2019
MU

Strictly as per the New Revised Syllabus (Rev - 2016) of
Mumbai University w.e.f. academic year 2018-2019
(As per Choice Based Credit and Grading System)

Computer Networks

(Code : CSC503)

Semester V - Computer Engineering

Same Subject, Same Author with New Publication

J. S. Katre

With Solved Latest University Question Papers
upto Dec. 2018.

TechKnowledge
Publications

Scanned by CamScanner

Computer Networks

(Code : CSC503)

Semester V – Computer Engineering
(Mumbai University)

Strictly as per New Choice Based Credit and Grading System Syllabus (Revise 2016) of Mumbai University with effective from Academic Year 2018-2019

THE JAGDISH BOOK DEPOT
Near Punjab National Bank,
Shivaji Path, Thane (W)

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

TechKnowledge™ Publications

MO45A Price ₹ 365/-

(Book Code : MO45A)

Scanned by CamScanner

Computer Networks (Code : CSC503)

J. S. Katre.

(Semester V, Computer Engineering, Mumbai University)

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 : July 2018

Second Revised Edition : June 2019 **(TechKnowledge Publications)**

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

Printed at : 37/2, Ashtavinayak Industrial Estate, Near Pari Company,
Narhe, Pune, Maharashtra State, India.
Pune - 411041

ISBN : 978-93-89233-52-0

Published by :

TechKnowledge Publications

Head Office : B/5, First floor, Maniratna Complex, Taware Colony, Aranyeshwar Corner,
Pune - 411 009. Maharashtra State, India
Ph : 91-20-24221234, 91-20-24225678.
Email : info@techknowledgebooks.com,
Website : www.techknowledgebooks.com

[CSC503] (FID : MO45) (Book Code : MO45A)

Scanned by CamScanner

Syllabus...

Computer Networks : Sem. V, (Computer Engineering (MU))

Module 1

Introduction to Networking :

Introduction to computer network, network application, network software and hardware components (Interconnection networking devices), Network topology, protocol hierarchies, design issues for the layers, connection oriented and connectionless services. Reference models: Layer details of OSI, TCP/IP models. Communication between layer. **(Refer chapter 1)**

Module 2

Physical Layer :

Introduction to Communication System, digital Communication, Electromagnetic Spectrum, Guided **Transmission Media :** Twisted pair, Coaxial, Fiber optics. Unguided media (Wireless Transmission): Radio Waves, Microwave, Bluetooth, Infrared, Circuit and Packet Switching. **(Refer chapter 2)**

Module 3

Data Link Layer :

DLL Design Issues (Services, Framing, Error Control, Flow Control), Error Detection and Correction (Hamming Code, CRC, Checksum); Elementary Data Link protocols, Stop and Wait, Sliding Window (Go Back N, Selective Repeat), HDLC, **Medium Access Control sublayer :** Channel Allocation problem, Multiple access Protocol (Aloha, Carrier Sense Multiple Access (CSMA/CD), Local Area Networks - Ethernet (802.3)

(Refer chapters 3 and 4)

Module 4

Network layer :

Network Layer design issues, Communication Primitives: Unicast, Multicast, Broadcast. IPv4 Addressing (classfull and classless), Subnetting, Supernetting design problems, IPv4 Protocol, Network Address Translation (NAT), **Routing algorithms :** Shortest Path (Dijkastra's), Link state routing, Distance Vector Routing, **Protocols - ARP, RARP, ICMP, IGMP Congestion control algorithms :** Open loop congestion control, Closed loop congestion control, QoS parameters, Token & Leaky bucket algorithms. **(Refer chapter 5)**

Module 5

Transport Layer :

The Transport Service : Transport service primitives, Berkeley Sockets, Connection management (Handshake), UDP, TCP, TCP state transition, TCP timers, TCP Flow control (sliding Window), TCP Congestion Control: Slow Start. **(Refer Chapter 6)**

Module 6

Application Layer :

DNS: Name Space, Resource Record and Types of Name Server. HTTP, SMTP, Telnet, FTP, DHCP.

(Refer chapter 7)

□□□

Scanned by CamScanner

Module 1

Chapter 1 : Introduction to Networking 1-1 to 1-44

Syllabus : Introduction to computer network, Network application, Network software and hardware components (Interconnection networking devices), Network topology, Protocol hierarchies, Design issues for layers, Connection oriented and connectionless services, Reference models : Layer details of OSI, TCP/IP models, Communication between the layers.

1.1 Introduction 1-1
- 1.1.1 Introduction to Computer Networks 1-1
- 1.1.2 Need and Applications of Computer Network 1-2
- 1.1.3 Components of a Computer Network 1-2

1.2 Network Benefits 1-2
- 1.2.1 Sharing Information 1-2
- 1.2.2 Sharing Resources 1-2
- 1.2.3 Facilitating Centralized Management 1-3
- 1.2.4 Other Benefits of Computer Networks 1-4
- 1.2.5 Disadvantages of Networks 1-4

1.3 Network Services 1-4
- 1.3.1 Service Provided by the Network for Organizations 1-4
- 1.3.2 Services Provided by the Network to People 1-5

1.4 Network Topology Types 1-5
- 1.4.1 Bus Topology 1-6
- 1.4.2 Ring Topology 1-7
- 1.4.3 Star Topology 1-8
- 1.4.4 STAR LANs 1-8
- 1.4.5 Mesh Topology 1-9
- 1.4.6 Tree Topology 1-9
- 1.4.7 Logical Topology 1-10
- 1.4.8 Comparison of Ring and Star Topologies 1-10
- 1.4.9 Comparison of Bus and Star Topologies 1-10
- 1.4.10 Hybrid Topology 1-10
- 1.4.11 Comparison of Star Bus and Star Ring Topologies 1-11

1.5 Line Configurations 1-11
- 1.5.1 Type of Connections (Topology) 1-11
- 1.5.2 Point-to-Point Connection 1-11
- 1.5.3 Multipoint Connection 1-11

1.6 Types of Communication Simplex, Half Duplex, Duplex 1-11

1.7 Network Hardware 1-12
- 1.7.1 Types of Transmission Technology 1-12

1.8 Network Scale 1-12

1.9 Network Classification by their Geography (Categories of Networks) 1-12
- 1.9.1 Local Area Networks (LAN) 1-13
- 1.9.2 Metropolitan Area Network (MAN) 1-14
- 1.9.3 Wide Area Network (WAN) 1-14
- 1.9.4 Wireless Networks 1-15
- 1.9.5 Internetworks 1-16
- 1.9.6 Comparison of LAN, WAN and MAN 1-16
- 1.9.7 Network Classification by their Component Role 1-16
- 1.9.8 Peer-to-Peer Networks 1-16
- 1.9.9 Client / Server Network (Server Based Network) 1-17
- 1.9.10 Factors Influencing the Choice of Network 1-19
- 1.9.11 Comparison between Peer-to-Peer Network and Client-Server Network 1-19
- 1.9.12 Network Features 1-19
- 1.9.13 Layered Tasks 1-19

1.10 Network Software 1-20
- 1.10.1 Protocol Hierarchies (Layered Architecture) 1-20
- 1.10.2 Reasons for having Layered Protocols and its Benefits 1-20
- 1.10.3 Disadvantages of Layered Architecture 1-21
- 1.10.4 How does Data Transfer take Place ? 1-21

1.11 Network Architecture 1-21
- 1.11.1 Virtual Communication between Layers 1-21

1.12 Design Issues for the Layers 1-22
- 1.12.1 Addressing 1-22
- 1.12.2 Direction of Transmission 1-22
- 1.12.3 Error Control 1-23
- 1.12.4 Avoid Loss of Sequencing 1-23
- 1.12.5 Ability of Receiving Long Messages 1-23
- 1.12.6 To use Multiplexing and Demultiplexing 1-23

1.13 Interfaces and Services 1-23
- 1.13.1 Entities and Peer Entities 1-24

Scanned by CamScanner

1.13.2 Service Provider and Service User 1-24
1.13.3 Service Access Points (SAPs) 1-24
1.13.4 Interface Data Unit (IDU) 1-24
1.13.5 Service Data Unit (SDU) 1-24
1.13.6 Protocol Data Unit (PDU) 1-24
1.14 Connection Oriented and Connectionless Services 1-24
1.14.1 Connection Oriented Service 1-25
1.14.2 Connectionless Service 1-25
1.14.3 Comparison of Connection Oriented and Connectionless Services 1-25
1.14.4 Quality of Service (QoS) 1-25
1.14.5 Service Primitives 1-26
1.15 Relationship of Services to Protocols 1-26
1.15.1 Service 1-26
1.15.2 Protocol 1-26
1.16 Reference Models 1-26
1.17 OSI Model 1-27
1.17.1 Functions of Different Layers 1-28
1.17.2 Exchange of Information using the OSI Model 1-29
1.17.3 Physical Layer 1-30
1.17.4 Data Link Layer 1-30
1.17.5 Network Layer 1-31
1.17.6 Transport Layer 1-32
1.17.7 The Session Layer 1-32
1.17.8 Presentation Layer 1-33
1.17.9 Application Layer 1-34
1.17.10 Merits of OSI Reference Model 1-34
1.17.11 Demerits of OSI Model 1-34
1.18 TCP/IP Protocol Suite 1-34
1.18.1 Layered Architecture 1-34
1.18.2 Layers in the TCP/IP Protocol Suite 1-35
1.19 Detailed Description of Each Layer in TCP/IP 1-36
1.19.1 Detailed Introduction to Physical Layer 1-36
1.19.2 Detailed Introduction to Data Link Layer 1-36
1.19.3 Detailed Introduction to Network Layer 1-37
1.19.4 Detailed Introduction to Transport Layer 1-37
1.19.5 Detailed Introduction to Application Layer 1-38
1.20 Encapsulation and Decapsulation 1-38
1.20.1 Encapsulation at the Source Host 1-39
1.20.2 Decapsulation and Encapsulation at the Router 1-39
1.20.3 Decapsulation at the Destination Host 1-39
1.21 Addressing in TCP/IP 1-40
1.22 Multiplexing and Demultiplexing in TCP/ IP 1-40
1.23 Comparison of OSI and TCP/IP Models 1-41
1.23.1 Similarities between OSI and TCP/IP Models 1-41
1.23.2 Difference between OSI & TCP/IP 1-41
1.23.3 Demerits of TCP/IP Model 1-41
1.23.4 Hybrid (Internet) Reference Model 1-41
1.24 Addressing 1-42
1.24.1 MAC Address (Physical Address) 1-42
1.24.2 Logical Addresses (IP Addresses) 1-42
1.24.3 Port Address 1-43
1.24.4 Specific Addresses 1-43
1.25 University Questions and Answers (New Syllabus) 1-44
• **Review Questions** 1-43

Module 2

Chapter 2 : Physical Layer 2-1 to 2-32

Syllabus : Introduction to communication system, Digital communication, Electromagnetic spectrum, Guided transmission media : Twisted pair, Coaxial, Fiber optics, Unguided media (Wireless transmission) : Radio waves, Microwave, Bluetooth, Infrared, Circuit and packet switching.

2.1 Introduction to Communication System 2-1
2.1.1 Elements of Communication System 2-1
2.2 The Electromagnetic Spectrum 2-2
2.2.1 Different Frequency Bands 2-3
2.2.2 Frequency and Wavelength 2-3
2.2.3 Infrared Signals 2-3
2.2.4 Visible Light 2-4
2.3 Digital Communication 2-4
2.3.1 Advantages of Digital Communication 2-4
2.3.2 Disadvantages 2-4
2.3.3 Digital Communication System 2-4
2.4 Introduction to Physical Layer 2-5
2.4.1 Physical Layer Design Issues 2-5
2.4.2 Transmission Media and Physical Layer 2-6
2.5 Transmission Media 2-6

Scanned by CamScanner

2.5.1 Classification of Transmission Media 2-6
2.5.2 Wired Media (Guided Media) 2-7
2.5.3 Wireless Media (Unguided Media) 2-7
2.5.4 Comparison of Wired and Wireless Media 2-7
2.5.5 Guided Media 2-7
2.6 Twisted Pair Cables 2-7
2.6.1 Types of Twisted Pair Cables 2-7
2.6.2 Characteristics of STP 2-8
2.6.3 Categories of UTP 2-8
2.6.4 Characteristics of UTP 2-9
2.6.5 Applications of Twisted Pair Cables 2-9
2.6.6 Comparison of Twisted Pair Cables 2-9
2.6.7 Connectors 2-9
2.6.8 Connector for Twisted Pair Cable 2-10
2.7 Co-axial Cables 2-10
2.7.1 Characteristics of a Co-axial Cable 2-10
2.7.2 Co-axial Cable Standards 2-11
2.7.3 Applications of Co-axial Cables 2-11
2.7.4 Advantages of Co-axial Cable 2-11
2.7.5 Disadvantages 2-11
2.7.6 Baseband Co-axial Cable 2-11
2.7.7 Broadband Co-axial Cable 2-11
2.7.8 Connector for Co-axial Cable 2-11
2.8 Optical Fiber Cables 2-12
2.8.1 Light Sources for Fiber 2-12
2.8.2 Principle of Light Propagation in a Fiber 2-12
2.8.3 Relation between Incident Angle and Emerging Angle 2-13
2.8.4 Modes of Propagation 2-13
2.8.5 Single Mode Fibers 2-13
2.8.6 Multimode Fibers 2-14
2.8.7 Comparison of Step Index and Graded Index Fibers 2-15
2.8.8 Comparison of Single Mode and Multimode Fibers 2-15
2.8.9 Characteristics of Optical Fiber Cables 2-15
2.8.10 Advantages of Optical Fibers 2-16
2.8.11 Disadvantages of Optical Fiber 2-16
2.8.12 Applications 2-16
2.8.13 Fiber Optic Cable Connectors 2-16
2.8.14 Comparison of Wired Media 2-17
2.9 Unguided (Wireless) Media 2-17
2.9.1 EM Spectrum for Wireless Media 2-17
2.9.2 Propagation Methods 2-17
2.9.3 Bands 2-17
2.9.4 EM Spectrum and Communication Applications 2-18
2.9.5 Infrared Signals 2-18
2.9.6 Visible Light 2-19
2.10 Types of Wireless Media 2-19
2.10.1 Radio Wave Transmission Systems 2-19
2.10.2 Microwave Transmission System 2-20
2.11 Use of Infrared Light for Transmission 2-21
2.11.1 Applications and Standards 2-21
2.11.2 Comparison of Point to Point and Broadcast Infrared System 2-22
2.11.3 Applications of Infrared 2-22
2.12 Bluetooth 2-22
2.12.1 Architecture 2-22
2.12.2 Piconets 2-22
2.12.3 Scatternet 2-23
2.12.4 Bluetooth Devices 2-23
2.12.5 Bluetooth Layers (Bluetooth Protocol Architecture) 2-23
2.12.6 TDMA 2-24
2.12.7 Logical Link Control and Adaptation Protocol (L2CAP) 2-24
2.12.8 Frame Format 2-24
2.12.9 Data (Payload) Field 2-24
2.12.10 Security Limitations in Bluetooth 2-25
2.12.11 Bluetooth Advantages 2-25
2.13 Introduction to Switching 2-25
2.13.1 Switching Methods 2-25
2.14 Circuit Switching Networks 2-25
2.14.1 Three Phases 2-26
2.14.2 Efficiency 2-26
2.14.3 Delay 2-26
2.14.4 Advantages 2-27
2.14.5 Disadvantages 2-27
2.14.6 Circuit Switched Technology in Telephone Networks 2-27
2.15 Packet Switching 2-27
2.15.1 Datagram Packet Switching 2-27
2.15.2 Routing Table 2-28
2.15.3 Efficiency 2-28
2.15.4 Delay 2-28
2.15.5 Advantages of Packet Switching 2-28

Scanned by CamScanner

2.15.6 Disadvantages of Packet Switching 2-29
2.15.7 Datagram Networks In Internet 2-29
2.16 Virtual Circuit Packet Switching 2-29
2.16.1 Addressing 2-29
2.16.2 Three Phases of Communication 2-30
2.16.3 Efficiency 2-30
2.16.4 Delay 2-30
2.16.5 Circuit Switched Technology in WANs 2-30
2.16.6 Advantages of Virtual Circuit Packet Switching 2-30
2.16.7 Disadvantages of Virtual Circuit Packet Switching 2-30
2.16.8 Comparison of Datagram and Virtual Circuits 2-31
2.17 Comparison of Circuit and Packet Switching 2-31
2.18 University Questions and Answers (New Syllabus) 2-32
• **Review Questions** 2-31

Module 3

Chapter 3 : Data Link Layer 3-1 to 3-47

Syllabus : DLL design issues (Services, Framing, Error control, flow control) Error detection and correction (Hamming code, CRC, Checksum), Elementary data link layer protocols, Stop and wait, Sliding window (Go back-N, Selective repeat), HDLC.

3.1 Introduction 3-1
3.1.1 Position of Data Link Layer 3-1
3.2 Data Link Layer Design Issues (Functions of Data Link Layer) 3-1
3.3 Services Provided to Network Layer 3-2
3.3.1 Types of Services Provided 3-2
3.3.2 Unacknowledged Connectionless Service 3-2
3.3.3 Acknowledged Connectionless Service 3-2
3.3.4 Acknowledged Connection Oriented Service 3-3
3.4 Framing 3-3
3.4.1 Framing Methods 3-3
3.4.2 Character Count 3-3
3.4.3 Starting and Ending Character with Character Stuffing 3-4
3.4.4 Character Stuffing 3-4
3.4.5 Starting and Ending Flags, with Bit Stuffing 3-5
3.4.6 Physical Layer Coding Violations 3-6
3.5 Error Control 3-7
3.5.1 Function of a Timer 3-7
3.6 Error Detection and Correction 3-7
3.6.1 Important Definitions Related to Codes 3-8
3.6.2 Error Detection 3-9
3.6.3 Error Detection Methods 3-9
3.6.4 Parity 3-9
3.6.5 Two Dimensional Parity Check 3-11
3.6.6 Cyclic Redundancy Check (CRC) 3-12
3.6.7 Error Correction 3-14
3.6.8 Linear Block Codes 3-15
3.6.9 Hamming Codes 3-15
3.6.10 Solved Examples 3-19
3.6.11 ARQ Technique 3-23
3.7 Flow Control 3-24
3.8 Elementary Data Link Protocols 3-24
3.8.1 An Unrestricted Simplex Protocol 3-24
3.8.2 A Simplex Stop and Wait Protocol 3-25
3.8.3 A Simplex Protocol for Noisy Channel 3-25
3.8.4 Piggybacking 3-26
3.9 Sliding Window Protocols 3-26
3.9.1 A One Bit Sliding Window Protocol (Stop and Wait ARQ) 3-29
3.9.2 A Protocol using GO Back n 3-31
3.9.3 Pipelining 3-33
3.9.4 Selective Repeat ARQ 3-33
3.9.5 Protocol Performance 3-34
3.9.6 Comparison of Sliding Window Protocols 3-34
3.10 Other Data Link Protocols 3-36
3.11 High Level Data Link Control (HDLC) Protocol 3-36
3.11.1 Frame Structure in HDLC 3-37
3.11.2 Frame Types in HDLC 3-37
3.11.3 Transparency in HDLC 3-38
3.11.4 Bit Stuffing 3-38

Scanned by CamScanner

3.12 Why is CRC in Data Link Protocols in Trailer and not in Header ? 3-39
3.13 Solved Examples 3-39
3.14 SLIP-Serial Line IP 3-42
3.15 Point-to-Point Protocol (PPP) 3-43
3.15.1 Services Provided by PPP 3-43
3.15.2 Frame Format of PPP 3-43
3.15.3 Transition Phases 3-44
3.15.4 Multiplexing 3-44
3.15.5 PPP Stack 3-45
3.15.6 Link Control Protocol (LCP) 3-45
3.15.7 Authentication Protocols 3-45
3.15.8 Network Control Protocol (NCP) 3-45
3.15.9 Multilink PPP 3-45
3.15.10 Difference between SLIP and PPP 3-46
3.16 University Questions and Answers 3-46
3.17 University Questions and Answers (New Syllabus) 3-47
• **Review Questions** 3-46

Module 3

Chapter 4 : Medium Access Control Layer & LAN **4-1 to 4-39**

Syllabus : Channel allocation problem, Multiple access, Protocol (ALOHA, Carrier sense multiple access (CSMA/CD), Local Area Networks - Ethernet (802.3).

4.1 Introduction 4-1
4.1.1 MAC and LLC Sublayers 4-1
4.2 The Channel Allocation Problem 4-1
4.2.1 Static Channel Allocation in LANs and MANs 4-2
4.2.2 Dynamic Channel Allocation 4-2
4.3 Multiple Access 4-2
4.3.1 Random Access 4-2
4.3.2 Evolution of Random Access Methods 4-2
4.4 Multiple Access (ALOHA System) 4-3
4.4.1 Pure ALOHA 4-3
4.4.2 Protocol Flow Chart for ALOHA 4-3
4.4.3 Efficiency of an ALOHA Channel 4-4
4.4.4 Slotted ALOHA 4-4
4.4.5 Comparison of Pure and Slotted ALOHA 4-5
4.5 Carrier Sense Multiple Access (CSMA) 4-6
4.5.1 Carrier Sense Multiple Access/Collision Detection (CSMA/CD) 4-6
4.5.2 CSMA/CD Procedure 4-7
4.5.3 CSMA/CA 4-8
4.6 Collision Free Protocols 4-8
4.6.1 Bit-map Protocol 4-8
4.6.2 Binary Countdown 4-9
4.6.3 Limited Contention Protocols 4-9
4.6.4 The Adaptive Tree Walk Protocol 4-10
4.7 Controlled Access 4-10
4.7.1 Reservation Systems 4-10
4.7.2 Polling 4-11
4.7.3 Token Passing 4-12
4.8 Channelization 4-12
4.8.1 FDMA 4-12
4.8.2 TDMA 4-13
4.8.3 Code Division Multiple Access (CDMA) 4-13
4.8.4 Comparison of FDMA, TDMA and CDMA 4-14
4.9 Ethernet 4-14
4.9.1 Traditional Ethernet 4-15
4.9.2 Bridged Ethernet 4-15
4.9.3 Switched Ethernet 4-15
4.9.4 Full Duplex Ethernet 4-15
4.9.5 Fast Ethernet 4-15
4.9.6 Gigabit Ethernet 4-15
4.10 IEEE Standards 4-16
4.11 Traditional Ethernet (IEEE 802.3) 4-16
4.11.1 Traditional Ethernet Frame 4-16
4.11.2 Frame Length 4-17
4.11.3 Addressing 4-17
4.11.4 Types of Addresses 4-17
4.11.5 Physical Properties of Ethernet 4-17
4.11.6 Physical Layer Implementation of Traditional Ethernet 4-18
4.12 Changes in the Standards 4-18
4.13 Bridged Ethernet 4-19
4.14 Switched and Full Duplex Ethernet 4-19
4.14.1 Switched Ethernet 4-19
4.14.2 Full Duplex Ethernet 4-20
4.15 Fast Ethernet 4-20
4.15.1 Autonegotiation 4-20
4.15.2 Physical Layer Implementation 4-20

Scanned by CamScanner

4.16 Gigabit Ethernet 4-21
4.16.1 MAC Sublayer 4-21
4.16.2 Physical Layer 4-22
4.16.3 Physical Layer Implementation 4-22
4.16.4 Ten Gigabit Ethernet 4-22
4.17 Solved Examples 4-23
4.18 Data Link Layer Switching 4-26
4.19 LAN Bridges 4-26
4.19.1 802 Bridges 4-27
4.19.2 Transparent Bridges 4-27
4.19.3 Source Routing Bridges 4-28
4.19.4 Comparison of Transparent and Source Routing Bridge 4-29
4.19.5 Remote Bridges 4-29
4.19.6 Loop Problem in Bridge LAN 4-30
4.20 Mixed Media Bridges 4-31
4.21 NIC (Network Interfacing Card) 4-31
4.21.1 NIC Operation 4-31
4.22 Transceivers 4-32
4.23 Network Connecting Devices 4-32
4.24 Hubs 4-33
4.24.1 Passive Hubs 4-34
4.24.2 Active Hubs 4-34
4.24.3 Intelligent Hubs 4-34
4.25 Repeaters 4-34
4.26 Bridges 4-35
4.27 Routers 4-36
4.28 Gateways 4-36
4.29 Switches 4-37
4.29.1 Two Layer Switch 4-38
4.29.2 Three Layer Switch 4-38
4.29.3 Comparison of Hub and Switch 4-38
4.29.4 Media Converters 4-38
4.29.5 Comparison of Router and Bridge 4-39
4.29.6 Comparison of Bridge, Switch and Hub 4-39
4.30 University Questions and Answers 4-39
4.31 University Questions and Answers (New Syllabus) 4-39
• **Review Questions** 4-39

Module 4

Chapter 5 : Network Layer 5-1 to 5-98

Syllabus : Network layer design issues, Communication primitives : Unicast, Multicast, Broadcast, IPv4 addressing (Classful and classless), Subnetting, Supernetting design problems, IPv4 protocol, Network Address Translation (NAT). **Routing algorithms :** Shortest path (Dijkastra's), Link state routing, Distance vector routing, **Protocols :** ARP, RARP, ICMP, IGMP, **Congestion control algorithms :** Open loop congestion control, Closed loop congestion control, QoS parameters, Token and leaky bucket algorithms.

