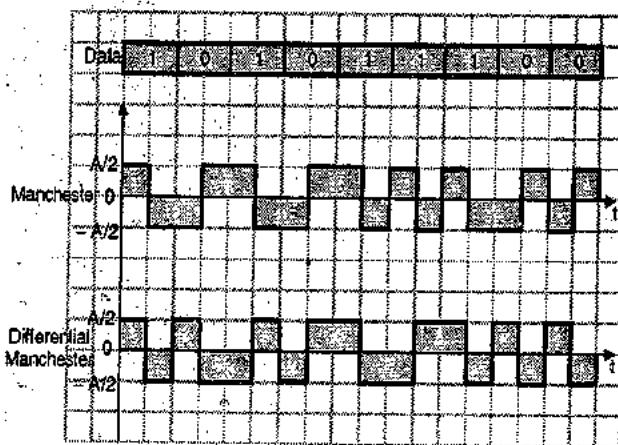
Dec. 2017

Chapter 1 : Physical Layer

Q. 1(a) Differentiate between OSI and TCP/IP reference model. (Section 1.21.4) (4 Marks)

Q. 1(b) Represent 101011100 using Manchester and differential Manchester line coding technique. (4 Marks)

Ans.



(G-2277) Fig. 1

Q. 2(a)OR Explain in brief : FHSS and DSSS. (Sections 1.45 and 1.46) (6 Marks)

Q. 2(b)OR Explain fiber optic modes of propagation. (Section 1.25.4) (4 Marks)

Chapter 2 : Logical Link Control

Q. 3(a) Explain control field of HDLC with respect to I-frame, S-frame and U-frame. (Section 2.11.2) (6 Marks)

Q. 4(a)OR Explain selective repeat ARQ in detail. (Section 2.9.4) (5 Marks)

Q. 4(b)OR A bit stream 1001101 is transmitted using an hamming code. Show the actual bit string transmitted. Suppose 7th bit from left is inverted during transmission, show that this error is detected and corrected at the receiver's end. (5 Marks)

Ans.:

Step 1 : Codeword format :

Number of data bits = 7

Number of parity bits = 4. Codeword structure is as shown in Fig. 2(a).

	11	10	9	8	7	6	5	4	3	2	1
Codeword :	1	0	0	P ₈	1	1	0	P ₄	1	P ₂	P ₁

(G-2278) Fig. 2(a)

Step 2 : Decide P₁, P₂, P₄ and P₈:

Assume even parity.

Table 1

Parity bit	Bits to be checked	Bit values	Value of parity bit
P ₁	1, 3, 5, 7, 9, 11	P ₁ 10101	P ₁ = 1
P ₂	2, 3, 6, 7, 10, 11	P ₂ 11101	P ₂ = 0
P ₄	4, 5, 6, 7	P ₄ 011	P ₄ = 0
P ₈	8, 9, 10, 11	P ₈ 001	P ₈ = 1

The transmitted codeword is as follows :

	11	10	9	8	7	6	5	4	3	2	1
Codeword :	1	0	0	0	1	1	0	0	1	0	1

(G-2279) Fig. 2(b)

Step 3 : Error detection and correction :

If seventh bit from left is inverted during transmission. So the received codeword is as shown in Fig. 2(c).

	11	10	9	8	7	6	5	4	3	2	1
Received codeword :	1	0	0	1	0	1	0	0	1	0	1

(G-2280) Fig. 2(c)

1. Analyze bits 1, 3, 5, 7, 9, 11 :

∴ 110001 → Odd parity so error exists

∴ Put P₁ = 1

2. Analyze bits 2, 3, 6, 7, 10, 11 :

∴ 011001 → Odd parity so error exists

∴ Put P₂ = 1

3. Analyze bits 4, 5, 6, 7 :

∴ 0010 → Odd parity so error exists

∴ Put P₄ = 1

4. Analyze bits 8, 9, 10, 11 :

$\therefore 1001 \rightarrow$ Even parity so no error

$$\therefore \text{Put } P_8 = 0$$

The error word is shown in Fig. 2(d).