5.1 Network Layer 5-1
5.1.1 Position of Network Layer 5-1
5.1.2 Network Layer Duties 5-1
5.2 Network Layer Design Issues 5-2
5.2.1 Store and Forward Packet Switching 5-2
5.2.2 Services Provided to the Transport Layer 5-3
5.2.3 Implementation of Connectionless Service 5-3
5.2.4 Implementation of Connection-Oriented Service 5-3
5.2.5 Internal Organization of the Network Layer 5-4
5.2.6 Comparison of Virtual Circuit and Datagram Subnets 5-4
5.3 Delivery 5-5
5.3.1 Direct Delivery 5-5
5.3.2 Indirect Delivery 5-5
5.4 Forwarding 5-5
5.4.1 Forwarding Techniques 5-5
5.4.2 Next Hop Method Versus Route Method 5-5
5.4.3 Network Specific Method Versus Host Specific Method 5-5
5.4.4 Default Method 5-6
5.4.5 Forwarding Process 5-6
5.5 Routers 5-6
5.5.1 Routing Tables 5-7
5.5.2 Unicast Routing 5-7
5.5.3 Broadcast Routing 5-8

Scanned by CamScanner

5.5.4 Multicast Routing 5-8
5.6 Network Layer Services 5-8
5.6.1 Logical Addressing 5-9
5.6.2 Services Provided at the Source Computer 5-9
5.6.3 Services Provided at Each Router 5-10
5.6.4 Services Provided at the Destination Computer 5-10
5.7 Other Services 5-10
5.7.1 Error Control 5-10
5.7.2 Flow Control 5-10
5.7.3 Congestion Control 5-11
5.7.4 Quality of Service (QoS) 5-11
5.7.5 Security 5-11
5.8 IPv4 Addresses 5-11
5.8.1 Uniqueness of IP Addresses 5-11
5.8.2 Address Space 5-11
5.8.3 Notation 5-11
5.8.4 IPv4 Address Format 5-12
5.9 Classful Addressing 5-12
5.9.1 IPv4 Address Classes 5-12
5.9.2 Formats of Various Classes 5-12
5.9.3 How to Recognize Classes ? 5-13
5.9.4 Two Level Addressing 5-14
5.9.5 Extracting Information in a Block 5-14
5.9.6 Network Address 5-14
5.9.7 Network Mask or Default Mask 5-15
5.9.8 Default Masks for Different Classes 5-16
5.9.9 Finding Network Address using Default Mask 5-16
5.9.10 Three Level Addressing Subnetting 5-16
5.9.11 Special IP Addresses 5-17
5.9.12 Limitations of IPv4 5-17
5.9.13 Classless Addressing 5-18
5.9.14 Supernetting 5-18
5.9.15 Who Decides the IP Addresses ? 5-18
5.9.16 Registered and Unregistered Addresses 5-18
5.9.17 Solved Examples 5-19
5.10 Classless Addressing in IPv4 5-24
5.10.1 Variable Length Blocks 5-24
5.10.2 The Slash Notation (CIDR Notation) 5-25
5.10.3 Network Mask 5-26
5.10.4 Extracting the Block Information 5-26
5.10.5 Block Allocation 5-28
5.10.6 Relation to Classful Addressing 5-28
5.10.7 Subnetting 5-29
5.10.8 Designing Subnets 5-29
5.10.9 Finding Information about Each Network 5-29
5.10.10 Address Aggregation 5-30
5.11 Special Addresses 5-31
5.11.1 Special Blocks 5-31
5.11.2 All Zeros Address 5-31
5.11.3 All one Address-Limited Broadcast Address 5-31
5.11.4 Loopback Address 5-31
5.11.5 Private Addresses 5-31
5.11.6 Multicast Addresses 5-31
5.11.7 Special Addresses in Each Block 5-31
5.11.8 Network Address 5-31
5.11.9 Direct Broadcast Address 5-31
5.12 NAT – Network Address Translation 5-31
5.13 Internet Protocol Version 4 (IPv4) 5-32
5.13.1 Position of IP 5-32
5.13.2 Internet Protocol (IP) 5-32
5.13.3 Datagrams 5-33
5.13.4 IPv4 Header Format 5-33
5.14 Fragmentation 5-36
5.14.1 Maximum Transfer Unit (MTU) 5-36
5.14.2 Fields Related to Fragmentation 5-36
5.15 Options 5-37
5.15.1 Format 5-37
5.16 Option Types 5-37
5.16.1 No Operation Option 5-38
5.16.2 End of Option Option 5-38
5.16.3 Record-Route Option 5-38
5.16.4 Strict-Source-Route Option 5-38
5.16.5 Loose-Source-Root Option 5-38
5.16.6 Time Stamp Option 5-39
5.17 Checksum 5-39
5.17.1 Checksum Calculation at the Sender 5-39
5.17.2 Checksum Calculation at the Receiver 5-39
5.18 Routing 5-39
5.18.1 Types of Routing 5-40
5.18.2 Intra and Interdomain Routing 5-40
5.18.3 Unicast Routing 5-40
5.18.4 Broadcast Routing 5-41
5.18.5 Multicast Routing 5-41

Scanned by CamScanner

5.19 Routing Algorithms 5-41
5.19.1 Desired Properties of a Routing Algorithm 5-41
5.19.2 Types of Routing Algorithms 5-41
5.19.3 Optimality Principle 5-42
5.20 Static Algorithms 5-42
5.20.1 Shortest Path Routing 5-42
5.20.2 Dijkstra's Algorithm 5-43
5.20.3 Flooding 5-46
5.21 Dynamic Routing Algorithms 5-46
5.21.1 Distance Vector Routing Algorithm 5-46
5.21.2 Count to Infinity Problem 5-49
5.21.3 Link State Routing 5-50
5.21.4 Comparison of Link State Routing and Distance Vector Routing 5-51
5.21.5 Hierarchical Routing 5-51
5.22 Network Layer Protocols 5-53
5.23 Addressing 5-53
5.23.1 MAC Address (Physical Address) 5-53
5.23.2 Logical Addresses (IP Addresses) 5-54
5.23.3 Port Address 5-54
5.23.4 Specific Addresses 5-54
5.23.5 Address Mapping 5-54
5.23.6 Mapping of IP Address to a MAC Address (ARP) 5-55
5.24 Address Resolution Protocol (ARP) 5-55
5.24.1 Address Mapping 5-55
5.24.2 The ARP Protocol 5-56
5.24.3 ARP Cache Memory 5-57
5.24.4 ARP Packet Format 5-57
5.24.5 Encapsulation 5-57
5.24.6 Operation of ARP on Internet 5-57
5.24.7 Four Different Cases 5-58
5.24.8 Proxy ARP 5-58
5.25 Mapping Physical Address to Logical Address 5-58
5.25.1 The Reverse Address Resolution (RARP) Protocol 5-58
5.26 ICMPv4 (Internet Control Message Protocol) 5-59
5.26.1 ICMP Encapsulation 5-59
5.26.2 ICMP Messages 5-59
5.26.3 Message Format 5-59
5.27 Error Reporting Messages (ICMPv4) 5-60
5.27.1 Destination Unreachable 5-60
5.27.2 Source Quench Error Message 5-61
5.27.3 Time Exceeded Error Message 5-61
5.27.4 Parameter Problem Error Message 5-62
5.27.5 Redirection Error Message 5-62
5.28 Query Messages (ICMPv4) 5-63
5.28.1 Echo Request and Reply 5-63
5.28.2 Timestamp Request and Reply 5-63
5.28.3 Deprecated Messages 5-64
5.28.4 Checksum 5-64
5.29 IGMP (Internet Group Management Protocol) 5-64
5.29.1 Messages 5-64
5.29.2 Operation of IGMP 5-65
5.29.3 How to Join a Group ? 5-65
5.29.4 How to Leave a Group ? 5-66
5.29.5 Monitoring Membership 5-66
5.29.6 Query Router 5-66
5.29.7 IGMP Messages 5-66
5.29.8 Multicast Forwarding 5-67
5.29.9 Multicasting Approaches 5-68
5.30 IPv6 (Next Generation IP) 5-68
5.30.1 IPv6 Packet Format 5-69
5.30.2 Payload 5-69
5.31 IPv6 Addressing 5-70
5.31.1 IPv6 Address 5-70
5.31.2 Notations 5-70
5.31.3 Abbreviation 5-70
5.32 Address Space 5-71
5.32.1 Three Address Types 5-71
5.32.2 Broadcasting and Multicasting 5-72
5.33 Address Space Allocation 5-72
5.33.1 The First Section 5-72
5.33.2 Second Section 5-72
5.33.3 Algorithm 5-73
5.33.4 Assigned or Reserved Blocks 5-73
5.33.5 Unspecified Address 5-73
5.33.6 Loopback Address 5-73
5.33.7 Difference between Loopback Address of IPv4 and IPv6 5-74
5.33.8 Embedded IPv4 Addresses 5-74
5.33.9 Compatible Address 5-74
5.33.10 A Mapped Address 5-74
5.33.11 Calculation of Checksum 5-74
5.34 Global Unicast Block 5-74
5.34.1 Unique Local Unicast Block 5-74
5.34.2 Link Local Block 5-74

Scanned by CamScanner

5.34.3 Multicast Block 5-75
5.35 Global Unicast Address 5-75
5.35.1 Three Levels of Hierarchy 5-75
5.35.2 Global Routing Prefix 5-75
5.35.3 Autoconfiguration 5-76
5.36 Renumbering 5-76
5.36.1 Migrating to IPv6 (Compatibility to IPv4) 5-76
5.36.2 Comparison between IPv4 and IPv6 5-76
5.36.3 Extension Headers 5-77
5.36.4 Solved Examples 5-78
5.37 Network Layer Congestion 5-83
5.37.1 Congestion 5-84
5.37.2 Need of Congestion Control 5-84
5.37.3 Causes of Congestion 5-84
5.37.4 Difference between Congestion Control and Flow Control 5-85
5.37.5 Principle of Congestion Control 5-85
5.37.6 Congestion Prevention Policies 5-86
5.37.7 Congestion Control in Virtual Circuit Subnets 5-87
5.37.8 Approaches to Congestion Control 5-87
5.37.9 Congestion Control in Datagram Subnets 5-88
5.38 Quality of Service (QoS) 5-90
5.38.1 Techniques for Achieving Good QoS 5-91
5.38.2 Traffic Shaping 5-91
5.38.3 Leaky Bucket Algorithm 5-91
5.38.4 Token Bucket Algorithm 5-92
5.38.5 Comparison of Token Bucket and Leaky Bucket 5-94
5.38.6 Combination of Token Bucket and Leaky Bucket 5-94
5.38.7 Resource Reservation 5-94
5.38.8 Admission Control 5-94
5.38.9 Queuing Disciplines 5-94
5.38.10 FIFO Queuing 5-94
5.38.11 Fair Queuing 5-95
5.38.12 Weighted Fair Queuing 5-95
5.39 University Questions and Answers 5-97
5.40 University Questions and Answers (New Syllabus) 5-98
• **Review Questions** 5-95

Module 5

Chapter 6 : Transport Layer 6-1 to 6-54

Syllabus : The transport service : Transport service primitives, Berkeley sockets, Connection management (Handshakes), UDP, TCP, TCP state transition, TCP timers, TCP flow control (sliding window), TCP congestion control : Slow start.

6.1 Introduction 6-1
6.2 Transport Layer Duties and Functionalities 6-1
6.3 Transport Layer Services 6-2
6.3.1 Process-to-Process Communication 6-2
6.3.2 Addressing Port Number 6-2
6.3.3 Encapsulation and Decapsulation 6-3
6.3.4 Multiplexing and Demultiplexing 6-4
6.3.5 Flow Control 6-4
6.3.6 Flow Control at Transport Layer 6-5
6.3.7 Error Control 6-6
6.3.8 Combination of Flow and Error Control 6-6
6.3.9 Congestion Control 6-7
6.3.10 Connectionless and Connection Oriented Services 6-8
6.3.11 Reliability at Transport Layer Versus Reliability at DLL 6-10
6.3.12 Quality of Service (QoS) 6-10
6.4 Transport Service Primitives 6-11
6.4.1 Nesting of TPDUs, Packets and Frames 6-11
6.5 Sockets 6-12
6.5.1 Socket Types 6-12
6.5.2 Berkeley Sockets 6-13
6.5.3 Connectionless Iterative Server 6-14
6.5.4 Connection Oriented Concurrent Server 6-14
6.6 Transport Layer Protocols 6-15
6.6.1 Simplex Protocol 6-15
6.6.2 Stop and Wait Protocol 6-16
6.6.3 Go Back-N Protocol (GBN) 6-18
6.6.4 Selective Repeat Protocol 6-20

Scanned by CamScanner

6.6.5 Bidirectional Protocols Piggybacking 6-22
6.7 Connection Management 6-22
6.7.1 Connection Establishment 6-22
6.7.2 Three Way Handshake Technique 6-23
6.7.3 Connection Release 6-24
6.8 The Internet Transport Protocols (TCP and UDP) 6-24
6.9 User Datagram Protocol (UDP) 6-25
6.9.1 Responsibilities of UDP 6-25
6.9.2 Advantages of UDP 6-25
6.9.3 User Datagram 6-25
6.9.4 UDP Pseudo Header 6-26
6.10 UDP Services 6-27
6.10.1 Process to Process Communication 6-27
6.10.2 Connectionless Services 6-28
6.10.3 Flow and Error Control 6-28
6.10.4 Checksum 6-28
6.10.5 Congestion Control 6-28
6.10.6 Encapsulation and Decapsulation 6-28
6.10.7 Queuing 6-29
6.10.8 Multiplexing and Demultiplexing 6-29
6.10.9 Comparison of UDP and Generic Simple Protocol 6-30
6.11 UDP Applications 6-30
6.12 UDP Features 6-30
6.12.1 Connectionless Service 6-30
6.12.2 Lack of Error Control 6-30
6.12.3 Lack of Congestion Control 6-30
6.12.4 Typical Applications of UDP 6-30
6.13 Transmission Control Protocol (TCP) 6-30
6.13.1 Relationship Between TCP and IP 6-31
6.13.2 Ports and Sockets 6-31
6.14 TCP Services 6-32
6.14.1 Process to Process Communication 6-32
6.14.2 Stream Delivery Service 6-32
6.14.3 Sending and Receiving Buffers 6-32
6.14.4 Bytes and Segments 6-33
6.14.5 Full Duplex Service 6-33
6.14.6 Connection Oriented Service 6-33
6.14.7 Reliable Service 6-34
6.15 Features of TCP 6-34
6.15.1 Numbering System 6-34
6.15.2 Flow Control 6-34
6.15.3 Error Control 6-34
6.15.4 Congestion Control 6-34
6.16 The TCP Protocol 6-34
6.16.1 TCP Segment 6-35
6.16.2 The TCP Segment Header 6-35
6.16.3 Checksum 6-36
6.16.4 Encapsulation 6-37
6.17 A TCP Connection 6-37
6.17.1 TCP Connection Establishment 6-37
6.17.2 Connection Termination Protocol [Connection Release] 6-37
6.17.3 TCP Connection Management 6-38
6.17.4 TCP Connection Release 6-38
6.18 TCP State Transition Diagram 6-39
6.19 Windows in TCP 6-40
6.19.1 Send Window 6-40
6.19.2 Receive Window 6-41
6.20 Flow Control 6-41
6.20.1 Opening and Closing Windows 6-42
6.20.2 Shrinking of Windows 6-42
6.20.3 An Example of Flow Control 6-42
6.20.4 Silly Window Syndrome 6-43
6.20.5 Nagle's Algorithm 6-43
6.21 TCP Congestion Control 6-44
6.21.1 Slow Start Algorithm 6-45
6.21.2 Internet Congestion Control Algorithm 6-45
6.21.3 Congestion Avoidance (Additive Increase) 6-46
6.22 TCP Timer Management 6-46
6.22.1 Jacobson's Algorithm 6-47
6.22.2 Karn's Algorithm 6-47
6.22.3 Other Timers in TCP 6-47
6.23 Options 6-48
6.23.1 End of Option (EOP) 6-48
6.23.2 No Operation (NOP) 6-48
6.23.3 Maximum Segment Size (MSS) 6-48
6.23.4 Window Scale Factor 6-49
6.23.5 Timestamp 6-49
6.23.6 SACK-Permitted and SACK Options 6-49
6.24 TCP Package 6-50

Scanned by CamScanner

6.24.1 Transmission Control Blocks (TCBs) 6-50
6.24.2 Timers 6-50
6.24.3 Main Module 6-50
6.24.4 Input Processing Module 6-51
6.24.5 Output Processing Module 6-51
6.25 Comparison of UDP and TCP 6-51
6.26 Socket Programming with TCP 6-52
6.26.1 Socket Programming with TCP 6-52
6.26.2 Socket Programming with UDP 6-53
6.27 University Questions and Answers (New Syllabus) 6-54
• **Review Questions** 6-53

Module 6

Chapter 7 : Application Layer 7-1 to 7-37

Syllabus : DNS : Name space, Resource record and types of Name server, HTTP, SMTP, Telnet, FTP, DHCP.

7.1 Introduction 7-1
7.1.1 Position of Application Layer 7-1
7.2 Providing Services 7-2
7.2.1 Standard and Non-standard Protocols 7-2
7.2.2 Standard Protocols (Application Layer) 7-2
7.2.3 Nonstandard Protocols (Application Layer) 7-2
7.3 Application Layer Paradigms 7-2
7.3.1 Traditional Paradigm Client Server 7-2
7.3.2 New Paradigm Peer-to-Peer (P2P) 7-4
7.3.3 Mixed Paradigm 7-4
7.4 Client Server Paradigm 7-4
7.4.1 Application Programming Interface (API) 7-4
7.4.2 Types of APIs 7-5
7.5 Socket 7-5
7.5.1 Socket Interface 7-5
7.5.2 Socket Address 7-5
7.5.3 Finding Socket Addresses 7-6
7.5.3.1 At The Server Site 7-6
7.5.3.2 At the Client Site 7-6
7.6 Using the Services of The Transport Layer 7-7
7.6.1 Users Datagram Protocol (UDP) 7-7
7.6.2 TCP Protocol 7-7
7.6.3 SCTP Protocol 7-7
7.7 Standard Client Server Applications 7-7
7.8 Domain Name System (DNS) 7-8
7.8.1 How does DNS Work ? 7-8
7.8.2 Name Space 7-8
7.8.3 Flat Name Space 7-8
7.8.4 Hierarchical Name Space 7-8
7.9 Domain Name Space 7-8
7.10 Distribution of Name Space 7-10
7.10.1 Hierarchy of Name Servers 7-10
7.11 DNS in the Internet 7-11
7.11.1 Generic Domains 7-11
7.11.2 Country Domain 7-11
7.11.3 Inverse Domain 7-11
7.12 Name Address Resolution 7-11
7.12.1 Recursive Resolution 7-11
7.12.2 Iterative Resolution 7-12
7.12.3 The DNS Message Format 7-12
7.12.4 Caching 7-12
7.13 DNS Records 7-12
7.13.1 Question Records 7-13
7.13.2 Resource Record 7-13
7.13.3 Encapsulation 7-13
7.13.4 Registrars 7-13
7.14 DDNS 7-13
7.14.1 Security of DNS 7-14
7.15 World Wide Web (WWW) 7-14
7.15.1 Web from the Users Side 7-14
7.15.2 Web from the Servers Side 7-15
7.15.3 WWW Architecture 7-16
7.15.4 Browser (Web Client) 7-16
7.15.5 Server 7-16
7.15.6 Uniform Resource Locator (URL) 7-17
7.15.7 Cookies User-Server Interaction 7-17
7.16 Web Documents 7-17
7.16.1 Static Documents 7-17
7.16.2 HTML (Hypertext Markup Language) 7-18
7.16.3 Dynamic Document 7-18
7.16.4 Common Gateway Interface (CGI) 7-18
7.16.5 Active Documents 7-18
7.17 HTTP (Hypertext Transfer Protocol) 7-19
7.17.1 Principle of HTTP Operation 7-19
7.17.2 The Web and HTTP 7-20

Scanned by CamScanner

7.17.3 Non-persistent and Persistent Connection 7-20
7.17.4 HTTP Messages 7-21
7.17.5 Request Message 7-21
7.17.6 Methods (Request Type) 7-22
7.17.7 Response Message 7-22
7.17.8 Headers 7-22
7.18 Proxy Server 7-23
7.18.1 HTTP Security 7-23
7.19 File Transfer Protocol (FTP) 7-23
7.19.1 Communication in FTP 7-24
7.19.2 File Types 7-24
7.19.3 Data Structure 7-25
7.19.4 Transmission Mode 7-25
7.19.5 File Transfer 7-25
7.19.6 FTP Commands 7-25
7.19.7 Anonymous FTP 7-25
7.19.8 Security for FTP 7-25
7.20 Message Transfer Agent : SMTP 7-26
7.20.1 Commands and Responses 7-26
7.20.2 SMTP (Simple Mail Transfer Protocol) 7-26
7.20.3 Components of E-mail System 7-26
7.20.4 SMTP Commands 7-27
7.20.5 SMTP Operation 7-27
7.20.6 Comparison of HTTP and SMTP 7-27
7.21 Message Access Agent POP and IMAP 7-28
7.21.1 POP 3 7-28
7.21.2 IMAP4 7-28
7.21.3 Comparison of IMAP and POP 3 7-29
7.22 Remote Login TELNET and SSH 7-29
7.22.1 TELNET 7-29
7.22.2 Network Virtual Terminal (NVT) 7-30
7.22.3 Security Problems of TELNET 7-30
7.22.4 Secure Shell (SSH) 7-31
7.22.5 Port Forwarding 7-31
7.22.6 SSH Packet Format 7-31
7.23 Host Configuration DHCP 7-32
7.23.1 Previously used Protocols 7-32
7.23.2 DHCP 7-32
7.23.3 Advantages of DHCP 7-33
7.23.4 Components of DHCP 7-33
7.23.5 DHCP Operation 7-34
7.23.6 DHCP Operation on Different Networks 7-34
7.23.7 UDP Ports 7-34
7.23.8 Using TFTP 7-35
7.23.9 Error Control 7-35
7.23.10 Optimizations in DHCP 7-35
7.23.11 Packet Format 7-35
7.24 University Questions and Answers (New Syllabus) 7-37
- **Review Questions** 7-37
- **Solved University Question Paper of Dec. 2018** ....Q-1 to Q-3

□□□

Scanned by CamScanner

CHAPTER 1

Module 1

Introduction to Networking

Syllabus :

Introduction to computer network, Network application, Network software and hardware components (Interconnection networking devices), Network topology, Protocol hierarchies, Design issues for layers, Connection oriented and connectionless services, Reference models : Layer details of OSI, TCP/IP models, Communication between the layers.

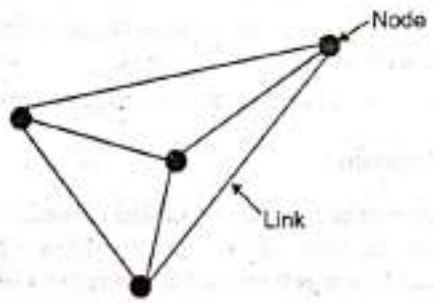
1.1 Introduction :

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 :

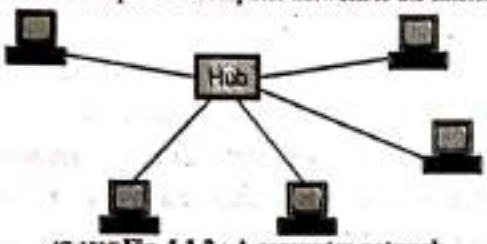
- In contest with the computers we can say that a "computer network" is a system which allows communication among the computers connected in the network.
- During 20th century the most important technology has been the information gathering, its processing and distribution.
- The computers and communications have been merged together and their merger had a very deep impact on the manner in which computer systems are organized.
- In the old model a single computer used to serve all the computational needs of an organization. But now it is replaced by a new model 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 exchange information. The connection between the separate computers can be done via a copper wire, fiber optics, microwaves or communication satellite.

Definition :

- A **computer network** is defined as the interconnection of two or more computers. It is done to enable the computers to communicate and share the available resources.

Scanned by CamScanner

- As shown in Fig. 1.1.2, each node in a computer network is a computer, or a connecting device such as a hub, or a switch etc.
- The computers connected in a network share files, folders, applications and resources like scanners, web-cams, printers etc.
- The best example of a computer network is the Internet.



(G-1395)**Fig. 1.1.2 : A computer network**

- In a computer network we need to make use of hardware and software.
- The **hardware** consists of connecting cables, connectors, network connecting devices and the **software** consists of protocols, programs etc.
- This enables the systematic exchange of information between the computers connected in the network.
- There are various ways of interconnecting the computers.

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 conciously 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 need to 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.

1.1.2 Need and Applications of Computer Network :

The computer networks are needed because of the following points :

1. For sharing the resources such as printers among all the users.
2. For sharing of expensive softwares and database.
3. To facilitate communication from one computer to the other.
4. To have exchange of data and information amongst the users, via the network.
5. For sharing of information over the geographically wide areas.
6. For connecting the computers between various buildings of an organization.
7. For educational purposes.

1.1.3 Components of a Computer Network :

Following are some of the important components of a computer network :

1. Two or more computers.
2. Cables (coaxial, twisted pair or fiber optic) as links between the computers.
3. A Network Interfacing Card (NIC) on each computer.
4. Switches or other suitable connecting device.
5. A software called network operating system.

1.2 Network Benefits :

- A network is supposed to provide its uses some unique capabilities, better than what the individual machines and their software can provide.
- The benefits provided by the network to the users can be divided into two categories as follows :

  1. Sharing 2. Connectivity

1.2.1 Sharing Information :

- Networking allows the users to access the data stored on other's computers.
- It is possible for every user to share his bit of information with the other users over the network.
- The information sharing can be in the form of exchange of data, chatting, sending E-mails, sharing video information, groups etc.
- It is also possible for the users to share the information about various products, movies, technical information, cooking, travel books on internet.
- Sharing of information via Internet has become very common now a days.
- The information which is to be shared or being shared should be shared centrally, it must be kept consistent and secured.
- The access to this stored information should be allowed only to the authorised users.
- Sharing of information eliminates the need of transferring files on CDs or pen drives etc.

1.2.2 Sharing Resources :

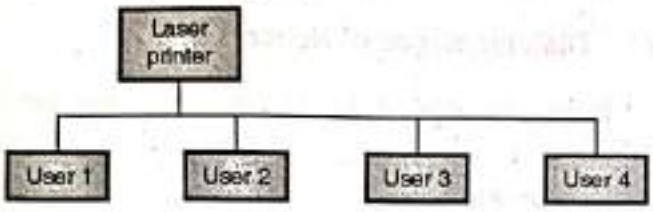
Networks can allow its users to share various types of resources. We can broadly categorise the shared resources as follows :

1. Shared hardware resources
2. Shared software resources

Scanned by CamScanner

1. Sharing of hardware resources :

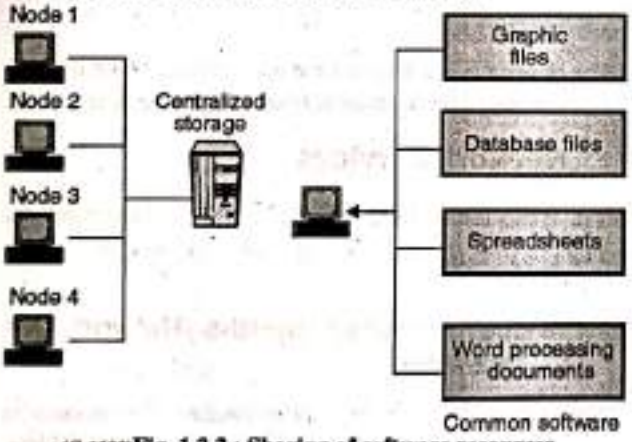
- A network allows its users to share the many hardware devices such as printers, modems, fax machines, CD ROM players etc.
- These resources are available to any one on the network irrespective of the physical location of the resource and the user.
- This will save the expenses on duplication of such hardware resources Fig. 1.2.1 shows a laser printer being shared by many users.



(G-1398)**Fig. 1.2.1 : Sharing of hardware resources**

2. Sharing of software resources :

- With every computer, we need to install some basic software's on each computer's hard disk.
- So each computer on the network will have to purchase a separate copy of each software required to be used. This will increase the cost to be incurred.
- In addition, installing software on each computer is time consuming and difficult.
- This problem can be overcome by using the concept of software resource sharing.
- In a network, we can centrally install and configure only one copy of each software and share it among rest of the computers.
- This actually saves a lot of time and cost Fig. 1.2.2 shows the principle of software sharing.



(G-1399)**Fig. 1.2.2 : Sharing of software resources**

1.2.3 Facilitating Centralized Management :

- The computer network facilitates centralized network management with respect to following :
  1. Management of software
  2. Maintenance of network
  3. Keeping the data back up
  4. Central network security
- All this is allowed by the **client – server** network.

1. Managing software :

- As discussed earlier, it is a very good idea to share the software resources, instead of installing a separate copy of software on each computer.
- It is possible to load all the important software on a single computer (server).
- All the other computers can make use of this centralized software as per their requirements.
- This reduces the expenses in buying the expensive software's for each individual computer. It also makes the virus checks easy.
- We can add new computers on the existing network without purchasing the software's again.
- Thus the network helps in maintaining a centralized software bank.

Maintenance of network :

- The second aspect in the centralized management is the maintenance of network.
- The centralized management allows quick and easy way to the routine maintenance of network.
- The client server networks are maintained centrally. It is an important but difficult job.
- A central administrator keeps track of the status of the network in respect of its speed, traffic, performance and security.
- Some of the network maintenance tools available to help the network maintenance are as follows :
  1. Protocol analyzer.
  2. Event viewer.
  3. Performance monitor.
  4. Network analyzer.
  5. Network management protocol.

Backing up data :

- In the process of data backup, data from computer system is copied from the disk to some other medium for keeping it safe.
- Taking back up periodically is important because it protects the data against any unpredictable, accidental loss of data due to system failure, computer viruses, or human error.
- But taking a backup of individual user's data separately is a time consuming and unorganized.
- Hence in a network, the users first save their important data on the central server and then the backup can be taken on the server data.

Scanned by CamScanner

- This reduces the time and stores the backup data at a signal place only. This makes the data retrieval easy.
- We can have two or three sets of the entire backup data. This helps in the event of one or two sets getting corrupt. The duplication of backup data becomes easily possible due to centralized storage.
- The centralized backup procedures have become easy now a days due to the advanced technology.
- There are two basic network backup strategies :
  1. Isolated backup
  2. Centralized backup
- The operating systems will provide tools required for data backups. For example windows NT proves a tape backup program called as **backup.**
- A proper backup policy which is suitable for the given network should be selected. Some of the backup policies are as follows :
  1. Full backup
  2. Replication
  3. Incremental or partial backup.

1.2.4 Other Benefits of Computer Networks :

Following are some of the other advantages of computer networks.

1. Increased speed :

- Networks provide a very fast means for sharing and transfer of files.
- If the computer networks would not have been there, then we would have to copy the files on CDs or pen drive and send them to the other computers.

2. Reduced cost :

- Many popular versions of softwares usable for the entire network are now available at a considerably reduced costs as compared to individual licensed copies.
- In addition to this it is also possible to share a program on a network. It is also possible to upgrade the program.

3. Improved security :

- It is possible to protect the programs and files from illegal copying.
- By allotting password the access can be restricted to authorised users only.

4. Centralized software managements :

- Due to the use of computer networks, all the softwares can be loaded on one computer.
- All the other computers can make use of this centralized software. It is not necessary to waste time and energy in installing updates and tracking files on independent computers.

5. Electronic-mail :

- The computer network makes the hardware available which is necessary to install an e-mail system.
- The person to person communication is improved due to a presence of e-mail system.

6. Flexible access :

- It is possible for the authorized users to access their files from any computer connected on the network.
- This provides tremendous flexibility in accessing.

1.2.5 Disadvantages of Networks :

Following are some of the disadvantages of computer networks.

1. High cost of installation :

- The initial cost of installation of a computer network is high. This is due to the cost of cables, network cards, computers, printers and various softwares that are required to be installed.
- The cost of services of technicians may also get added.

2. Requires time for administration :

Computer networks need proper and careful administration and maintenance. This is a time consuming job.

3. Failure of server :

- If the file servers "goes down" then the entire network comes to a standstill.
- If this happens then the entire organization can lose its valuable time and access to the necessary programs and files.

4. Cable faults :

The computers in a network are interconnected with the help of connecting cables. So cable faults can paralize a network.

1.3 Network Services :

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

1.3.1 Service Provided by the Network for Organizations :

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

Scanned by CamScanner

- 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 Services Provided by the Network to People :

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

1. Access to remote information
2. Person to person communication
3. E-commerce
4. 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 new groups in which one person posts a message and all other subscribers to the newsgroup can read it or give their feedbacks.

3. Interactive entertainment :

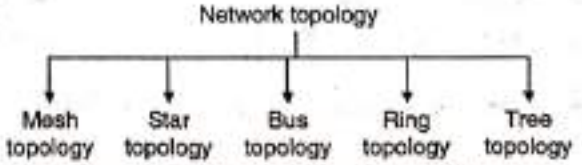
Interactive entertainment includes :

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

1.4 Network Topology Types :

New Syll. : MU : Dec. 18

- 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. 1.4.1.



(G-14) **Fig. 1.4.1 : Classification of network topology**

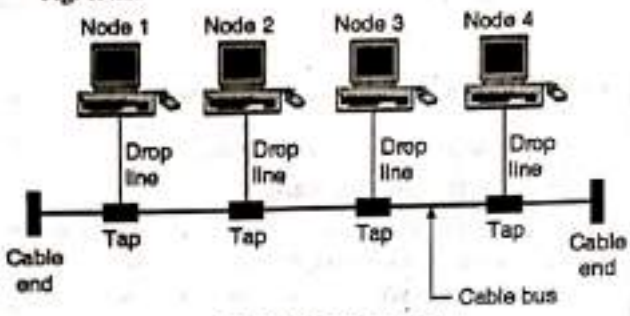
- These topologies can be classified into two types :
  1. Peer to peer
  2. Primary – secondary

Scanned by CamScanner

- 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.

1.4.1 Bus Topology : New Syll. : MU : Dec. 18

- The bus topology is usually used when a network under consideration is small, simple or temporary as shown in Fig. 1.4.2.



(G-18) **Fig. 1.4.2 : 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 50 Ω 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 :

1. 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.
2. The signal strength of the transmitted signal should be adequately high so as to meet the minimum signal strength requirements of the receiver.
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 fibre

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.

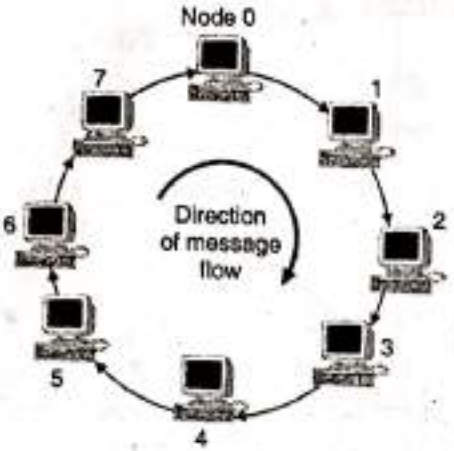
Note :

- Ethernet 10 base 2 also known as thinnet is an inexpensive network based on the bus topology.
- A bus network behaves erratically if it is not terminated or improperly terminated.

Scanned by CamScanner

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

1.4.2 Ring Topology : New Syll. : MU : Dec. 18

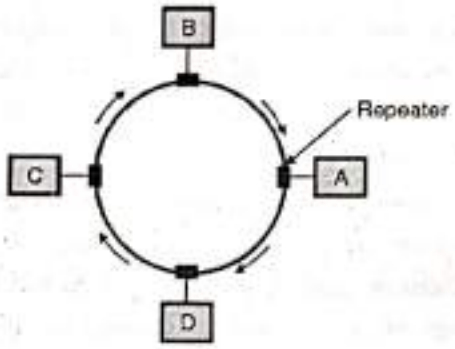


(G-16) **Fig. 1.4.3 : Ring topology**

- In a ring topology, each computer is connected to the next computer, with the last one connected to the first as shown in Fig. 1.4.3.
- 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.
- 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. 1.4.4, which shows that along with the nodes A, B, C, D equal number of repeaters are used and that the transmission is unidirectional.
- The data travels in a sequential manner around the ring. Each repeater will receive regenerate and retransmit this data bit.



(G-17) **Fig. 1.4.4 : Ring topology**

Problems faced in the ring topology :

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

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

Advantages of ring topology :

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

Disadvantages of ring topology :

1. Failure of one computer on the ring can affect the whole network.
2. It is difficult to trouble short the ring.
3. Adding or removing the computers disturbs the network activity.

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

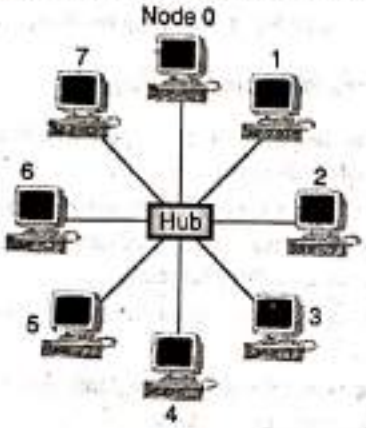
Fibre Distributed Data Interface (FDDI) is a fast fibre-optic network based on the ring topology.

Scanned by CamScanner

1.4.3 Star Topology : New Syll. : MU : Dec. 18

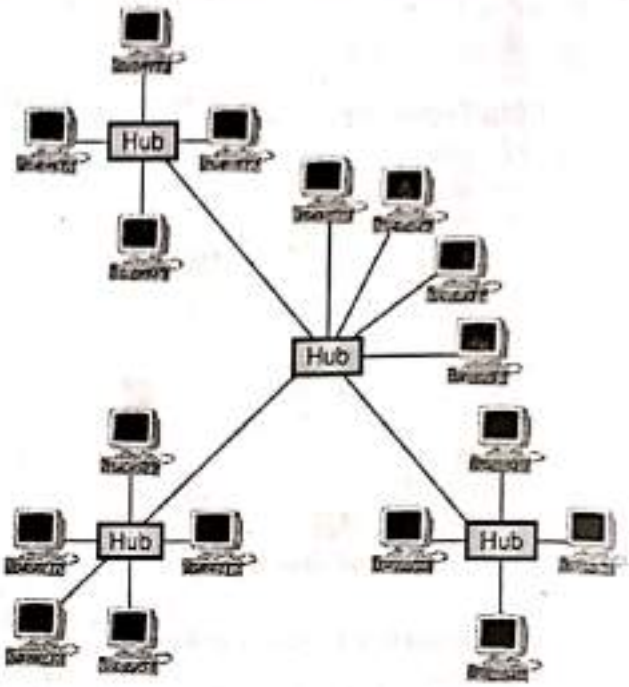
In a star topology all the computers are connected via cables to a central location where they are all connected by a device called a hub as shown in Fig. 1.4.5. There is no direct connections among the computers. All the connections are made via the central hub.

- 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.
- 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.



(G-18) **Fig. 1.4.5 : Star topology**

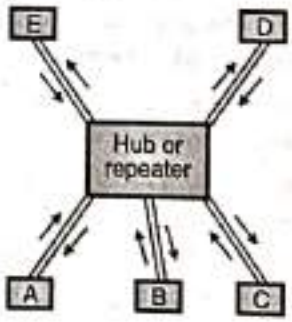
- The hub in a broadcast star network can be active or passive. An active hub generates the electrical signal and sends it to all the computers connected to it.
- This type of hub is usually called a multiport repeater. Active hubs require external power supply.
- A passive hub is a wiring panel or punch 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. 1.4.6.
- This arrangement allows several more computers or hubs to be connected to that hub. This creates a hybrid star network.



(G-19) **Fig. 1.4.6 : Expansion of star topology**

1.4.4 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 :
  1. So no additional installation cost is required for the installation of LAN.
  2. Since the telephone wires cover the entire building it is possible to spread the network in every part of each building.



(G-20) **Fig. 1.4.7 : Single level star topology**

- The basic star topology is as shown in Fig. 1.4.7. This is called as a single level star topology.
- As shown in Fig. 1.4.7, 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.

Scanned by CamScanner

- 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 :

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

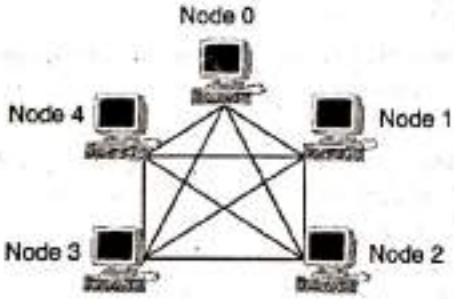
Note : Ethernet 10 base T is a popular network based on the star topology.

Intelligent hubs with microprocessor that implement features in addition to repeating network. Signals provide for centralized monitoring and management of the network.

It is the most flexible and the easiest to diagnose when there is a network fault.

1.4.5 Mesh Topology : New Syll. : MU : Dec. 18

In a mesh topology every device is physically connected to every other device with a point to point dedicated link as shown in Fig. 1.4.8.



(G-21) **Fig. 1.4.8 : Mesh topology**

- 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.

Advantages :

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

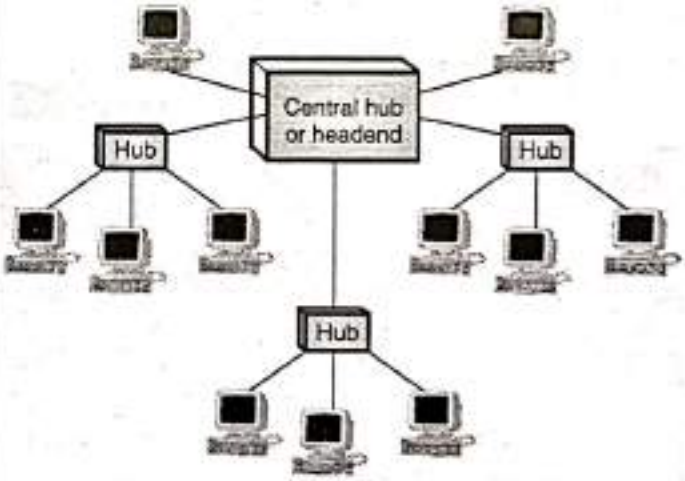
Disadvantages :

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

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

1.4.6 Tree Topology : New Syll. : MU : Dec. 18

- 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. 1.4.9.



(G-22) **Fig. 1.4.9 : Tree topology**

- The central hub in the tree is an active hub which contains repeater. The repeater amplify the signal and increase the distance a signal can travel.
- The secondary hubs may be active or passive. A passive hub provides a simple physical connection between the attached devices.

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.

Scanned by CamScanner

Disadvantages :

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

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

1.4.7 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.

1.4.8 Comparison of Ring and Star Topologies : MU : Dec. 15

University Questions

Q. 1 Compare various types of network topologies. **(Dec. 15, 5 Marks)**

Sr. No.	Ring	Star
1.	Media failure on uni-directional or single loop ring causes complete network failure.	Media faults are automatically isolated to the failed segment.
2.	Relatively difficult to reconfigure.	Relatively easy to configure.
3.	It is difficult to troubleshoot.	Easy to troubleshoot.
4.	The failure of one computer can affect the whole network.	The failure of single computer or cable doesn't bring the network down.
5.	No computer has a monopoly over the network.	Failure of the central hub causes the whole network failure.
6.	Adding and removing computers disrupts the network.	Adding and removing the computers is relatively easier.