Error word E =	P_8	P_4	P_2	P_1	=	0	1	1	1
----------------	-------	-------	-------	-------	---	---	---	---	---

Fig. 2(d)

The decimal equivalent of error word is $(7)_{10}$. Hence bit 7 contains an error.

Q. 7(b) In a Stop-and-Wait system, the bandwidth of the line is 2 Mbps, and 1 bit takes 20 milliseconds to make a round trip. What is the bandwidth-delay product ? If the system data packets are 2,000 bits in length, what is the utilization percentage of the link ?

(4 Marks)

Ans. :

Part I : Find BW Delay product :

Given : Stop and wait system, BW = 2 Mbps, RTT = 20 ms

BW delay product = BW × Round trip delay for 1 bit

$$= 2 \times 10^6 \times 20 \times 10^{-3}$$

$$= 40,000 \text{ bits} \quad \dots \text{Ans.}$$

Part II : Find the link utilization percentage :

Given : Data packet length = 2000 bits

The BW-delay product is equal to 40 kbits. That means the system is capable of sending 40,000 bits during the time taken by the data to go from sender to receiver and its acknowledgement comes back.

But in reality the system is sending only 2000 bits.

$$\therefore \text{Link utilization} = \frac{\text{Actually sent bits}}{\text{Capacity of the link}} \times 100$$

$$= \frac{2000}{40 \times 10^3} \times 100 = 5\% \quad \dots \text{Ans.}$$

Chapter 3 : Medium Access Control

Q. 1(c) Draw flowchart of CSMA/CA (Section 3.5.3)

(2 Marks)

Q. 3(b) A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system (All stations together) produces :

1. 1000 frames per second

2. 500 frames per second

(4 Marks)

Ans. :

1. In slotted ALOHA for $G = 1$ maximum throughput = 0.368

$$\text{Throughput} = 0.368 \times 1000 = 368 \text{ frames/sec.}$$

2. In this case $G = 500$ frames/sec. i.e. $\frac{1}{2}$

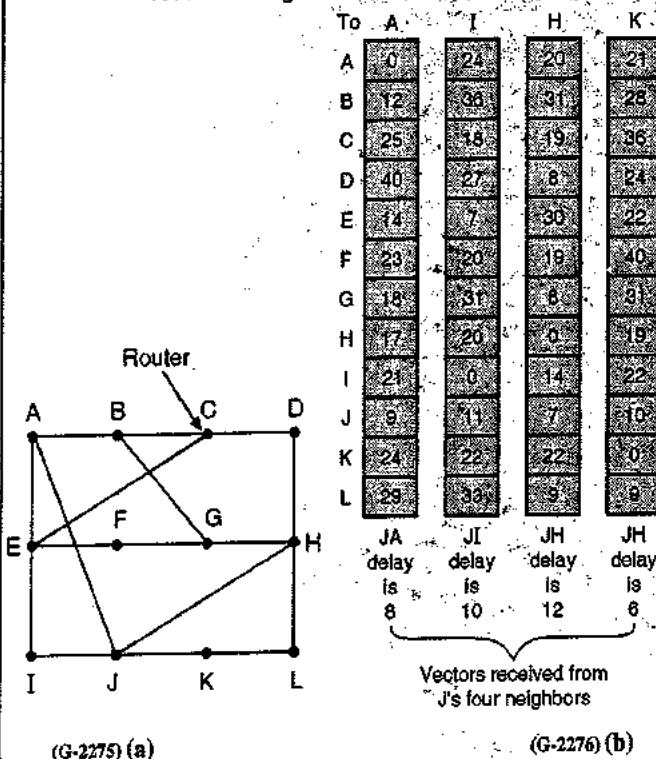
$$S = Ge^{-4} = \frac{1}{2} e^{-(1/2)} = 0.3032$$

$$\text{Throughput} = 0.3032 \times 500$$

$$= 151.63 \cong 151 \text{ frames/sec.}$$

Chapter 4 : Network Layer

Q. 6(c)OR Explain distance vector routing algorithm. Consider topology given in Fig. 3(a) and vectors received from router J's four neighbors are given in Fig. 3(b). Calculate new routing table for router J using Distance vector routing algorithm.