1.4.9 Comparison of Bus and Star Topologies : MU : Dec. 15

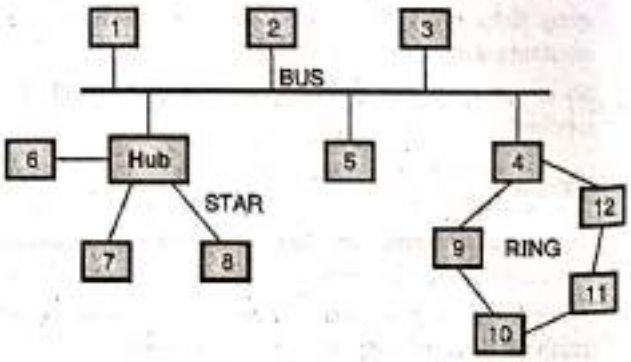
University Questions

Q. 1 Compare various types of network topologies. **(Dec. 15, 5 Marks)**

Sr. No.	Bus	Star
1.	Uses a cable as bus or backbone to connect all nodes.	Uses a central hub to connect the nodes to each other.
2.	Baseband or broadband coaxial cable is used.	Twisted pair, coaxial cables or optical fiber cables are used.
3.	If a part of bus fails, the whole network fails.	Failure of the central hub will make the entire network collapse.
4.	Adding an new node is difficult.	Adding and removing a node is relatively easy.
5.	Fault diagnosis is relatively difficult.	Fault diagnosis is easy.

1.4.10 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. 1.4.10 shows the hybrid topology in which bus, star and ring topologies are used simultaneously.
- In Fig. 1.4.10, 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.
- 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.

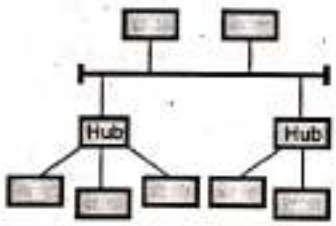


(G-23) **Fig. 1.4.10 : Hybrid topology**

Scanned by CamScanner

1.4.11 Comparison of Star Bus and Star Ring Topologies :

Sr. No.	Parameter	Star bus	Star ring
1.	Topology	Hybrid. It is a combination of star and bus topologies.	Hybrid. It is a combination of star and ring topologies.
2.	Configuration	Fig. A	Fig. B
3.	Peculiarity	Many stars are connected to a bus.	Many rings are connected in star.
4.	Applications	Suitable for large networks.	Suitable for interconnection of many small networks.



(G-24) Fig. A

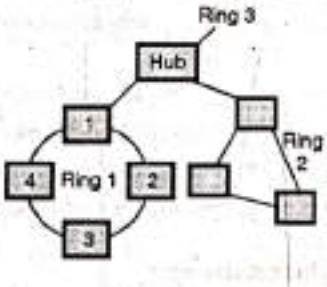


Fig. B

1.5 Line Configurations :

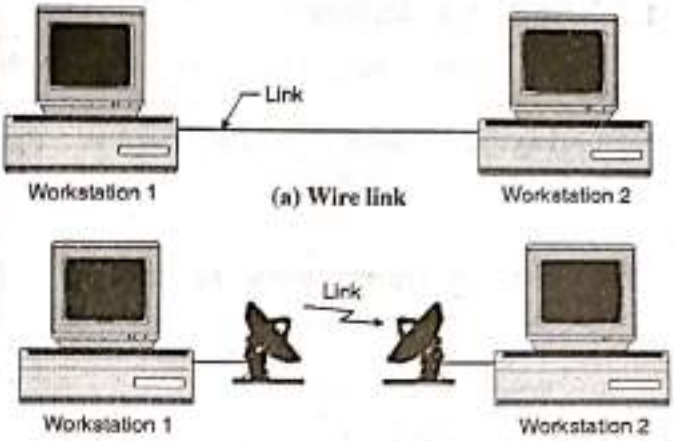
Two characteristics which can be used as the basis of distinguishing various data link configurations are topology and whether the link is half duplex or full duplex.

1.5.1 Type of Connections (Topology) :

- In a network two or more devices are connected to each other through connecting links.
- There are two possible ways to connect the devices. They are follows :
  1. Point to point connection
  2. Multipoint connection.

1.5.2 Point-to-Point Connection :

- A point to point connection provides a dedicated link between two devices as shown in Fig. 1.5.1. The meaning of the word dedicated is that the entire capacity of the link is reserved for transmission between these two devices only.
- It is possible to connect the two devices by means of a pair of wires (see Fig. 1.5.1(a)) or using a microwave or satellite link (wireless link) as shown in Fig. 1.5.1(b).

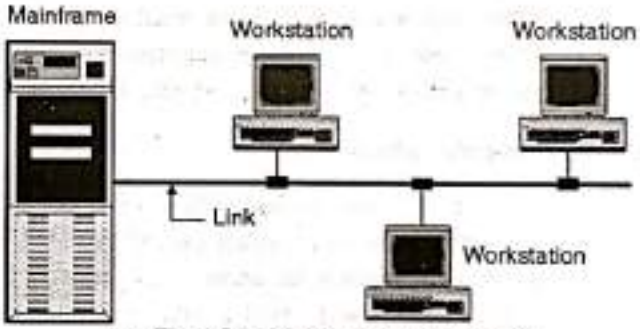


(b) Microwave link

(G-8) Fig. 1.5.1 : Point to point connection

1.5.3 Multipoint Connection :

- A multipoint connection is also called as a multidrop connection.
- In such a connection more than two devices are connected to and share a single link as shown in Fig. 1.5.2.
- In the multipoint connection the channel capacity is shared among multiple users. If many devices share the link simultaneously, it is called spatically shared connection.
- But if users share it turn by turn then it is time sharing connection.



(G-9) Fig. 1.5.2 : Multipoint configuration

1.6 Types of Communication : Simplex, Half Duplex, Duplex :

Based on whether the given communication system communicates only in one direction only or in both the directions, the communication systems are classified as :

- Simplex systems.
- Half duplex systems.
- Full duplex systems.
- We have discussed them in the section of design issues of the layers.

Scanned by CamScanner

1.7 Network Hardware :

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

1.7.1 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.

1.8 Network Scale :

- This is an alternative criterion for classification of networks.
- Fig. 1.8.1 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. 1.8.1 : 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.

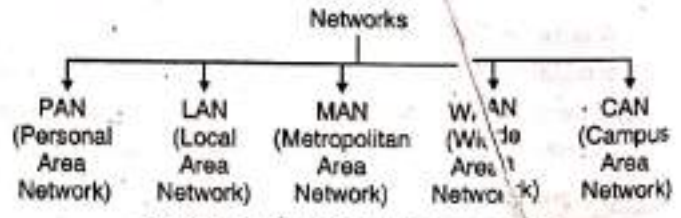
1.9 Network Classification by their Geography (Categories of Networks) :

MU : Dec. 13

University Questions

Q. 1 What are the different categories of the network classification ? **(Dec. 13, 5 Marks)**

- 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. 1.9.1.
- In this section, we will discuss the following categories of networks :



(G-1400)**Fig. 1.9.1 : Network categories**

Scanned by CamScanner

1.9.1 Local Area Networks (LAN) :

MU : May 05

University Questions

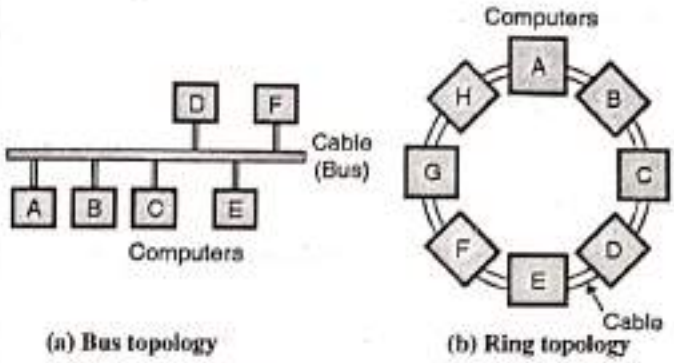
Q. 1 Design a LAN network for your institute.

(May 05, 6 Marks)

- 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. 1.9.1.
- 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.

LAN topologies :

Various topologies are possible for the broadcast LANs such as bus topology or ring topology as shown in Fig. 1.9.2.



(a) Bus topology (b) Ring topology

(G-32)Fig. 1.9.2 : 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.

Scanned by CamScanner

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 :

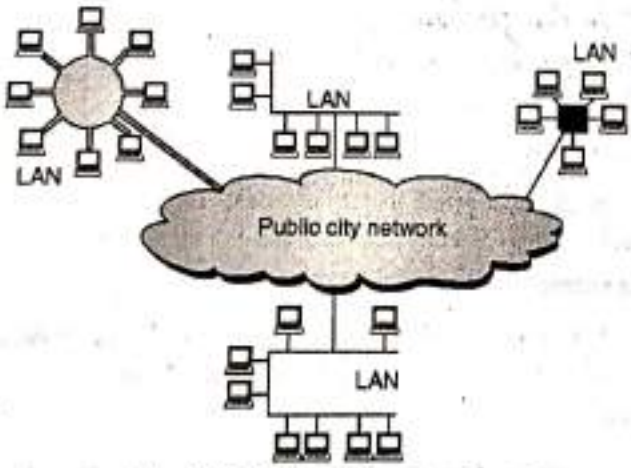
1. High reliability. Failure of individual computers does not affect the entire LAN.
2. It is possible to add a new computer easily.
3. The transmission of data is at a very high rate.
4. Sharing of peripheral devices such as printer is possible.

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.

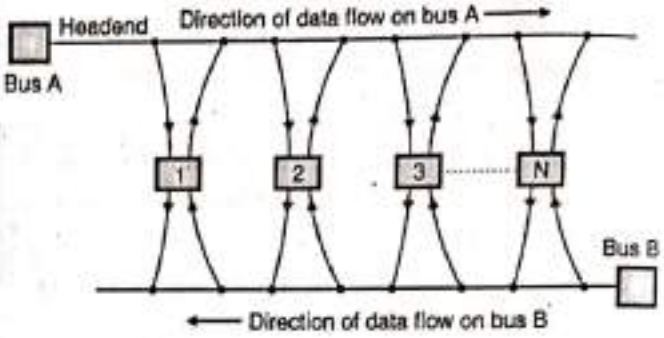
1.9.2 Metropolitan Area Network (MAN) :

- 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. 1.9.3.



(G-33)**Fig. 1.9.3 : Metropolitan area network**

- 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. 1.9.4.
- 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. 1.9.4.

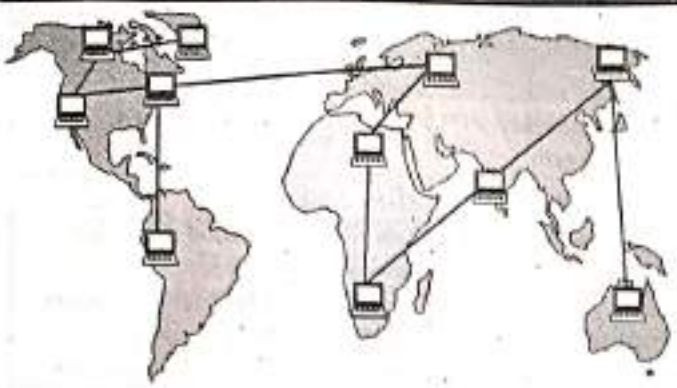


(G-34)**Fig. 1.9.4 : Distributed queue dual bus architecture (DQDB)**

1.9.3 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.

Scanned by CamScanner



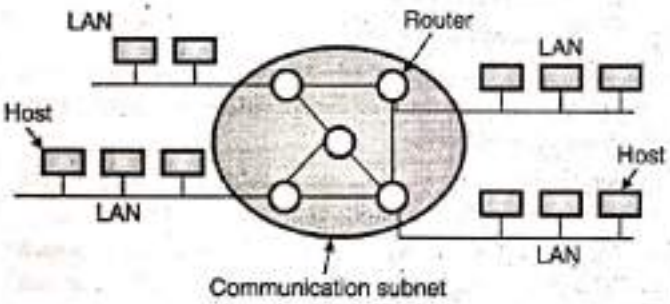
(G-35)Fig. 1.9.5 : Wide area network

- 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. 1.9.5.

Host : Host is a large computer. It can provide services to many computers. The services provided are :

1. Providing computing capabilities
2. Providing access to database.

- 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. 1.9.6.

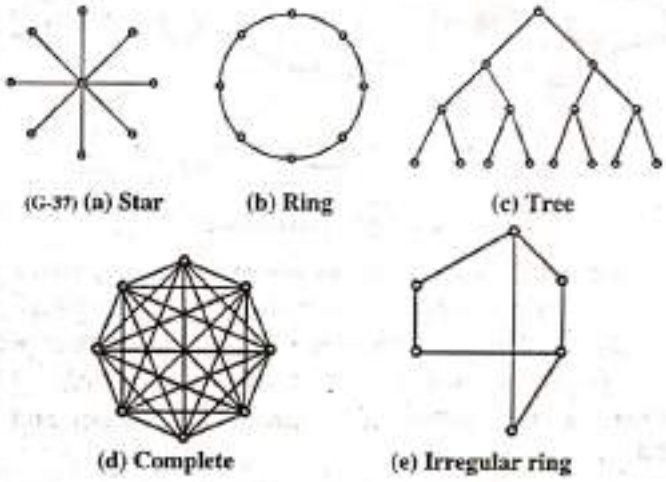


(G-36)Fig. 1.9.6 : Communication subnet and hosts

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



(G-38)Fig. 1.9.7 : Router interconnection topologies

1.9.4 Wireless Networks :

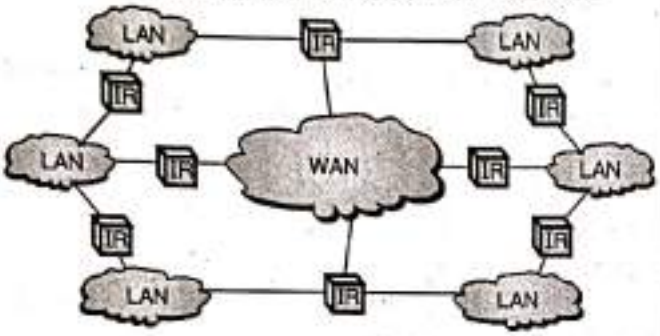
- The fastest growing segment of the computer industry is the mobile computers such as notebook computers and Personal Digital Assistant (PDAs).
- The wireless networks are becoming increasingly important because the wired connection is not possible in cars or aeroplanes.
- Wireless networks can have 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.

Scanned by CamScanner

- 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.

1.9.5 Internetworks :

- When two or more networks are connected together they are called as internetwork or internet as shown in Fig. 1.9.8.



(G-39)Fig. 1.9.8 : Internetwork

- Individual networks are joined into internetworks by the use of internetworking devices like bridges, routers and gateways.
- Fig. 1.9.8 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 peripheri contains only routers then it is called as a subnet. But if it contains routers as well as hosts then it is a WAN.

1.9.6 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

1.9.7 Network Classification by their Component Role :

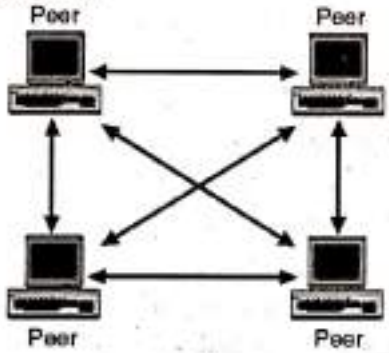
- The local area networks are classified into two types :
  1. Peer to peer networks.
  2. Client server networks.
- The relationship between each PC or device on the network with the others in terms of control will be dependent on the choice of network type.
- For these two types, the special software 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 analogus 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.

1.9.8 Peer-to-Peer Networks :

- Fig. 1.9.9 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.

Scanned by CamScanner

- 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. 1.9.9 : 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.

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.

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.

1. No extra investment in server hardware or software is required.
2. **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.
3. **Easy to administer :** In peer-to-peer network each machine performs its own administration.
4. **No NOS required :** Peer-to-peer network does not require a Network Operating System (NOS).
5. **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/achieve more redundancy because of smaller possibility of single point of failure.
6. Easy setup and lower cost for small networks.
7. Users can control resource sharing.
8. A user is not dependent on other computers for its operation.

Disadvantages of Peer to Peer Networks :

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

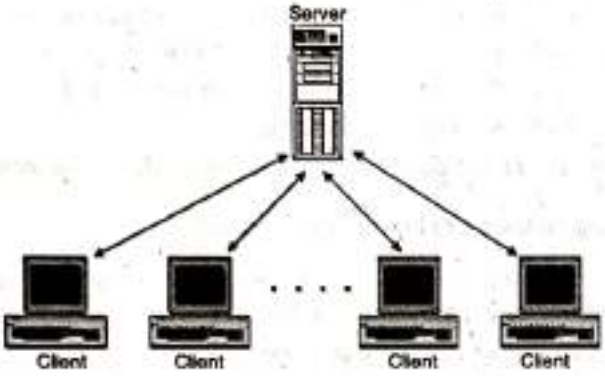
1. **Individual performance is affected :** If some workstations have frequently used resources on them, then the use of these resources by other computer might adversely affects the person using this particular workstation.
2. **Less security :** A peer-to-peer network operates on the most common desktop 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 final 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.

1.9.9 Client / Server Network (Server Based Network) :

- In client-server network relationships, certain computers act as server and other 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.

Scanned by CamScanner

- 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 a 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 are accessed by client.
- Fig. 1.9.10 shows client-server network relationship.



(G-41)**Fig. 1.9.10 : 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 :

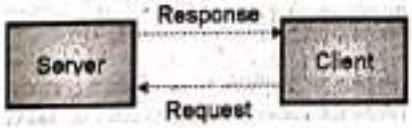
The individual workstations in the network are called as the clients.

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.

Communication in Client-Server Configuration :

- Fig. 1.9.11 explains the principle of communication in the client server configuration.



(G-42)**Fig. 1.9.11 : Client/server communication**

- The client places a request on the server machine when he wants an access to the centralised resources.
- The server responds to this request and sends the signal accordingly to the client as shown in Fig. 1.9.11.
- 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 :

(a) Shared resources are located in a centralized area and they are administered centrally.

(b) The servers are physically placed in secure location such as lockable separate server room.

(c) The operating system runs on client-server are designed to provide better security to network.

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

Scanned by CamScanner

Disadvantages of client-server networks :

1. **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.
2. We have to use a high speed server computer with lots of memory and disk space.
3. It requires a special network operating system and a number of client licenses.
4. 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.

1.9.10 Factors Influencing the Choice of Network :

- The factors which influence the choice between the peer to peer or client server networks are as follows :
  1. Need of network security.
  2. Is the network administration needed ?
  3. Is the central storage of files essential ?
  4. How much important is cost effectiveness ?
  5. Is resource sharing necessary ?
  6. Will there be any future expansions of the network ?

1.9.11 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.

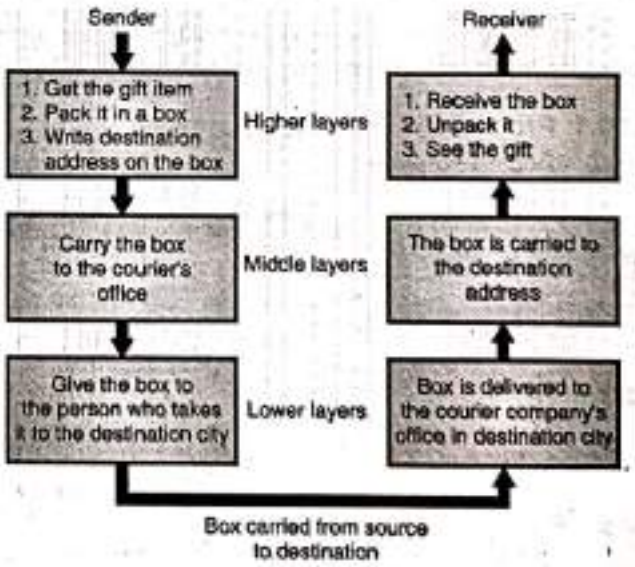
1.9.12 Network Features :

Now you can understand the types of things you can do with a network. The following are the features of network :

1. File sharing.
2. Printer sharing.
3. Application services.
4. E-mail.
5. Remote access.
6. Internet and intranet.
7. Network security : Internal and external.

1.9.13 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. 1.9.12 shows the steps involved in this process.
- In Fig. 1.9.12, 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.



(G-1546) **Fig. 1.9.12 : Layered tasks**

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.

Scanned by CamScanner

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.

1.10 Network Software :

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

1.10.1 Protocol Hierarchies (Layered Architecture) :

MU : May 12, Dec. 14, Dec. 17

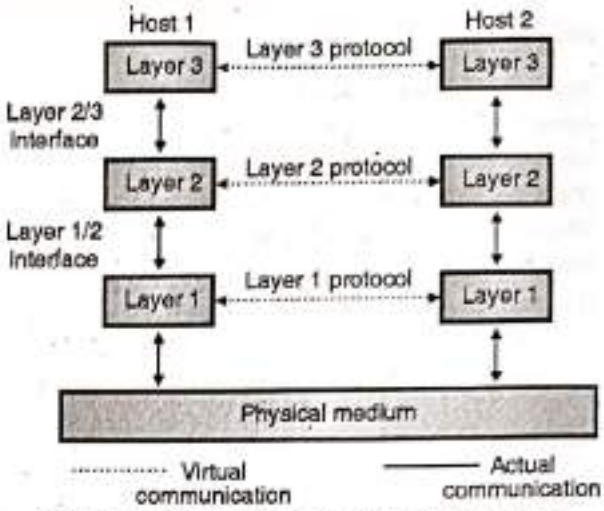
University Questions

Q. 1 Draw the layered structures and compare the two network reference models – OSI and TCP/IP. **(May 12, 10 Marks)**

Q. 2 Why there is a need for layered designing for networking and communication ? Compare the TCP/IP and OSI reference models. **(Dec. 14, 10 Marks)**

Q. 3 Explain the need of layered design for communication and networking. Compare the OSI reference model & TCP/IP. **(Dec. 17, 10 Marks)**

- Most networks are organized in the form of a series of layers or levels as shown in Fig. 1.10.1.
- To reduces the design complexity.



(G-49) **Fig. 1.10.1 : Layers, protocols and interfaces**

- 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. 1.10.1. 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. 1.10.1 shows the virtual communication and physical communication is shown by solid lines.

1.10.2 Reasons for having Layered Protocols and its Benefits :

MU : May 05, Dec. 05, May 07, Dec. 09, May 13

University Questions

Q. 1 Explain the need for the layered architecture of computer network. Also explain data transmission and protocols in layered architectures. **(May 05, Dec. 05, May 07, 10 Marks)**

Q. 2 Explain the need for the layered architecture in computer network. Explain how information is exchanged between two nodes using OSI model. **(Dec. 09, 10 Marks)**

Scanned by CamScanner

Q. 3 What is the need for layering ? Discuss the design issues for layers. **(May 13, 10 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 :

1. It simplifies the design process as the functions of each layers and their interactions are well defined.
2. The layered architecture provides flexibility to modify and develop network services.
3. The number of layers, names of the layers, and the tasks assigned to them may change from network to network. But for all the networks, always the lower layer offers some services to its upper layer.
4. The concept of layered architecture is a new way of looking at the networks.
5. Addition of new services and management of network infrastructure becomes easy.
6. Due to segmentation (layered structure), it is possible to break difficult problems into smaller and more manageable tasks.
7. Logical segmentation allows parallel working by different teams on different tasks simultaneously.

1.10.3 Disadvantages of Layered Architecture :

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

1.10.4 How does Data Transfer take Place ?

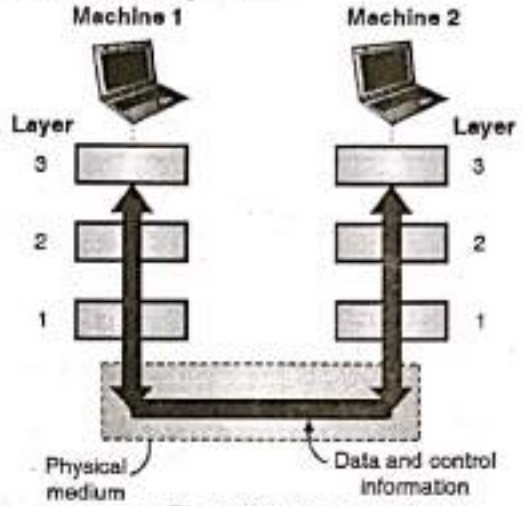
MU : May 10, Dec. 12, May 13

University Questions

Q. 1 What is the difference between protocol and service interface ? Explain your answer in terms of the OSI seven layer model. **(May 10, 10 Marks)**

Q. 2 Differentiate between protocol and interface ? **(Dec. 12, May 13, 10 Marks)**

- Data does not get transferred directly from layer n of one machine to layer n of the other machine. Instead the data transfer takes place as explained below.
- The data and control information is passed on to the lower layers until the lowest layer (layer 1) is reached. Below layer 1 lies the physical medium such as coaxial cable, through which the actual transfer of data and control information takes place.
- This is shown in Fig. 1.10.2.



(G-50) **Fig. 1.10.2 : Data transfer**

Interface :

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

1.11 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.

1.11.1 Virtual Communication between Layers :

MU : May 05, Dec. 05, May 07

University Questions

Q. 1 Explain the need for the layered architecture of computer network. Also explain data transmission and protocols in layered architectures. **(May 05, Dec. 05, May 07, 10 Marks)**

- Let us now go into technical details of the communication between say layer 5 of two machines.
- Refer Fig. 1.11.1 and go through the steps given below to understand the communication.

Step 1 : A messages 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.

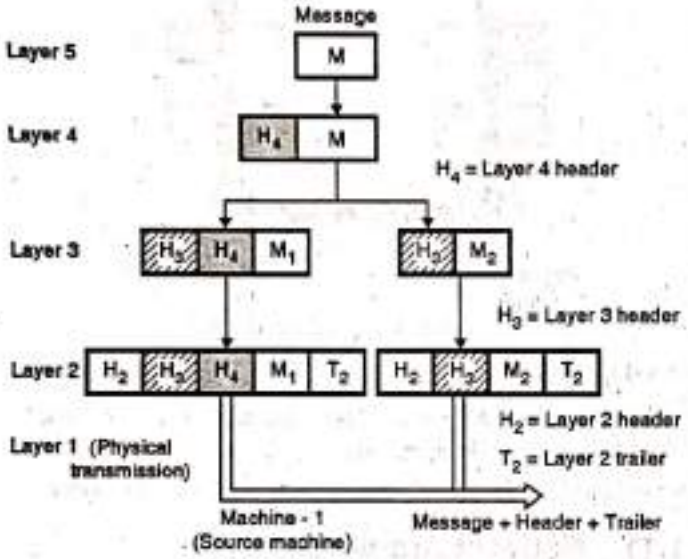
Scanned by CamScanner

A header includes the control information and it allow 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 adder to each packet M_1 and M_2 as shown in Fig. 1.11.1 and passes these packets to layer 2.

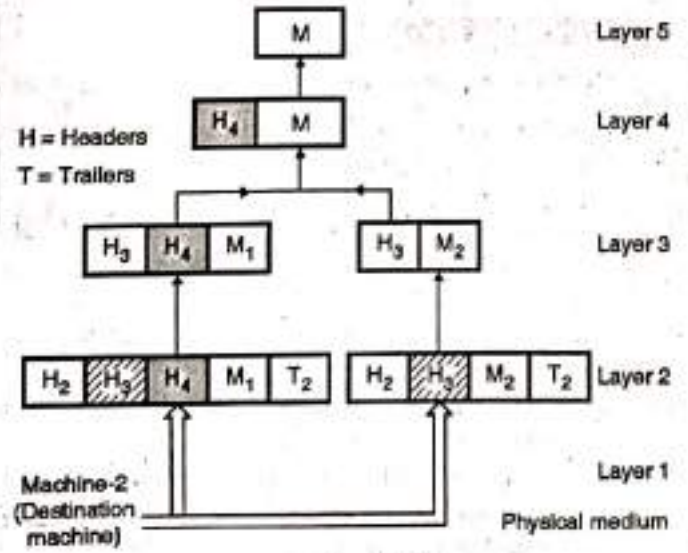
Step 4 : Layer 2 adds header as well as trailer to each packet obtained from layer 3 and hands over the resultant unit to layer 1 for physical transmission.

- This sequence of operation taking place at machine 1 is shown in Fig. 1.11.1.



(G-51) **Fig. 1.11.1 : Information flow for virtual communication between layers 5**

- 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. 1.11.2.



(G-52) **Fig. 1.11.2**

1.12 Design Issues for the Layers :

MU : Dec. 10, May 13, May 15, Dec. 15, Dec. 16, New Syll. : Dec. 18

University Questions

Q. 1 Describe any five design issues for the layers. **(Dec. 10, 5 Marks)**

Q. 2 What is the need for layering ? Discuss the design issues for layers. **(May 13, 10 Marks)**

Q. 3 What are the design issues for the layers ? **(May 15, 4 Marks)**

Q. 4 Discuss the design issues for various layers. **(Dec. 15, 5 Marks)**

Q. 5 List design issues in OSI layers. **(Dec. 16, 5 Marks)**

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

1.12.1 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.

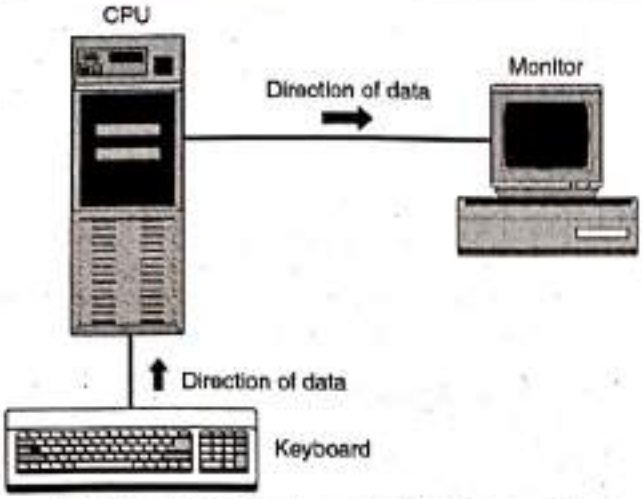
1.12.2 Direction of Transmission :

- Another important design issues 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 :
  1. Simplex systems.
  2. Half duplex systems.
  3. 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. 1.12.1.
- The communication from CPU to monitor or keyboard to CPU is unidirectional.
- Keyboard and traditional monitors are examples of simplex devices.

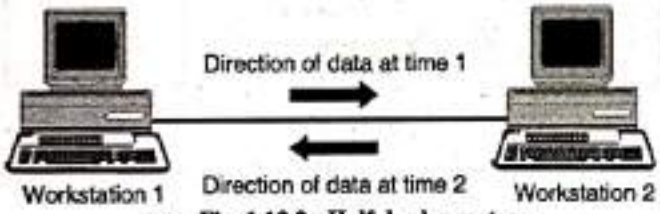
Scanned by CamScanner



(G-53) **Fig. 1.12.1 : Simplex mode of data transmission**

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 transreceiver 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. 1.12.2.
- Each station can transmit and receive, but not at the same time. When one device is ending the other one is receiving and vice versa.

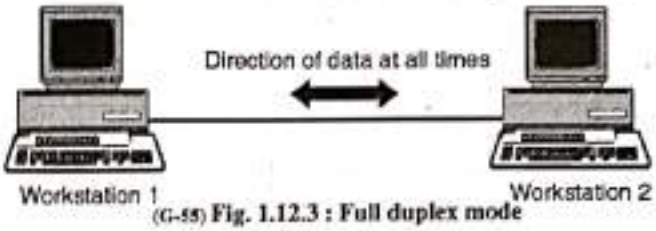


(G-54) **Fig. 1.12.2 : Half duplex system**

- In half duplex transmission, the entire capacity of the channel is utilized by the transmitting (sending) systems.

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. 1.12.3. 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.



(G-55) **Fig. 1.12.3 : Full duplex mode**

1.12.3 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.

1.12.4 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.

1.12.5 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.

1.12.6 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.

1.13 Interfaces and Services :

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

Scanned by CamScanner

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

1.13.1 Entities and Peer Entities :

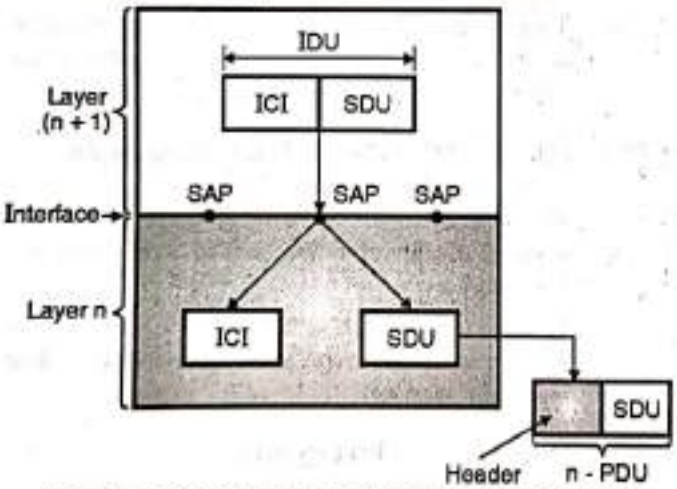
- An entity is defined as the active element in each layer. An entity can be either a software entity or a hardware entity.
- The example of software entity is a process and that of a hardware entity is an intelligent I/O chip.
- Entities in the same layer but on different machines are called as **peer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

1.13.2 Service Provider and Service User :

- The entities at layer n implement services for the layer (n + 1) which is above the nth 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.

1.13.3 Service Access Points (SAPs) :

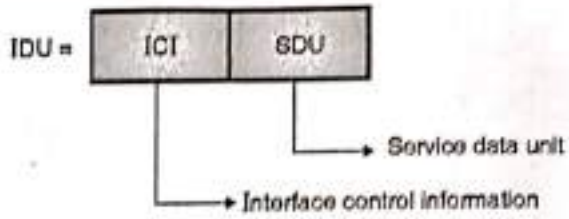
- Refer Fig. 1.13.1 to understand the definition of SAPs.
- The long form of SAP is service access point. They are available at the interface of n and n + 1 layer as shown in Fig. 1.13.1.
- Services are available at SAPs. That means the layer n SAPs are those places at the interface where layer (n + 1) can access the services being offered.
- Each SAP has a unique address for its identification.



(G-56) **Fig. 1.13.1 : Relation between layers at an Interface**

1.13.4 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. 1.13.2, the layer (n + 1) entity passes an IDU (interface data unit) to the layer n entity through the SAP.



(G-57) **Fig. 1.13.2 : IDU**

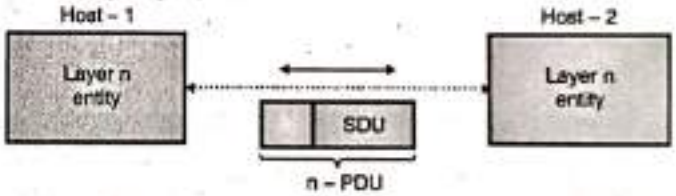
- An IDU consists of two parts namely SDU (service data unit) and ICI (interface control information).

1.13.5 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.

1.13.6 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.
- The PDU headers are used by the peer entities to carry out their peer protocol.



(G-58) **Fig. 1.13.3 : Layer n entities exchange n-PDUs in their layer n 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.

1.14 Connection Oriented and Connectionless Services :

MU : Dec. 03, May 04, Dec. 11

University Questions

Q. 1 Write advantages and disadvantages of connection oriented service with connection less service and write example application. **(Dec. 03, 10 Marks)**

Q. 2 What are the principle differences between connectionless and connection oriented communication ? Characterize all the aspects in terms of quality and service. **(May 04, 10 Marks)**

Scanned by CamScanner

Q. 3 What is the principle difference between connectionless communication and connection oriented communication ? **(Dec. 11, 5 Marks)**

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

1.14.1 Connection Oriented Service :

MU : May 04

University Questions

Q. 1 What are the principle differences between connectionless and connection oriented communication ? Characterize all the aspects in terms of quality and service. **(May 04, 10 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 :
  1. Establish a connection.
  2. Use the connection.
  3. 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.

1.14.2 Connectionless Service :

- The connectionless service is similar to the postal service.
- Each message (analogus 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.

1.14.3 Comparison of Connection Oriented and Connectionless Services :

MU : Dec. 12, May 13, May 16, New Syll. : Dec. 18

University Questions

Q. 1 Differentiate between the connectionless and connection oriented service. **(Dec. 12, May 13, 10 Marks)**

Q. 2 Compare connection oriented and connectionless services. **(May 16, 4 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

1.14.4 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.
- 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 1.14.1 lists various types of services and their examples.

Scanned by CamScanner

Table 1.14.1 : 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.

1.14.5 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 1.14.2.

Table 1.14.2 : 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.	DISCONNET	Terminate the connection

1.15 Relationship of Services to Protocols :

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

1.15.1 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.

1.15.2 Protocol : MU : May 10, Dec. 12, May 13

University Questions

Q. 1 What is the difference between protocol and service interface ? Explain your answer in terms of the OSI 7 layer model. **(May 10, 10 Marks)**

Q. 2 Differentiate between protocol and interface ? **(Dec. 12, May 13, 10 Marks)**

- 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 service. Once their predecided services are ensured, they are free to change the protocol.

1.16 Reference Models : MU : May 17

University Questions

Q. 1 What is ISO-OSI reference model ? Compare it with TCP/IP reference model. Which layer is used for the following :

1. To route packets
2. To convert packets to frame
3. To detect and correct errors.
4. To run services like FTP, telnet etc.

(May 17, 10 Marks)

- 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).

Scanned by CamScanner

- 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.

1.17 OSI Model

MU : Dec. 03, Dec. 07, May 10, May 11, Dec. 12, May 15

University Questions

Q. 1 What is the difference between protocol and service interface ? Explain your answer in terms of the OSI 7 layer model. **(Dec. 03, May 10, 10 Marks)**

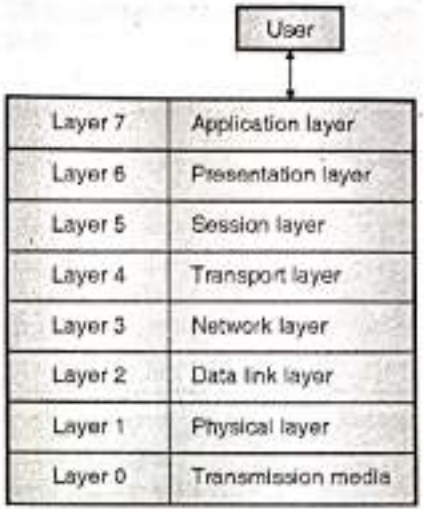
Q. 2 Explain why the ISO-OSI model of computer network is layered ? How it is different from TCP/IP Model ? **(Dec. 07, 10 Marks)**

Q. 3 Describe OSI reference model with a neat diagram. **(May 11, 10 Marks)**

Q. 4 Explain the layer details of OSI and TCP/IP models. **(Dec. 12, 10 Marks)**

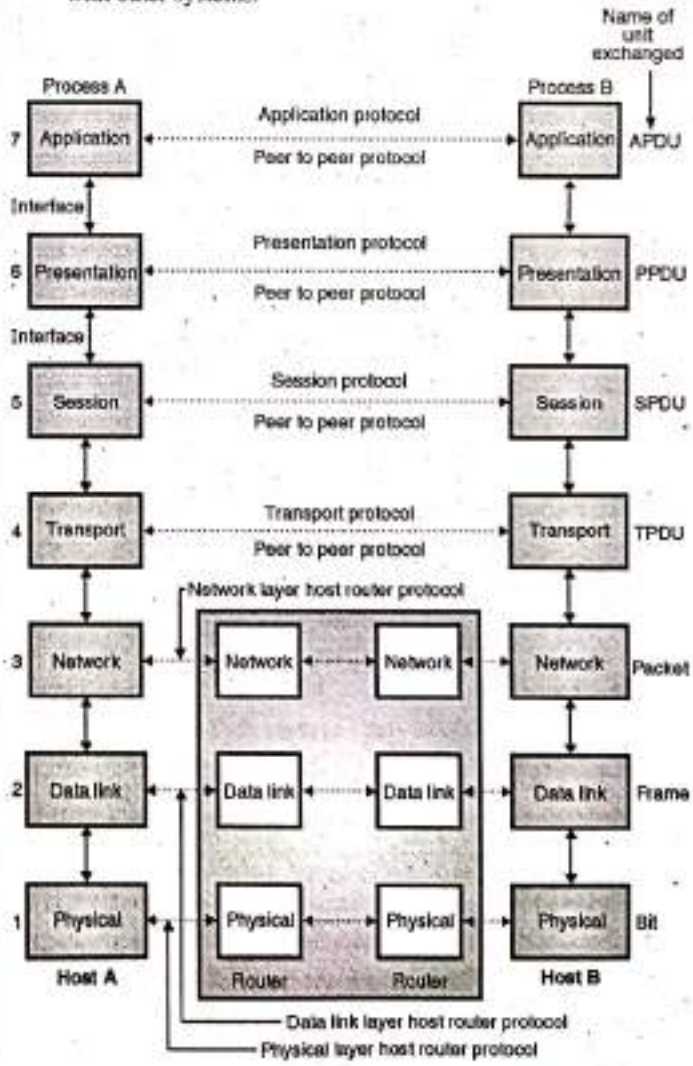
Q. 5 Describe the OSI Reference Model with a neat diagram. **(May 15, 10 Marks)**

- 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".
- Fig. 1.17.1 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. 1.17.2.
- The OSI model shown in Fig. 1.17.2 does not contain the physical medium.



(G-59) **Fig. 1.17.1 : A seven layer ISO-OSI reference model**

- 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.



(G-60) **Fig. 1.17.2 : The OSI reference model**

Scanned by CamScanner

- Table 1.17.1 shows various layers and its functions.

Table 1.17.1 : Functions of the layers of ISO-OSI model

Level	Name of the layer	Functions
1.	Physical layer	Make and break connections, define voltages and data rates, convert data bits into electrical signal. Decide whether transmission is simplex, half duplex or full duplex.
2.	Data link layer	Synchronization, error detection and correction. To assemble outgoing messages into frames.
3.	Network layer	Routing of the signals, divide the outgoing message into packets, to act as network controller for routing data.
4.	Transport layer	Decides whether transmission should be parallel or single path, multiplexing, splitting or segmenting the data, to break data into smaller units for efficient handling.
5.	Session layer	To manage and synchronize conversation between two systems. It controls logging on and off, user identification, billing and session management.
6.	Presentation layer	It works as a translating layer.
7.	Application layer	Retransferring files of information, LOGIN, password checking etc.

- All the applications need not use all the seven layers shown in Fig. 1.17.2.
- 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.

1.17.1 Functions of Different Layers :

MU : May 17

University Questions

Q.1 What is ISO-OSI reference model ? Compare it with TCP/IP reference model. Which layer is used for the following :

1. To route packets
2. To convert packets to frame
3. To detect and correct errors.
4. To run services like FTP, telnet etc.

(May 17, 10 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.

Scanned by CamScanner

- 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 :

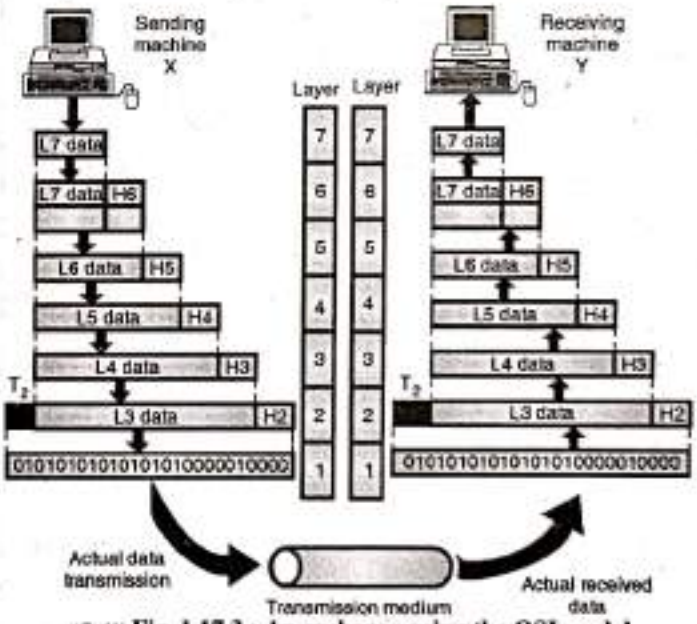
- Application layer is at the top of all as shown in Fig. 1.17.2. It provides different services such as manipulation of information in various ways, retransferring the files of information, distributing the results etc. to the user who is sitting above this layer.
- The functions such as LOGIN, or password checking are also performed by the application layer.
- Let us now go into the details of each and every layer.

1.17.2 Exchange of Information using the OSI Model : MU : Dec. 09

University Questions

Q. 1 Explain the need for the layered architecture in computer network. Explain how information is exchanged between two nodes using OSI model. **(Dec. 09, 10 Marks)**

- 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. 1.17.3.
- 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.