(G-2275) (a)

(G-2276) (b)

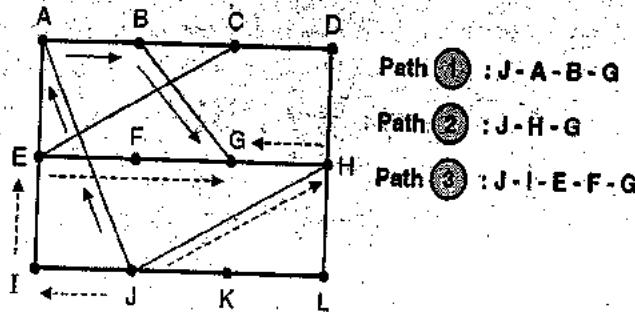
Fig. 3

Ans. : Refer section 4.17.1 for the distance vector routing algorithm.

Routing table for router J :

Let us understand how router "J" computes its new route to say router G.

There are many possible paths from J to G as shown in Fig. 3(c).



(G-2284) Fig. 3(c) : Different possible paths from J to G

(G-2285).

- The delay corresponding to path -1 (J - A - B - G) is as follows :

$$\begin{aligned} J \text{ to } A : \text{Delay} = 8 \text{ mS} \\ A \text{ to } G : \text{Delay} = 18 \text{ mS} \end{aligned} \quad \therefore \text{Path - 1 : } 26 \text{ mS}$$

- Similarly for path -2 (J - H - G) the delay is

$$\begin{aligned} J \text{ to } H : \text{Delay} = 12 \text{ mS} \\ H \text{ to } G : \text{Delay} = 6 \text{ mS} \end{aligned} \quad \therefore \text{Path - 2 : } 18 \text{ mS}$$

- And for path -3 (J - I - E - F - G) the delay is

$$\begin{aligned} J \text{ to } I : \text{Delay} = 10 \text{ mS} \\ I \text{ to } G : \text{Delay} = 31 \text{ mS} \end{aligned} \quad \therefore \text{Path - 3 : } 41 \text{ mS}$$

The best of these values is 18 msec corresponding to path-2 (J-H-G). Therefore in J's routing table shown in Fig. 3(d) we enter 18 mS delay and path via H.

We make the calculations for all the other destinations and complete the routing table for J as shown in Fig. 3(d).

From	To	J	Line
A	B	A	
B	20	A	
C	28	I	
D	20	H	
E	17	F	
F	30	I	
G	18	H	
H	12	H	
I	10	I	
J	0	-	
K	6	K	
L	15	K	

(G-2286) Fig. 3(d) : New routing table for J

Chapter 5 : Network Layer Protocols

- Q. 5(a) An organization is granted the block 130.34.12.64/26. The organization needs to have four subnets with equal number of addresses in each subnet. What are the subnet addresses and the range of addresses for each subnet ? (6 Marks)

Ans. :

- 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 130.34.12.64 / 26 whereas the last address will be 130.34.12.127 / 26.

Subnet design :

- Step 2 : Find number of hosts per subnetwork :

There are four subnetworks with equal number of hosts.