(G-61) **Fig. 1.17.3 : An exchange using the OSI model**

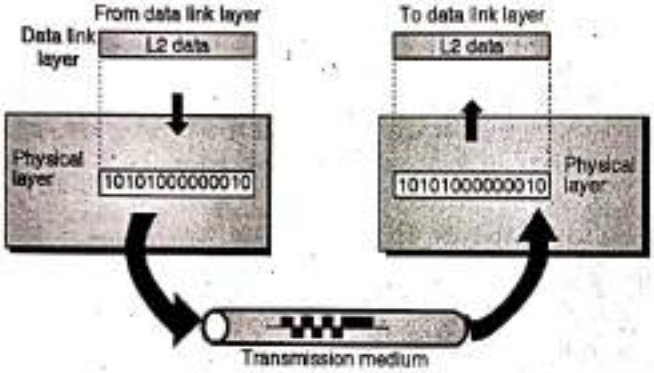
- The upper OSI layers are always implemented in software (4, 5, 6 and 7) and lower layers are a combination of hardware and software (2, 3) except for the physical layer which is mostly hardware.
- Layers 1, 2 and 3 (i.e. physical , data link and network) are the network support layers. They deal with 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.

Scanned by CamScanner

- Layers 5, 6 and 7 (i.e. session, presentation and application) they allow interoperability among unrelated software systems.

1.17.3 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. 1.17.4.



(G-62) **Fig. 1.17.4 : Physical layer**

Functions of the physical layer :

1. To define the type of encoding i.e. how 0's and 1's are changed to signals.
2. To define the transmission rate i.e. the number of bits transmitted per second.
3. To deal with the synchronization of the transmitter and receiver.
4. To deal with network connection types, including multipoint and point to point connections.
5. To deal with physical topologies i.e. bus, star, ring, or mesh.
6. To deal with the media bandwidth i.e. baseband and broadband transmission.
7. Multiplexing which deals with combining several data channels into one.
8. To define the characteristics between the device and the transmission medium.
9. To define the transmission mode between two devices i.e. whether it should be simplex, half duplex or full duplex.

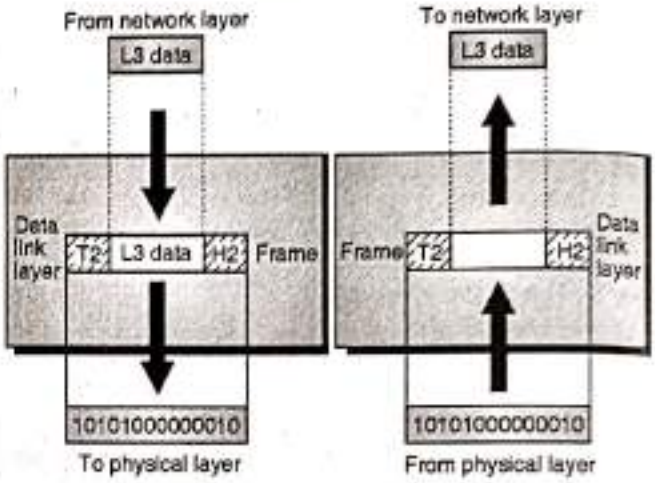
Note : Passive hubs, simple active hubs, terminators, couplers, cable and cabling, connectors, repeaters, multiplexers, transmitters, receivers, transceivers are associated with the physical layer.

1.17.4 Data Link Layer : MU : May 10

University Questions

Q. 1 Write short notes on : Differentiate Data Link Layer and Transport Layer. **(May 10, 5 Marks)**

- 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. 1.17.5.



(G-63) **Fig. 1.17.5 : Data link layer**

Functions of DLL :

Following are the functions of data link layer :

1. **Framing :**

The bits received from the network layer are divided into another type of data units called frames at the data link layer.

2. **Flow control :**

It provides a flow control mechanism to avoid a fast transmitter from over-running a slow receiver by buffering the extra bits.

3. **Physical addressing :**

It adds a header to the frame which consists of the physical address of the sender and / or receiver of that frame.

4. **Error control :**

A trailer is added at the end of the frame in order to achieve error control. It also uses a mechanism to prevent duplication of frames.

5. **Access control :**

- The data link layer protocol perform an important function of determining which device has control over the link at any given time, when two or more devices are connected to the same link.
- The Institution of Electrical and Electronics Engineers (IEEE) felt the need to define the data link layer in more details, so they split it into two sub-layers :

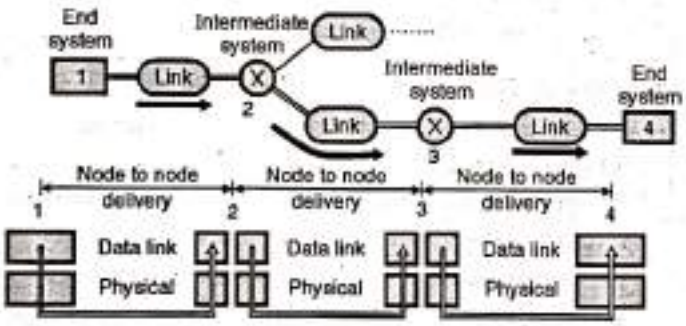
Scanned by CamScanner

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. 1.17.6 shows the node delivery by the data link layer.

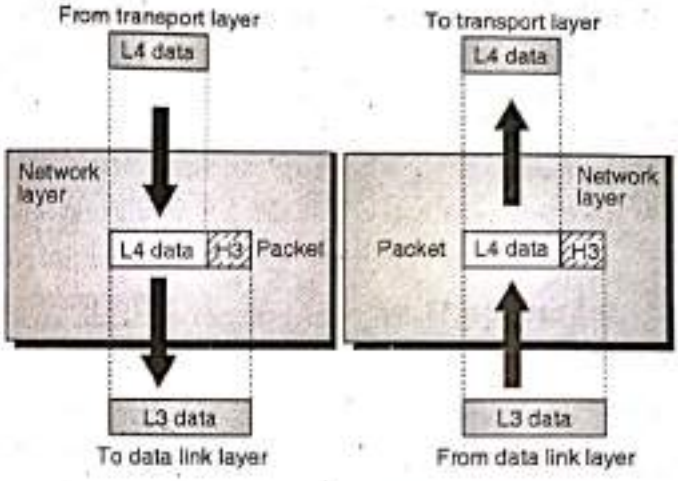


(G-64) **Fig. 1.17.6 : Node to node delivery**

- Fig. 1.17.6 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.

1.17.5 Network Layer :

- The main function of this layer is to delivery 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. 1.17.7.

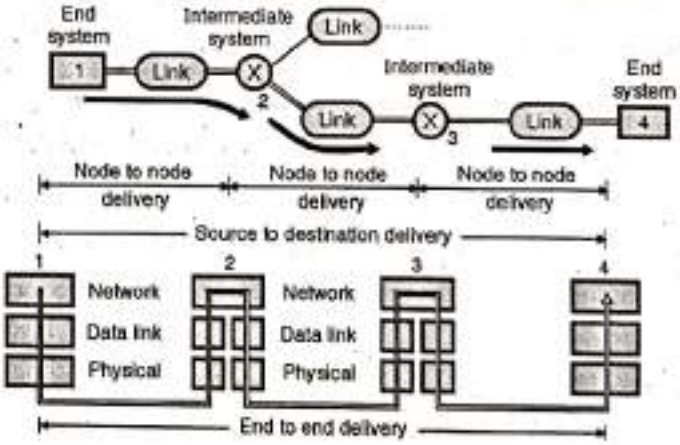


(G-65) **Fig. 1.17.7 : Network layer**

Functions of the network layer :

1. It translates logical network address into physical machine addresses i.e. the numbers used as destination IDs in the physical network cards.
2. It determines the quality of service by deciding the priority of message and the route a message will take if there are several ways a message can get to its destination.
3. It breaks the larger packets into smaller packets if the packet is larger than the largest data frame the data link will accept.
4. It is concerned with the circuit, message or packet switching.
5. It provides connection oriented services, including network layer flow control, network layer error control and packet sequence control.
6. Routers and gateways operate in the network layer.

The network layer carries out the end to end (source to destination) delivery and routing. This is illustrated in Fig. 1.17.8.



(G-66) **Fig. 1.17.8**

- 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.

Scanned by CamScanner

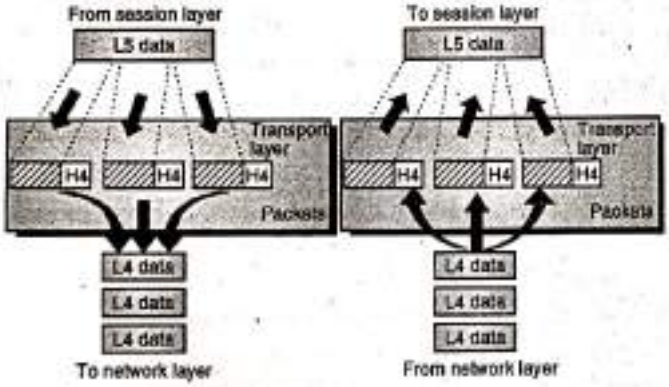
2. The router (2) decides the next node to which this packet should be sent on the basis of the final destination. The next hop is the router (3). The network layer of 2 forward the packet to the network layer of router 3.
3. The network layer of 3 (which is again a router) will direct the packet to the network layer of end system-4.

1.17.6 Transport Layer : MU : May 10

University Questions

Q. 1 Differentiate Data Link Layer and Transport Layer. **(May 10, 5 Marks)**

- 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. 1.17.9 shows the relationship of the transport layer to the network layer and session layer.



(G-67) **Fig. 1.17.9 : Transport layer**

Functions of transport layer :

The transport layer performs the following functions :

1. It divides each message into packets at the source and re-assembles then 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.

1.17.7 The Session Layer :

MU : May 04, May 15, Dec. 16

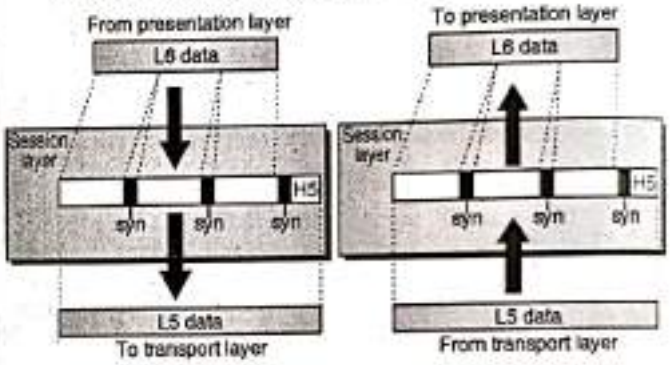
University Questions

Q. 1 Explain how a session layer establishes, maintains and synchronises the interaction between two communicating hosts. **(May 04, 10 Marks)**

Q. 2 Write short note on functions of Session layer. **(May 15, 5 Marks)**

Q. 3 Explain any four functions of session layer with example. **(Dec. 16, 10 Marks)**

- The main function of this layer is to establishe, maintain and synchronise the communication between interested systems.
- Fig. 1.17.10 shows the relationship of the session layer to the transport layer and the presentation layer.



(G-68) **Fig. 1.17.10 : 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.

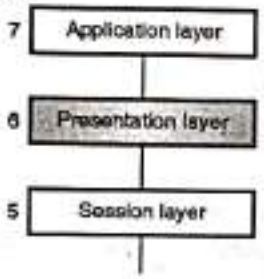
Scanned by CamScanner

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.

1.17.8 Presentation Layer :

- The presentation layer is the 6th layer the OSI model as shown in Fig. 1.17.11.
- Above it there is the application layer and below it there is the sessions layer.



(G-707) **Fig. 1.17.11 : 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 :

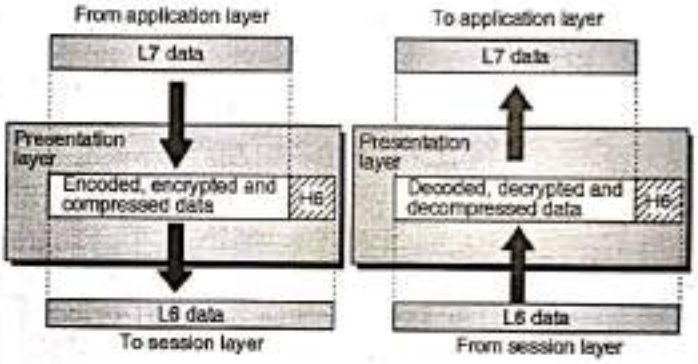
- For ensuring the security and privacy of the information that is being communicated, a process called data encryption is essential.
- Encryption is carried out at the sending end. In the encryption process, the sender transforms the original information to another form, and sends the transformed information.
- 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 relation of presentation layer with the application layer and session layer is illustrated in Fig. 1.17.12.



(G-69) **Fig. 1.17.12 : Relation of presentation layer with the application layer and session layer**

- The data from the application layer (L7 data) is encrypted, encoded and compressed at the presentation layer. A presentation layer header H-6 is also added as shown in Fig. 1.17.12.
- This is then sent to the session layer as L-6 data. These processes take place at the sending end of the system.
- While receiving the data from session layer, the operations carried out by the presentation layer are exactly opposite to those carried out while transmitting.
- The received data from the session layer undergoes decryption, decompression and decoding at the presentation layer.
- The header H-6 is detached from the data and then the L-7 data is sent to the application layer.

Functions of presentation layer :

The presentation layer performs the following function :

1. It translates data between the formats the network requires and the format the computer expects (e.g. ASCII or EBCDIC).
2. It does the protocol conversion.

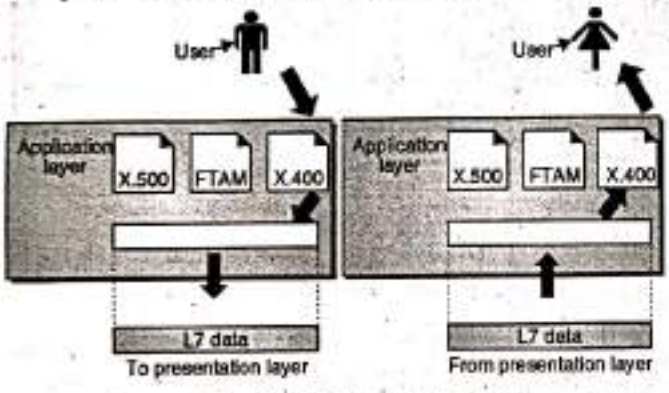
Scanned by CamScanner

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).

1.17.9 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. 1.17.13.



(G-70) **Fig. 1.17.13 : Application layer**

The application layer performs the following functions :

1. The application layer allows the creation of a virtual terminal which is the software version of a physical terminal. The user can log on to the remote host due to this arrangement.
2. The application layer provides File Transfer Access and Management (FTAM) which allows a user to access, retrieve, manage or control files in a remote computer.
3. It creates a basis for forwarding and storage of e-mails.

1.17.10 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.

1.17.11 Demerits of OSI Model :

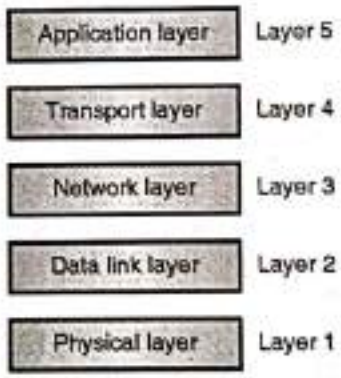
1. Sessions and presentation layers are not of much use.
2. This model was devised before the protocols were invented. So in real life there is a problem of fitting protocol into a model.

1.18 TCP/IP Protocol Suite : MU : May 16

University Questions

Q. 1 Explain in short TCP/IP model. **(May 16, 4 Marks)**

- After discussing about the concept of protocol layering and about the logical communication taking place between layers, now it is time to introduce the **TCP/IP protocol suite.**
- TCP/IP is the short form of two important protocols namely Transmission Control Protocol/Internet Protocol.
- **A protocol suite** is defined as the set of protocols organized in different layers. The TCP/IP protocol suite is used in Internet today.
- TCP/IP is a hierarchical protocol suite means that each upper layer protocol receives support and services from either one or more lower level protocols.
- In the original TCP/IP protocol suite, there were four software layers built upon the hardware. But today's TCP/IP protocol suite uses a five layer model as shown in Fig. 1.18.1.



(G-2065) **Fig. 1.18.1 : Layers in TCP/IP protocol suite**

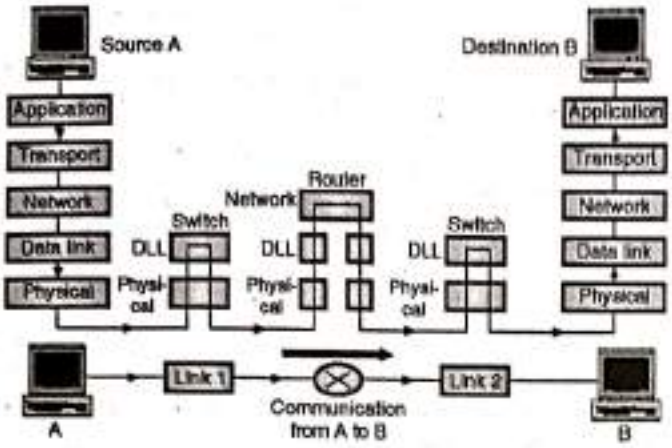
1.18.1 Layered Architecture : MU : May 16

University Questions

Q. 1 Explain in short TCP/IP model. **(May 16, 4 Marks)**

- In order to understand how the communication takes place between various layers of TCP/IP protocol suite, we have considered a small internetwork consisting of three LANs (links) with all LANs connected to each other via a router as shown in Fig. 1.18.2.

Scanned by CamScanner



(G-2176) **Fig. 1.18.2 : Communication through an Internet**

- In Fig. 1.18.2, there are two computers A and B communicating with each other and three more devices namely : the link layer switch in link-1, the router and the link layer switch in link-2.
- Computer A is called as the **source host** and computer B is called as the **destination host.**
- Each device in the Internet has a specific role to play, depending on which each device uses a set of layers as shown in Fig. 1.18.2.
- All the five layers are involved in communication for the source and destination hosts A and B respectively.
- At the source host, a message is created at the application layer and then it is sent in down the layers in order to physically send it to the destination host.
- At the destination host this message is received at the physical layer and then it is delivered to the application layer via the other layers between the physical and application layers.
- At the router, as shown in Fig. 1.18.2 only three layers of TCP/IP protocol suite are needed to be involved. Thus a router does not need the transport or application layers when it is being used only for routing.
- The router is connected to multiple links. At each link we use a switch which involves only two layers of the TCP/IP protocol suite as shown in Fig. 1.18.2.
- However note that the link layer and physical layer protocols used by each link can be completely different.
- Thus the router may have to receive a packet from link-1 based on one pair of protocol and may have to deliver a packet to link-2 based on a totally different pair of protocols.
- Now consider a switch in Fig. 1.18.2 which shows that it has two different connections. But both of them belong to the same link. Therefore two different protocol pairs will not be involved. A switch has to deal with only one pair of DLL and physical layer protocols.

1.18.2 Layers in the TCP/IP Protocol Suite :

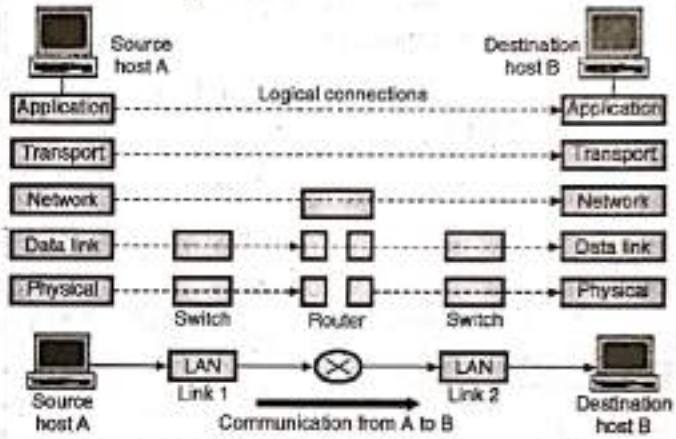
MU : Dec. 12, May 16

University Questions

Q. 1 Explain the layer details of OSI and TCP/IP models. **(Dec. 12, 10 Marks)**

Q. 2 Explain in short TCP/IP model. **(May 16, 4 Marks)**

- Now we are going to discuss the functions and duties of various layers in the TCP/IP protocol suite.
- In this section, we will think about the logical connections between various layers, so as to clearly understand the duties of each layer.
- The logical connections in a simple internetwork have been shown in Fig. 1.18.3.



(G-2177) **Fig. 1.18.3 : Logical connections between the layers of TCP/IP suite**

- Each layer has some specific duties and we can use the logical connections to think about them easily.
- From Fig. 1.18.3 it is clear that the network, transport and application layers have an **end-to-end** duty. But the data link and physical layers have the **hop to hop** duty. (Hop is a host or router).
- In this way the upper three layers have a **domain of duty** of the entire Internet while the lower two have a domain of duty of only link.

Data unit created by every layer :

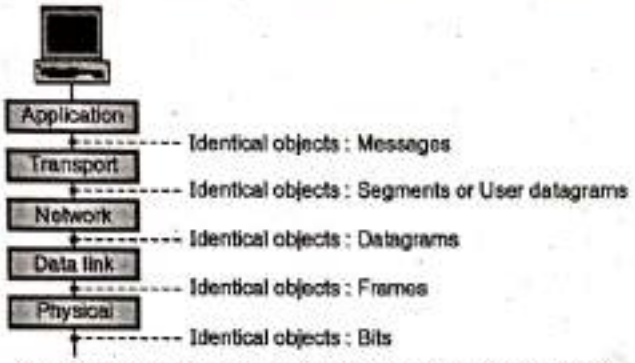
- We can think about the logical connections in a different way i.e. in terms of the **data unit** created by each layer.
- The names of data units (packets) created by different layers are as follows :

Layer	Data unit	Layer	Data unit
Application	Message	Datalink	Frame
Transport	Segment	Physical	Bits
Network	Datagram		

- The data unit (packet) created by the top three layers, should not be changed by a router or a link layer switch.

Scanned by CamScanner

- However the data unit created at the lower two levels can be changed only by the router. The link layer switches cannot modify it.
- The second principle that we discussed for the protocol layering has been shown in Fig. 1.18.4. Note that the objects shown below each layer related to each device are identical.



(G-2178) **Fig. 1.18.4 : Identical objects in the TCP/IP suite**

1.19 Detailed Description of Each Layer in TCP/IP :

In this section we are going to discuss the duties of various layers in TCP/IP.

1.19.1 Detailed Introduction to Physical Layer : MU : Dec. 12

University Questions

Q. 1 Explain the layer details of OSI and TCP/IP models. **(Dec. 12, 10 Marks)**

- Physical layer is the lowest layer in the TCP/IP protocol suite. The communication at the physical layer level is still **logical** because of the presence of a hidden layer (transmission media) under the physical layer.
- The **primary responsibility** of the physical layer is to carry the individual bits present in a frame across the link.
- The transmission media (wired or wireless) is used for connecting two devices to each other. Here it is important to understand that the transmission media does not actually carry the bits.
- Instead it carries the electrical or optical signals which represents the bits which are to be carried from one device to the other.
- That means the bits received in a frame from the data link layer are transformed into an electrical or optical signal and sent over the transmission media.
- Still we consider bit as the data unit for communication between physical layers of two communicating devices.
- For the transformation of bits to signal, several physical layer protocols are available.

Following are the functions of the physical layer :

1. To define the type of encoding i.e. how 0's and 1's are changed to signals.
2. To define the transmission rate i.e. the number of bits transmitted per second.
3. To deal with the synchronization of the transmitter and receiver.
4. To deal with network connection types, including multipoint and point-to-point connections.
5. To deal with physical topologies i.e. bus, star, ring, or mesh.
6. To deal with the media bandwidth i.e. baseband and broadband transmission.
7. Multiplexing which deals with combining several data channels into one.
8. To define the characteristics between the device and the transmission medium.
9. To define the transmission mode between two devices i.e. whether it should be simplex, half duplex or full duplex.

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

1.19.2 Detailed Introduction to Data Link Layer : MU : Dec. 12

University Questions

Q. 1 Explain the layer details of OSI and TCP/IP models. **(Dec. 12, 10 Marks)**

- An internetwork consists of many LANs and WANs, connected to each other by routers.
- While travelling from source to destination a datagram has to travel through many overlapping sets of links.
- It is the responsibility of router to choose the best possible link for a datagram to travel.
- When a router does so, it is the responsibility of the data link layer to take the datagram across the link.
- The said link can be anything such as a wired LAN, a wireless LAN, or a link layer switch etc. Every type of link will use different types of protocols. The data link layer should be able to handle all the different types of protocols and move the packet through the link.
- The data link layer receives a datagram from the network layer and encapsulates it into a packet called as **frame.**
- There are no specific data link layer protocols defined by the TCP/IP suite. Instead it supports all the standard protocols that can carry the datagram successfully over the link.
- The services provided by each data link layer protocol are different.

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.

Scanned by CamScanner

2. **Flow control :**

It provides a flow control mechanism to avoid a fast transmitter from over-running a slow receiver by buffering the extra bits.

3. **Physical addressing :**

It adds a header to the frame which consists of the physical address of the sender and / or receiver of that frame.

4. **Error control :**

A trailer is added at the end of the frame in order to achieve error control. It also uses a mechanism to prevent duplication of frames.

5. **Access control :**

- The data link layer protocol perform an important function of determining which device has control over the link at any given time, when two or more devices are connected to the same link.
- The Institution of Electrical and Electronics Engineers (IEEE) felt the need to define the data link layer in more details, so they split it into two sub-layers :
  1. Logical Link Control (LLC).
  2. Media Access Control (MAC).

1.19.3 Detailed Introduction to Network Layer : MU : Dec. 12

University Questions

Q. 1 Explain the layer details of OSI and TCP/IP models. **(Dec. 12, 10 Marks)**

- The primary responsibility of the network layer is to create a connection between the source and destination computers. The communication at the network layer level is called as host to host communication.
- The several routers present between the source and destination hosts choose the best route for each travelling packet.
- Therefore the two responsibilities of the network layer are : host to host communication and routing of the packet through the possible routers.
- The main protocol in the network layer of the Internet is IP (Internet Protocol). The format of the packet (datagram) at network layer is decided by IP.
- The routing of datagrams from their source to destination is also the responsibility of IP. It achieves this by making each router forward the datagrams to the next router in its path towards the destination.
- IP is a **connectionless** protocol. It does not provide services like **flow control, error control** or even the **congestion control.**
- Therefore it is dependent on the transport layer in case if an application needs these services.
- The routing protocols included in the network layer are of unicast (one-to-one) and multicast (one-to-many) nature.
- These routing protocols have a responsibility of creating the forwarding tables for the routers to help them in the process of routing.
- There are some auxiliary protocols at the network layer, that are designed to assist IP in its delivery and routing tasks. The examples of such protocols are ICMP, IGMP, DHCP, ARP etc.
- The functioning of these protocols is as follows :

Sr. No.	Protocol	Function
1.	ICMP	To help IP report problems when routing a packet
2.	IGMP	Helps IP in multitasking
3.	DHCP	To help IP to get the network layer address for a host.
4.	ARP	Helps IP to find the link layer address of a host or router.

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.

1.19.4 Detailed Introduction to Transport Layer : MU : Dec. 12

University Questions

Q. 1 Explain the layer details of OSI and TCP/IP models. **(Dec. 12, 10 Marks)**

- The primary responsibility of the transport layer is also to provide an end to end connection.
- At the source host, the application layer sends a message to the transport layer which **encapsulates** it into a transport layer packet (which is also called as a **segment** or **user datagram**) and sends it through the logical connection (which is imaginary) to the transport layer of the destination host.
- In short the transport layer takes message from the application layer of source host and via the transport layer at the destination host delivers the message to the application layer at the destination.

Scanned by CamScanner

- For the Internet applications, there are number of transport layer protocols designed to give specific service to various application programs.
- The main protocol in the transport layer is TCP (Transmission Control Protocol) which is a connection oriented protocol.
- The main task of TCP is to establish a logical connection between the transport layers of the source and destination hosts before actually transferring the data.
- Being connection oriented, the TCP is a reliable protocol which provides the following services to an application layer program :
  1. Flow control
  2. Error control and
  3. Congestion control
- The other commonly used transport layer protocol is UDP (User Datagram Protocol). This is a connectionless protocol. Therefore it does not need to create any logical connection before transmitting the user datagrams.
- The UDP treats each datagram as a totally in dependent packet with absolutely no relation with the previous or next datagrams.
- UDP is a very simple protocol as compared to TCP. It does not provide flow control, error control or congestion control.
- UDP is an attractive protocol for certain application program specially for those who want to send small messages or those who do not afford retransmission of a packet if the packet is corrupted or lost.
- For new emerging applications in the field of multimedia, a new transport layer protocol has been designed which is called as SCTP (Stream Control Transmission Protocol).

Functions of transport layer :

The transport layer performs the following functions :

1. It divides each message into packets at the source and re-assembles then 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.

1.19.5 Detailed Introduction to Application Layer : MU : Dec. 12

University Questions

Q. 1 Explain the layer details of OSI and TCP/IP models. **(Dec. 12, 10 Marks)**

- The logical connection between the application layers of source and destination hosts is **end-to-end** type.
- The communication between the application layers of source and destination hosts takes place through all the layers.
- The application layer communication is between **two processes.** A process is nothing but a program running at the application layer.
- Thus the primary responsibility of the application layer is the **process to process communication.**
- There are many predefined protocols at the application layer in the Internet. Some of these protocols are HTTP, WWW, SMTP, FTP, TELNET, SNMP etc. These protocols and their functions are shown in Table 1.19.1.

Table 1.19.1

Sr. No.	Protocol	Function
1.	HTTP	As tool to access World Wide Web i.e. WWW.
2.	SMTP	It is the main protocol used in e-mail service.
3.	FTP	To transfer files from one host to the other.
4.	TELNET	To access a website remotely.
5.	SNMP	To manage the Internet.
6.	DNS	To find the network layer address of a computer.
7.	IGMP	To collect the membership in a group.

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 Encapsulation and Decapsulation :

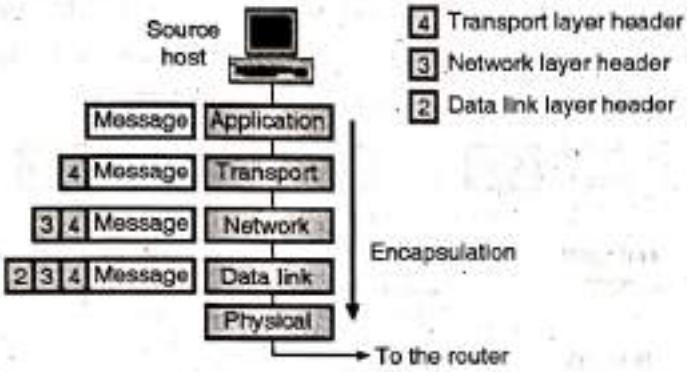
- The encapsulation / decapsulation is one of the most important concepts in the protocol layering in Internet.
- This concept applied to a small Internet has been illustrated in Fig. 1.20.1.
- In this figure, the layers of data link switches have not been shown because encapsulation or decapsulation does not take place in the data link layer switches.

Scanned by CamScanner

- In Fig. 1.20.1, the encapsulation takes place at the source host, decapsulation takes place at the destination host while both encapsulation and decapsulation takes place at the router.

1.20.1 Encapsulation at the Source Host :

Refer Fig. 1.20.1(a) to understand the process of encapsulation at the source host.



(G-2066) **Fig. 1.20.1(a) : Encapsulation at the source host**

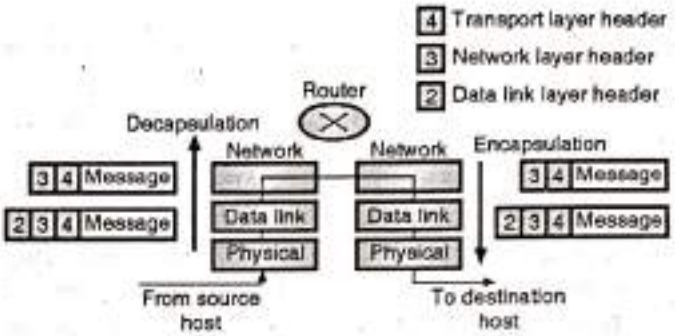
1. The data to be exchanged at the application layer is called as **message.** Normally a message does not contain any header or trailer. This message is passed on to the transport layer.
2. The transport layer takes this message which is also called as the **payload** and adds a transport layer header to it to produce the **segment** of **user datagram.** It is then passed on to the network layer. The transport layer header consists of the identifiers of the application programs at the source and destination and some additional information needed for the flow control, error control and congestion control.
3. The packet from transport layer is accepted by the network layer as its payload and adds its own header to it to produce a **datagram** as shown in Fig. 1.20.1(a). The network layer header contains the source and destination host's addresses and some additional information needed for checking errors in the header. This network layer packet (datagram) is then passed on to the data link layer.
4. The packet from the network layer is taken by the data link layer as its payload and adds its own header to it to produce a **frame** (packet at the data link layer). The link layer header contains the link layer addresses of the host or the next hop i.e. the router. This **frame** is then passed on to the physical layer for transmission.

1.20.2 Decapsulation and Encapsulation at the Router :

Refer Fig. 1.20.1(b) which illustrates the processes of decapsulation and then encapsulation occurring at a router connected to two or more links.

1. **Decapsulation :**

The router receives a set of bits at its input port. When these bits are delivered to the data link layer at the router, it decapsulates the datagram from the frame as passes it on to the network layer.

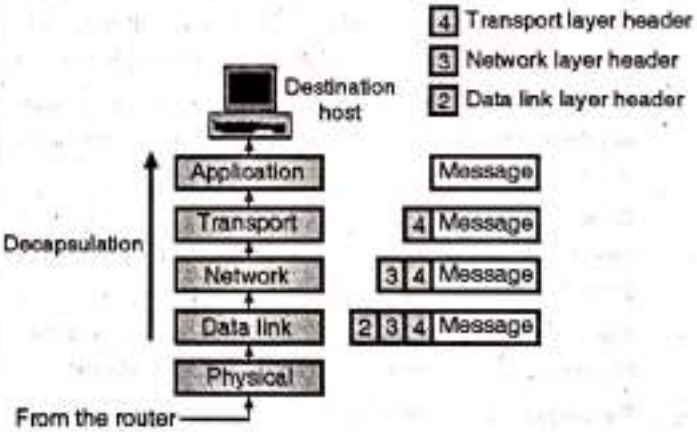


(G-2067) **Fig. 1.20.1(b) : Decapsulation / Encapsulation at the router**

2. The router checks the header for source and destination addresses. Then it refers to its forwarding tables and finds out the next hop to which this datagram is to be forwarded. Note here that the network layer at the router should not change the contents of the datagram unless fragmentation of the datagram is needed. Fragmentation is done if the datagram is too large in size. After all this, the datagram is passed to the data link layer.
3. At the data link layer, the datagram received from the network layer is encapsulated again into a frame and the frame is passed on to the physical layer which transmits it to the destination host.

1.20.3 Decapsulation at the Destination Host :

- At the destination host, only the decapsulation process is carried out at each layer, as shown in Fig. 1.20.1(c).



(G-2068) **Fig. 1.20.1(c) : Decapsulation at the destination host**

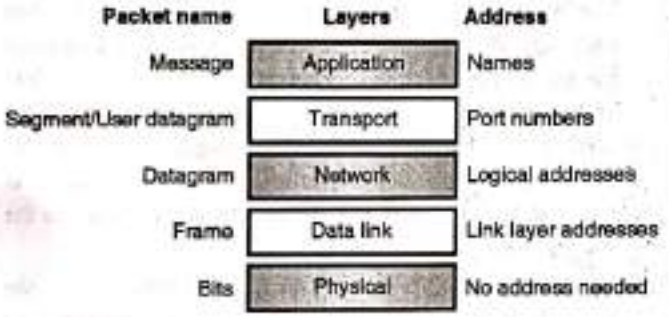
- At each layer, the payload is removed from the packet and the payload is delivered to the higher layer, by removing the headers at each stage.

Scanned by CamScanner

- Finally after removing all the headers, the message is delivered to the application layer.
- It is important to note that the **error checking** is involved in the process of decapsulation at the destination host.

1.21 Addressing in TCP/IP :

- Addressing is another important concept related to the protocol layering in the Internet.
- There is a logical connection between the pair of layers as discussed earlier. For any communication to take place between a source and a destination, two addresses namely source address and destination address are needed.
- Thus we will need four pairs of such addresses corresponding to the data link, network, transport and application layers.
- There is no need of addresses at the physical layer because communication at the physical layer takes place in bits which can not have an address.
- Fig. 1.21.1 shows the addressing at each layer.

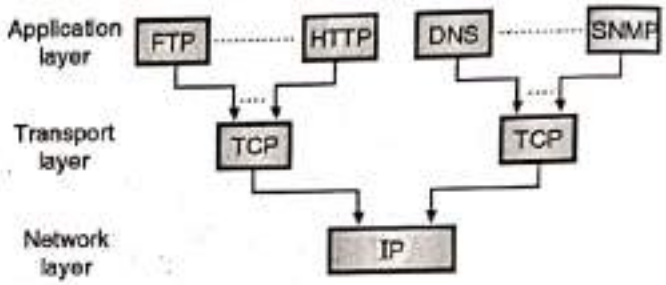


(G-2069) **Fig. 1.21.1 : Addressing in TCP/IP protocol suite**

- Fig. 1.21.1 also shows the relationship between various layers, the addresses used in each layer and the name of the packet at each layer.
- We generally use the **names** to define the **site address** which provides the required services. For example **techmaxbook.com,** at the application layer. It is also possible to use the email address such as **jayantkatre@gmail.com.**
- The addresses at the transport layer are called as **port numbers.** These define the programs at the application layer of source and destination.
- There are several application layer programs running at a time. Port numbers are the local addresses which are used to distinguish between these programs.
- The addresses at the network layer are global in nature because the whole Internet is the scope of these addresses.
- The connection of a device to the Internet is uniquely defined by a network layer address.
- The addresses at the data link layer are called as the **MAC addresses.** These are the locally defined addresses. Each host or router in a network such as LAN or WAN always has a MAC address.

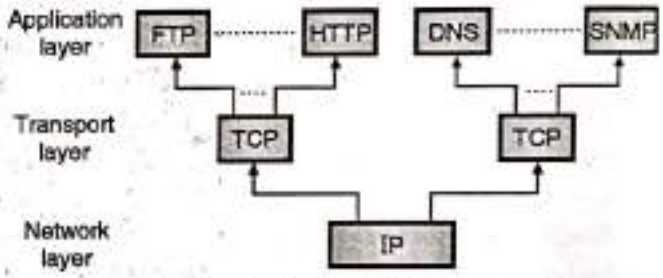
1.22 Multiplexing and Demultiplexing in TCP/ IP :

- In TCP/IP protocol, many protocols are being used at the same layer. Therefore multiplexing is needed at the source and demultiplexing is needed at the destination.
- In the process of **multiplexing** as shown in Fig. 1.22.1(a), a protocol at one layer in TCP/IP can encapsulate a packet (one at a time) from several protocols corresponding to the next higher layer in TCP/IP suite.



(G-2070) **Fig. 1.22.1(a) : Multiplexing in TCP/IP**

- In the process of demultiplexing, a protocol will decapsulate and deliver a packet one at a time to several protocols belonging to the next higher layer in TCP/IP protocol suite as shown in Fig. 1.22.1(b).



(G-2071) **Fig. 1.22.1(b) : Demultiplexing in TCP/IP**

- As shown in Fig. 1.22.1(a), at the transport layer two protocols TCP and UDP are capable of multiplexing the messages coming from various protocols at the application layer.
- Next the segments from TCP or user datagrams from UDP are accepted and multiplexed by IP at the network layer.
- IP can also multiplex the packets from some other protocols such as ICMP or IGMP etc.
- The frames at the data link layer level can carry the payload coming from the network layer protocols such as IP or ARP etc.

Scanned by CamScanner

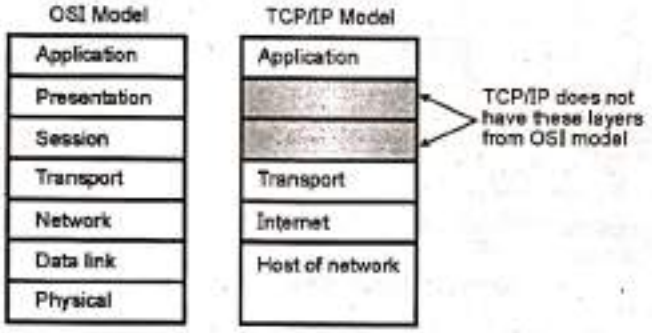
1.23 Comparison of OSI and TCP/IP Models :

1.23.1 Similarities between OSI and TCP/IP Models :

Following are some of the similarities between OSI and TCP/IP models :

1. In both the models the functions of layers is approximately same.
2. Both models use the concept of layered architecture.
3. The transport layers and the layers below it provide transport services independent of networks.
4. In both the models, the layers above transport layer are application oriented.

– Refer to Fig. 1.23.1 and Table 1.23.1 for the comparison of the two reference models.



(G-73) **Fig. 1.23.1 : Relationship between OSI and TCP/IP models**

1.23.2 Difference between OSI & TCP/IP :

MU : Dec. 14, May 17, Dec. 17

University Questions

Q. 1 Why there is a need for layered designing for networking and communication ? Compare the TCP/IP and OSI reference models.

(Dec. 14, 10 Marks)

Q. 2 What is ISO-OSI reference model ? Compare it with TCP/IP reference model. Which layer is used for the following :

1. To route packets
2. To convert packets to frame
3. To detect and correct errors.
4. To run services like FTP, telnet etc.

(May 17, 10 Marks)

Q. 3 Explain the need of layered design for communication and networking. Compare the OSI reference model & TCP/IP. **(Dec. 17, 10 Marks)**

Table 1.23.1 : 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 can not 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.

1.23.3 Demerits of TCP/IP Model :

1. TCP/IP model does not clearly distinguish the concepts of service, interface and protocol.
2. This model is not at all general and it can not describe any protocol stack other than TCP/IP.
3. The host-to-network layer is not a layer at all in the normal sense. It is simply an interface.
4. The TCP/IP model does not even mention the physical and data link layers. A proper model should include both as separate layers.

1.23.4 Hybrid (Internet) Reference Model :

– In spite of many problems associated with the OSI model, it has proved to be very useful one practically.

– But the OSI protocols have not become popular.

– On the other hand the TCP/IP model is practically non existing but the TCP/IP protocols are used widely.

– So sometimes a modified OSI model with primary concentration on TCP/IP is used which is called as the hybrid model.

Scanned by CamScanner

- The hybrid model is shown in Fig. 1.23.2. It is also called as the Internet model.

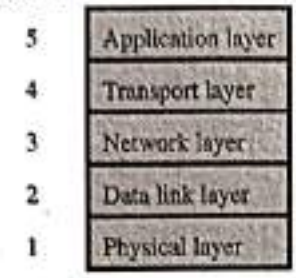
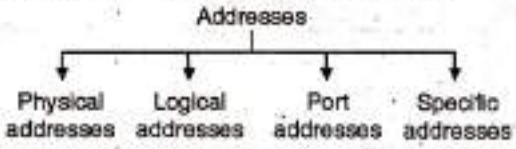


Fig. 1.23.2 : Hybrid model

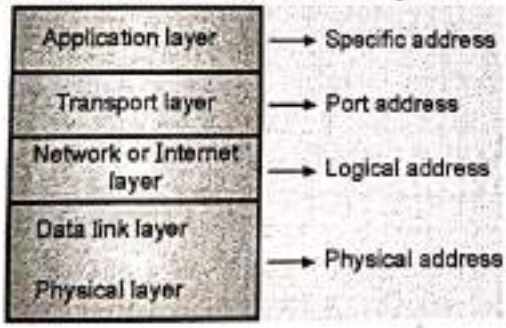
1.24 Addressing :

- When the computers wish to communicate with one another, they need to know the address of each other. Each computer has its own address.
- The addresses can be of different types such as physical addresses or logical address.
- In an internet employing the TCP/IP protocols, four levels of addresses are used by the computers.
  1. Physical address
  2. Logical address (IP)
  3. Port address and
  4. Specific address
- Fig. 1.24.1 shows the classification of addresses.



(G-75) **Fig. 1.24.1 : Classification of addresses in TCP/IP**

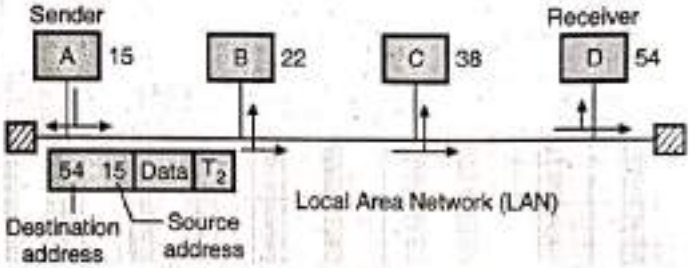
- Each of these addresses is associated with a specific layer of TCP/IP architecture as demonstrated in Fig. 1.24.2.
-



(G-76) **Fig. 1.24.2 : Relation between TCP/IP structure and addresses**

1.24.1 MAC Address (Physical 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 recognized by their MAC addresses.
- A MAC address is a local address. It is unique locally but it is not unique universally.
- The IP and MAC address are two different identifiers and both of them are needed, because a physical network can have two different protocols at the network layer at the same time.
- Similarly a packet may pass through different physical networks.
- So to deliver a packet to a host or a router, we require two levels of addressing namely IP addressing and MAC addressing.
- Most importantly we should be able to map the IP address into a corresponding MAC address.
- The size and format of the physical address varies depending on the nature of network.
- The Ethernet (LAN) uses a 48-bit (6-byte) physical address which is imprinted on the network interfacing card (NIC).
- Refer Fig. 1.24.3 which explains the concept of physical addressing.