- ∴ 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,

$$n_1 = n_2 = n_3 = n_4 = n + \log_2 \left[\frac{N}{N_{\text{sub}}} \right]$$

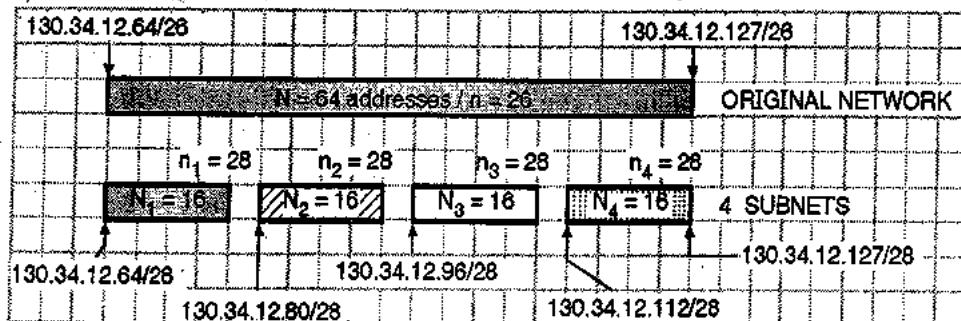
$$= 26 + \log_2 \left[\frac{64}{16} \right] = 26 + \log_2 4$$

$$\therefore n_1 = n_2 = n_3 = n_4 = 28 \quad \dots \text{Ans.}$$

- Step 4 : Starting and ending addresses of all the subnets :

Refer Fig. 4 which shows all the starting and ending addresses of the 4-subnets.

It should be noted from Fig. 3 that all the starting addresses should be divisible by the number of addresses in the subnet i.e. by 16.



(G-228) Fig. 4

Q. 5(c) Draw and explain IPv6 header. Explain the significance of extension header.

(Sections 5.4.5 and 5.5) (6 Marks)

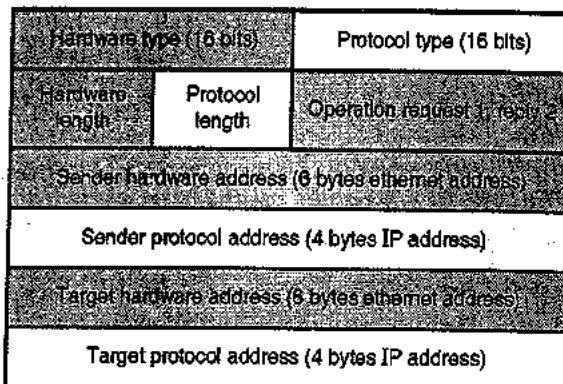
Q. 6(a)OR A host with IP address 130.23.43.20 and physical address B2 : 34 : 55 : 10 : 22 : 10 has a packet to send to another host with IP address 130.23.43.25 and physical address A4 : 6E : F4 : 59 : 83 : AB. The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames. (4 Marks)

Ans.:

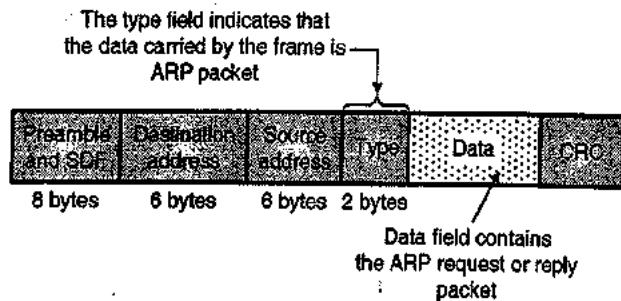
The ARP request and reply messages are as shown in Fig. 5(c). It should be noted that the ARP data field in this case is 28 bytes long. Therefore the individual addresses cannot be accommodated in the 4 byte boundary.

Therefore, the regular 4 bit boundaries have not been shown for these addresses. Another important point is that the IP addresses are shown using hexadecimal notation. Fig. 5(a) shows

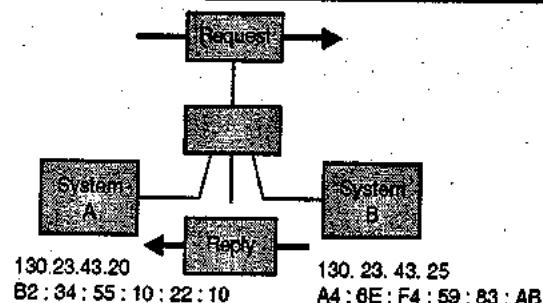
the format of ARP packet and Fig. 5(b) shows the encapsulation of ARP packet for your reference.



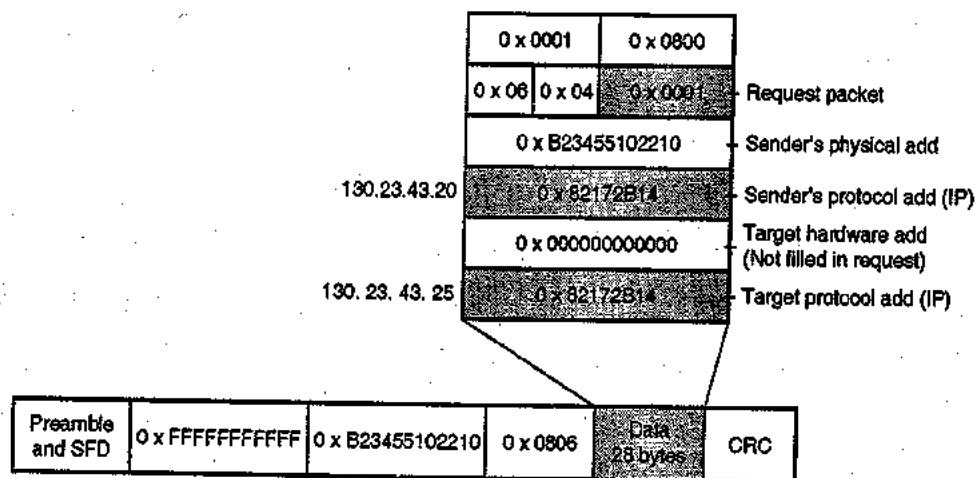
(G-228) Fig. 5(a) : ARP message format



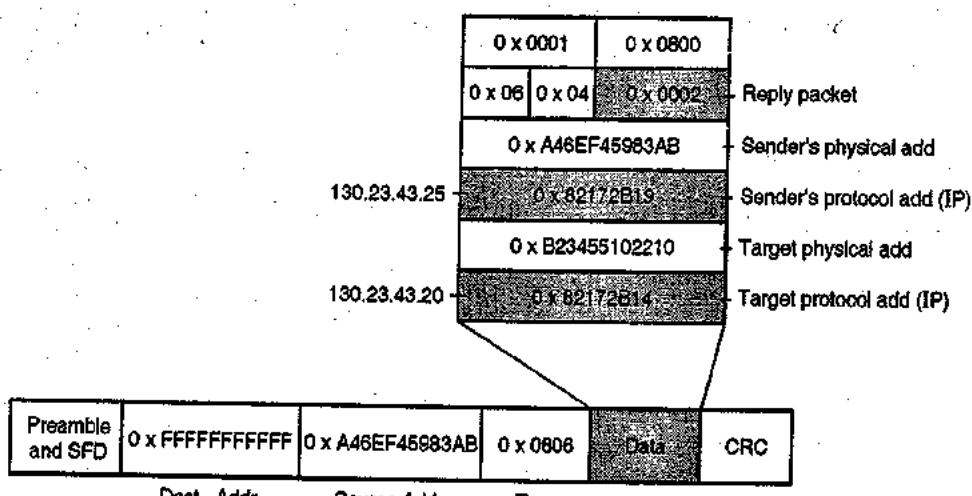
(G-578) Fig. 5(b) : Encapsulation of ARP packet



ARP request packet from A to B :



ARP reply packet from B to A :



(G-2283) Fig. 5(c)

Q. 6(b)OR Write a short note on :

1. NAT (Section 5.4.6)
 2. ICMP (Section 5.8) (8 Marks)

Chapter 6 : Transport Layer

Q. 5(b) What are general techniques to improve quality of service ? Explain any one in detail.

(Sections 6.22.2 and 6.22.3) (6 Marks)

Q. 7(a) What causes silly window syndrome ? How it is avoided ? Explain.

(Section 6.16.2) (4 Marks)

Q. 7(c) For each of the following applications, determine whether TCP or UDP is used as the transport layer protocol and explain the reason(s) for your choice.

1. Watching a real time streamed video.
 2. Web browsing.
 3. A voice over IP (VoIP) telephone conversation.
 4. You tube video. **(8 Marks)**



Ans. :

1. Watching a real time streamed video :

UDP is preferred for this application, because this application cannot tolerate the uneven delays, which get introduced if TCP is used (Refer section 6.8.2)

2. Web browsing :

TCP is preferred for this application, because in web browsing, bulk data transfer is required for which UDP is not suitable.

3. A VoIP telephone conversation :

UDP is preferred for this application. The reason for this is due to lack of congestion control, UDP does not create any additional traffic which is a desirable feature for a congestion prone network.

4. You tube video :

The you tube videos are of two types : Live stream and static. For the live stream videos, UDP is used for the reason stated earlier.

However for the static videos, TCP is preferred because video streaming requires pre-fetching and buffering for smooth play out. TCP provides also ensuring a much better quality than UDP.

Q. 8(a)OR What are the types of socket ? Explain various socket primitives used in connection oriented client server approach.
(Sections 6.5.1 and 6.5.2) (8 Marks)

Q. 8(b)OR Explain UDP header. Below is an Hexadecimal dump of an UDP datagram captured.

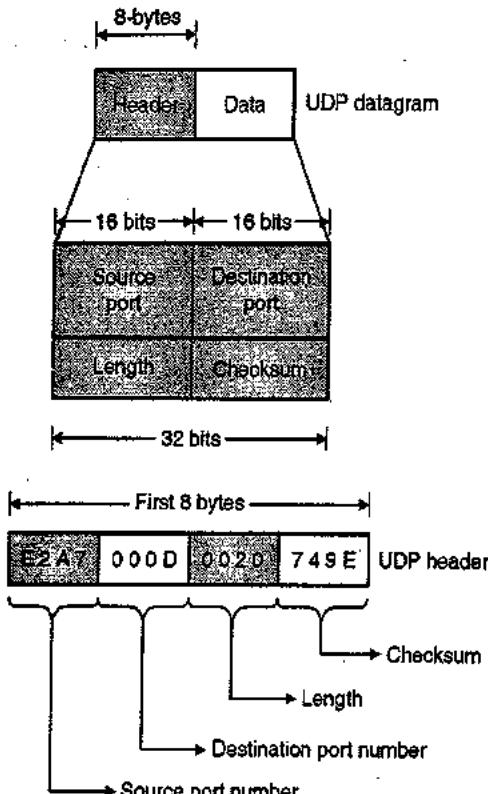
```
e2 a7 00 0D 00 20 74 9e 0e ff 00 00 00 01 00  
00 00 00 00 00 06 69 73 61 74 61 70 00 00 01  
00 01
```

1. What is source port number ?
 2. What is destination port number ?
 3. What is total length of the user datagram ?
 4. What is the length of the data ?
 5. Is packet directed from a client to server or vice versa ?
- (8 Marks)

Ans. : Refer section 6.8.3 for UDP header explanation.

Solution to the example :

The UDP datagram structure is as shown in Fig. 6, which shows that the UDP header is 8 byte long and the remaining bytes correspond to the data.



(G-228) Fig. 6 : UDP datagram and header

Note that only the first 8-bytes out of the given hexadecimal dump correspond to the UDP header which is shown in Fig. 6.

1. Source port number = $(E2\ A7)_{16}$...Ans.
2. Destination port number = $(000D)_{16}$...Ans.
3. Total length of UDP datagram = $(0020)_{16} = (32)_{10}$ bytes ...Ans.
4. Length of data = Total length - Length of header = $32 - 8 = 24$ 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.

Chapter 7 : Application Layer

Q. 9(a) What is the difference between persistent and non persistent HTTP ? Explain HTTP request and reply message format. (Sections 7.18.3, 7.18.5 and 7.18.7) (6 Marks)

Q. 9(b) Write short notes on :

1. DHCP (Section 7.23.3)
2. MIME (Sections 7.8 and 7.8.1) (6 Marks)

Q. 9(c) Explain DNS message format.
(Section 7.6.3) (4 Marks)