(G-77) **Fig. 1.24.3 : Physical addresses**

- The sender computer with a physical address of 15 wants to communicate with the receiver computer with a physical address 54.
- The frame sent by the sender consists of the destination address, sender's address, encapsulated data and a trailer (T_2) that contains the error control bit.
- When this frame travels over the bus topology, every computer receives it and tries to match it with its own physical address.
- If the destination address in the frame header does not match with the physical address it will simply drop the frame.
- At receiver computer (D), the destination address matches with its physical address (54). So the frame is accepted and decapsulation is carried out to recover the data.
- The example of a 48 bit or 6 byte physical address is as follows. It contains 12-hexadecimal digits.

08 : 63 : 4C : 81 : 08 : 1D

1.24.2 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.

Scanned by CamScanner

- Internet is a packed switched network that means the data form 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.

1.24.3 Port Address :

- The modern computers are designed to run multiple processes on it simultaneously.
- The main objective of internet is the process to process communication. For this purpose it is necessary to lable or name the processes.
- Thus the processes need addresses. The lable assigned to a process is called as a port address. It is a 16 bit address.

1.24.4 Specific Addresses :

- Some applications have user friendly addresses. The examples of specific addresses are the e-mail addresses or the University Resource Locators (URL).

Review Questions

Q. 1 State various services provided by the network for companies and people.

Q. 2 What is the difference between broadcast and point to point networks ?

Q. 3 What is meant by internetwork ?

Q. 4 Write a short note on MAN.

Q. 5 Write a short note on WAN.

Q. 6 Compare LAN, WAN and MAN.

Q. 7 Define peer.

Q. 8 How does the actual data transfer take place between two machines ?

Q. 9 Write a note on : Virtual communication between layers.

Q. 10 Discuss the important design issues for various layers.

Q. 11 Write a note on connection oriented and connectionless services.

Q. 12 What is relationship between services and protocols ?

Q. 13 Draw the OSI reference model and explain the functions of different layers.

Q. 14 Compare different types of network topologies.

Q. 15 State the difference between broadcast and point to point networks.

Q. 16 Compare peer to peer and client server networks.

Q. 17 State the reasons for having a 5 layered protocol architecture and state its advantages and disadvantages.

Q. 18 What are the design issues for the layers ?

Q. 19 Define : Interfaces and services.

Q. 20 Name the different network topology types.

Q. 21 Explain the basic concepts of bus topology with the help of suitable diagram.

Q. 22 State the important characteristics of bus topology.

Q. 23 Name the transmission media used for bus LANs.

Q. 24 State advantages and disadvantages of bus topology.

Q. 25 Write a note on : Ring topology.

Q. 26 What are the problems faced by the ring topology ?

Q. 27 State the advantages and disadvantages of ring topology.

Q. 28 Write a short note on star topology.

Q. 29 What is the difference between single level star topology and two level star topology ?

Q. 30 State the advantages and disadvantages of star topology.

Q. 31 Write a short note on Mesh topology.

Scanned by CamScanner

Q. 32 State advantages and disadvantages of mesh topology.

Q. 33 Write a short note on tree topology.

Q. 34 Compare Ring and Bus.

Q. 35 Compare Star and Ring.

Q. 36 Explain the TCP / IP reference model

Q. 37 Compare the OSI and TCP / IP reference models.

Q. 38 Explain the concept of addressing.

Q. 39 What is the IP address ?

Q. 40 What is the difference between IP and MAC address ?

Q. 41 Explain the concept of port addressing.

Q. 42 What is the difference between IP address and port numbers ?

1.25 University Questions and Answers (New Syllabus) :

Dec. 2018 [Total Marks : 18]

Q. 1 What are the design issues for the OSI layers ? **(Section 1.12)** **(4 Marks)**

Q. 2 Differentiate between connection oriented and connectionless service ?

(Section 1.14.3) **(4 Marks)**

Q. 3 What is topology ? Explain the types of topologies with diagram, advantages and disadvantages.

(Sections 1.4, 1.4.1, 1.4.2, 1.4.3, 1.4.5 and 1.4.6) **(10 Marks)**

❑❑❑

Scanned by CamScanner

CHAPTER 2

Module 2

Physical Layer

Syllabus :

Introduction to communication system, Digital communication, Electromagnetic spectrum, Guided transmission media : Twisted pair, Coaxial, Fiber optics, Unguided media (Wireless transmission) : Radio waves, Microwave, Bluetooth, Infrared, Circuit and packet switching.

2.1 Introduction to Communication System :

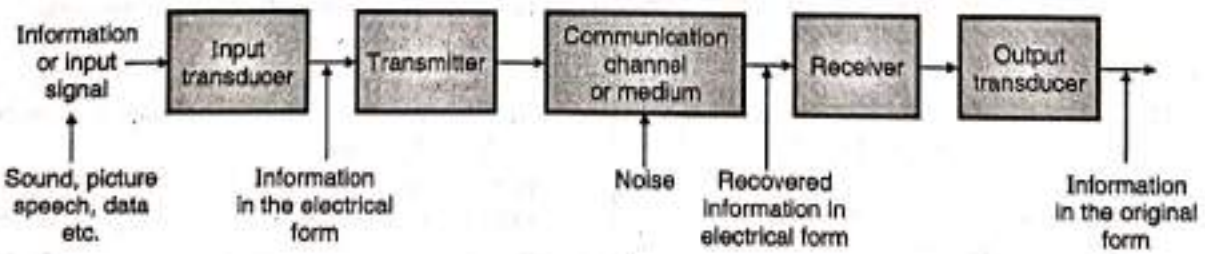
- The communication branch is the oldest branch of the electronics field. Telecommunication means communicating at a distance. A communication system is the means of conveying the information from one place to the other. This information can be of different types such as sound, picture, music, computer data etc.
- The field of communication engineering started developing rapidly in the nineteenth century when the telegraph, telephone and then the radio were invented. The development was still faster in the twentieth century when first the black and white and then colour TVs were brought in use. Then came the age of satellite communication, cable TV, mobile telephones etc.
- In order to understand the subject, it is necessary to understand the basic concepts in communication engineering such as, modulation, noise, demodulation, information theory etc.

2.1.1 Elements of Communication System :

- The block diagram of the simplest possible communication system is as shown in Fig. 2.1.1.
- As seen from the Fig. 2.1.1, the elements of a basic communication system are transmitter, a communication medium (channel) and the receiver.
- When the transmitted signal is travelling from the transmitter to the receiver over a communication channel, noise gets added to it.
- The elements of basic communication system are as follows :
  1. Information or input signal
  2. Input transducer
  3. Transmitter
  4. Communication channel or medium
  5. Noise 6. Receiver 7. Output transducer

Information or Input signal :

- The communication systems have been developed for communicating useful information from one place to the other.
- This information can be in the form of a sound signal like speech or music, or it can be in the form of pictures (TV signals) or it can be data information coming from a computer.



(D-1) **Fig. 2.1.1 : Block diagram of the basic communication system**

Scanned by CamScanner

Input transducer :

- The information in the form of sound, picture or data signals cannot be transmitted as it is.
- First it has to be converted into a suitable electrical signal. The input transducer block does this job.
- The input transducers commonly used in the communication systems are microphones, TV camera etc.

Transmitter :

- The function of the transmitter block is to convert the electrical equivalent of the information to a suitable form.
- In addition to that it increases the power level of the signal. The power level should be increased in order to increase the range of transmitted signal.
- The transmitter consists of the electronic circuits such as amplifier, mixer, oscillator and power amplifier.

Communication channel or medium :

The communication channel is the path used for transmission of electronic signal from one place to the other. The communication medium can be conducting wires, cables, optical fibre or free space. Depending on the type of communication medium, two types of communication systems will exist. They are :

- Wired communication or line communication
- Wireless communication or radio communication

1. **Line communication :**
   - The line communication systems use the communication mediums like the simple wires or cables or optical fibers.
   - The examples of such systems, are telegraph and telephone systems, cable T.V. etc.
   - Due to physical connection from one point to the other, these systems cannot be used for the communication over long distances.

2. **Radio communication :**
   - The radio communication systems use the free space as their communication medium. They do not need the wires for sending the information from one place to the other.
   - The radio or TV broadcasting, satellite communication are the examples of the wireless communication. These systems transmit the signal using a transmitting antenna in the free space.
   - The transmitted signal is in the form of electromagnetic waves. A receiving antenna will pick up this signal and feed it to the receiver.
   - Radio communication can be used for the long distance communication such as from one country to the other or even from one planet to the other.

Noise :

- Noise is an unwanted electrical signal which gets added to the transmitted signal when it is travelling towards the receiver.
- Due to noise, the quality of the transmitted information will degrade. Once added, the noise cannot be separated out from the information.
- Hence noise is a big problem in the communication systems. (Specially analog communication systems).
- The noise can be either natural or manmade. The sources of natural noise are lightning or radiation from the sun and stars etc.
- The man made noise includes the noise produced by electrical ignition systems of the automobiles, welding machines, electric motors etc.
- Eventhough noise cannot be completely eliminated, its effect can be reduced by using various techniques.

Receiver :

- The process of reception is exactly the opposite process of transmission. The received signal is amplified, demodulated and converted into a suitable form.
- The receiver consists of electronic circuits like mixer, oscillator, detector, amplifier etc.

Output transducers :

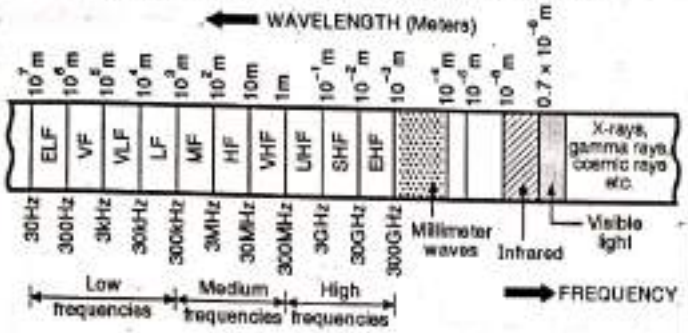
- The output transducer converts the electrical signal at the output of the receiver back to the original form i.e. sound or TV pictures etc.
- The typical examples of the output transducers are loud speakers, picture tubes, computer monitor etc.

2.2 The Electromagnetic Spectrum :

- The information signal should be first converted into an electromagnetic signal before transmission because the wireless transmission takes place using the electromagnetic waves.
- The electromagnetic waves consist of both electric and magnetic fields. The electromagnetic waves can travel a long distance through space.
- The electromagnetic signals are also called as Radio Frequency (RF) waves.
- The EM waves oscillate. They are sinusoidal and their frequency is measured in Hz.
- The frequency of EM signal can be very low or it can be extremely high. This entire range of frequencies of EM waves is called as **Electromagnetic spectrum.**
- The electromagnetic spectrum consists of signals such as 50 Hz line frequency and voice signals at the lower end.
- The radio frequencies which are used for the two way communication reside at the center of the EM spectrum. These frequencies are used for the applications such as radio or TV broadcasting as well.

Scanned by CamScanner

- The infrared and visible light are at the upper end of the EM spectrum.
- Fig. 2.2.1 shows the entire electromagnetic spectrum.



(D-16) **Fig. 2.2.1 : Complete electromagnetic (EM) spectrum**

- The short forms used in the EM spectrum of Fig. 2.2.1 have the following meanings.

2.2.1 Different Frequency Bands :

Table 2.2.1 : Segments of the electromagnetic spectrum

Sr. No.	Name	Frequency	Wavelength
1.	Extremely low frequencies (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-3 GHz	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	30 to 430 THz	0.7 to 10 μm
12.	Visible light	375-750 THz	0.4 μm to 0.8 μm

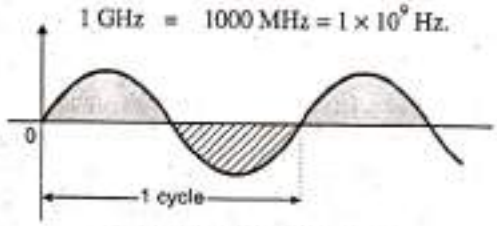
2.2.2 Frequency and Wavelength :

In the EM spectrum, we have used frequency as well as wavelength in order to define various segments. So let us define these terms and the relation between them.

Frequency :

- Frequency is defined as the number of cycles of a waveform per second. It it expressed in hertz (Hz).
- The units used to measure higher frequencies are kilohertz (kHz), Megahertz (MHz) and Gigahertz (GHz). Their relation with the basic unit Hz is as follows :

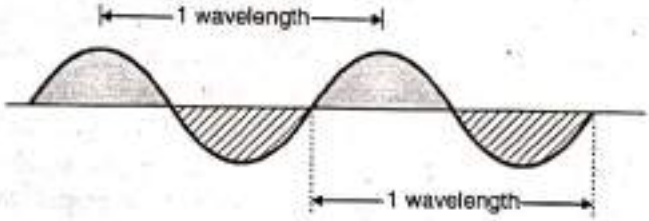
$$1 \text{ kHz} = 1000 \text{ Hz}$$
$$1 \text{ MHz} = 1000 \text{ kHz} = 1 \times 10^6 \text{ Hz.}$$
$$1 \text{ GHz} = 1000 \text{ MHz} = 1 \times 10^9 \text{ Hz.}$$



(D-17) **Fig. 2.2.2 : One cycle**

Wavelength (λ) :

- Wavelength is defined as the distance travelled by an electromagnetic wave during the time of one cycle. Refer Fig. 2.2.3 for the concept of wavelength.



(D-18) **Fig. 2.2.3 : Definition of wavelength**

- Since EM waves travel at the speed of light in the free space or vaccum, their wavelength is given by,

$$\lambda = \frac{\text{Speed of light}}{\text{Frequency}} = \frac{3 \times 10^8 \text{ m/S}}{f} \quad ...(2.2.1)$$

- Hence wavelength decreases with increase in frequency.

2.2.3 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 :
  1. In astronomy to detect stars and other heavenly bodies.
  2. In the guided weapon systems.
  3. TV remote control.
  4. Wireless keyboards and mouse.

Scanned by CamScanner

2.2.4 Visible Light :

- Light is a special type of electromagnetic radiation. It has wavelength in the range of 0.4 to 0.8 μm.
- Light is used for various kinds of communications.
- 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.

2.3 Digital Communication :

2.3.1 Advantages of Digital Communication :

Some of the advantages of digital communication are as follows :

1. Due to the digital nature of the transmitted signal, the interference of additive noise does not introduce many errors. So digital communication has a better noise immunity.
2. Due to the channel coding techniques used in digital communication, it is possible to detect and correct the errors introduced during the data transmission.
3. Repeaters can be used between transmitter and receiver to regenerate the digital signal. This improves the noise immunity further and also extends the range of communication.
4. Due to the digital nature of the signal, it is possible to use the advanced data processing techniques such as digital signal processing, image processing, data compression etc.
5. TDM (Time Division Multiplexing) technique can be used to transmit many voice channels over a single common transmission channel. Thus digital telephony is possible to achieve.
6. Digital communication is suitable in military applications where only a few permitted receivers can receive the transmitted signal.
7. Digital communication is becoming simpler and cheaper as compared to the analog communication due to the invention of high speed computers and integrated circuits (ICs).

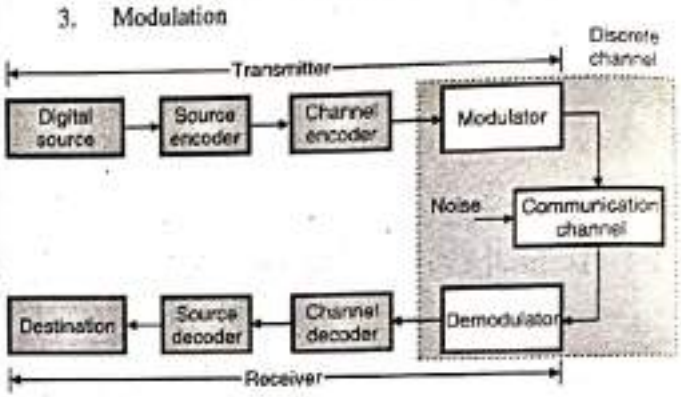
2.3.2 Disadvantages :

Some of the important disadvantages of digital communication are :

1. The bit rates of digital systems are high. Therefore they require a larger channel bandwidth as compared to analog systems.
2. Digital modulation needs synchronization in case of synchronous modulation.

2.3.3 Digital Communication System :

- Two of the most commonly used digital communication systems are PCM (Pulse Code Modulation) and DM (Delta Modulation).
- Fig. 2.3.1 shows the block diagram of a digital communication system. In this diagram three basic signal processing operations have been included. They are :
  1. Source coding 2. Channel coding
  3. Modulation



(E-3) **Fig. 2.3.1 : Digital communication system**

- The source of information is assumed to be digital. If it is analog then it must be converted first to digital.

Source coding :

- In source coding the source encoder converts the digital signal generated at the source output into another signal in digital form. Source encoding is used to reduce or eliminate redundancy for ensuring an efficient representation of the source output. Different source coding techniques are PCM, DM, ADM etc.
- The conversion of signal from one form to the other is called as mapping. Such a mapping is usually one as to one.
- Due to elimination of redundancy the source coding provides an efficient representation of the source output.

Source decoder :

- Source decoder is at the receiver and it behaves exactly in an inverse way to the source encoder.
- It delivers the destination (user) the original digital source output.

Main advantage of using the source coding is that it reduces the redundancy and therefore the bandwidth requirement.

Channel coding :

- Channel encoding is done to minimize the effect of channel noise.
- This will reduce the number of errors in the received data and will make the system more reliable. Channel coding technique introduces some redundancy.

Scanned by CamScanner

- The channel encoder maps the incoming digital signal into a channel input.

Channel decoder :

- The channel decoder is at the receiver and it maps the channel output into a digital signal in such a way that effect of channel noise is reduced to a minimum.
- Thus channel encoder and decoder together provide a reliable communication over a noisy channel. This is achieved by introducing redundancy (parity bits) in a prescribed form, at the transmitter.
- The output of the channel encoder is a series of codewords which includes the message and some parity bits. These additional parity bits introduce redundancy.
- The channel decoder converts these codewords into digital messages.

Thus in source coding the redundancy is removed whereas in channel coding the redundancy is introduced in a controlled manner.

- The source encoding alone or channel encoding alone can be performed. It is not essential to perform both but in many systems both these are performed together.
- It is possible to change the sequence in which channel encoding and source encoding are being performed.
- Channel and source encoding improve the system performance at the expense of increased circuit complexity.

Modulation :

- Modulation is used for providing an efficient transmission of the signal over the channel. The modulator can use any of the CW digital modulation techniques such as ASK (amplitude shift keyings), FSK (frequency shift keying) or PSK (phase shift keying).
- The demodulator is used for demodulation.

Discrete channel :

- As shown by a dotted box in Fig. 2.3.1, the discrete channel consists of modulator, channel and detector.
- It is called as discrete channel because its input as well as output are in the discrete form.
- In the traditional systems the modulation and coding are performed separately. But this increases the bandwidth requirement.
- Hence in some application these two operations are performed simultaneously.

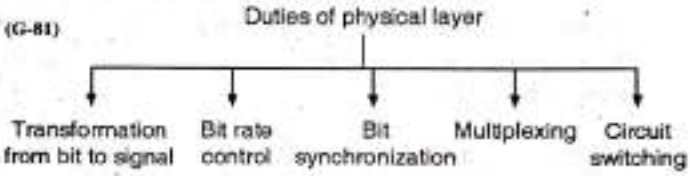
2.4 Introduction to Physical Layer :

- In this chapter we are going to discuss about the lowest layer in the OSI model called the physical layer.
- The physical layer defines the mechanical, electrical and timing interfaces to the network.
- This chapter also deals with the fundamental limits put by the nature on data transmission over a channel.
- Later on in the chapter various types of transmission media such as guided, wireless and satellite have been discussed.

2.4.1 Physical Layer Design Issues :

- The major task of physical layer is to provide services for the data link layer.
- Following are the services provided or duties of the physical layer or the design issues of the physical layer.

(G-81)



Transformation from bit to signal :

- The data link layer consists of 0's and 1's in the bit form. This bit stream can not travel as it is on the transmission medium.
- So the physical layer converts the bit stream into a signal which is suitable for the transmission medium.

Bit rate control :

- The highest value of bit rate depends on the transmission medium being used and the physical layer acts as a bit rate controller.
- The design of the physical layer hardware and software will determine the data rate.

Bit synchronization :

- The timing related to the data bit transfer is very important in computer communication.
- The physical layer governs the synchronization of the bits by providing a clock which controls the transmitter as well as receiver.

Multiplexing :

- Physical layer can use different techniques of multiplexing, in order to improve the channel efficiency.

Switching :

- There are three switching methods, namely circuit switching, message switching and packet switching. Out of which circuit switching is the function of physical layer.

Scanned by CamScanner

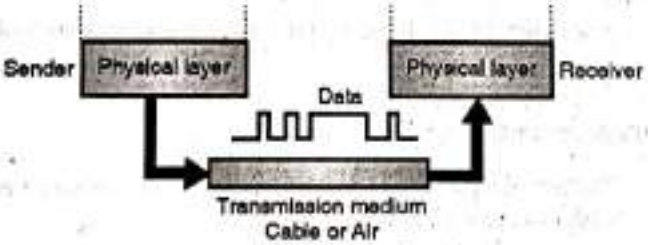
Medium :

- The signal always travels over some medium from sender to destination.
- The medium can be a coaxial cable or optical fiber etc. A medium does not pass all frequencies equally due to its inadequate frequency spectrum.
- It may pass some frequencies and weaken or block the other frequencies.
- Hence when a composite signal is passed over such a transmission medium, at the receiving end we get a wave, having a different shape as shown in Fig. 2.4.1.
- To avoid the signal distortion, the medium should pass all the frequencies present at the input without any change.
- But no medium is perfect and so some signal distortion is bound to take place.

(G-82) **Fig. 2.4.1 : Signal distortion on a transmission medium**

2.4.2 Transmission Media and Physical Layer :

- Fig. 2.4.2 shows the location of the transmission media in the OSI model.
- So we can say that transmission media belongs to the lowest layer (layer 0) of the OSI model, as shown in Fig. 2.4.2 and the physical layer controls the transmission media directly.



(L-570) **Fig. 2.4.2 : Relation between transmission medium and physical layer**

- Transmission medium is the cable or air over which data can travel from sender to receiver in the form of digital or analog signals.

2.5 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.

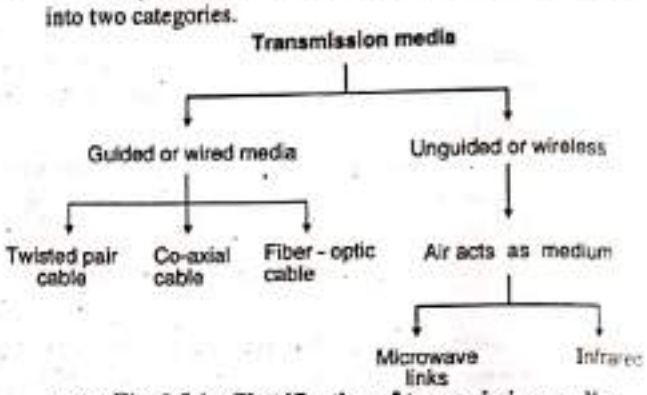
2.5.1 Classification of Transmission Media :

MU : May 17

University Questions

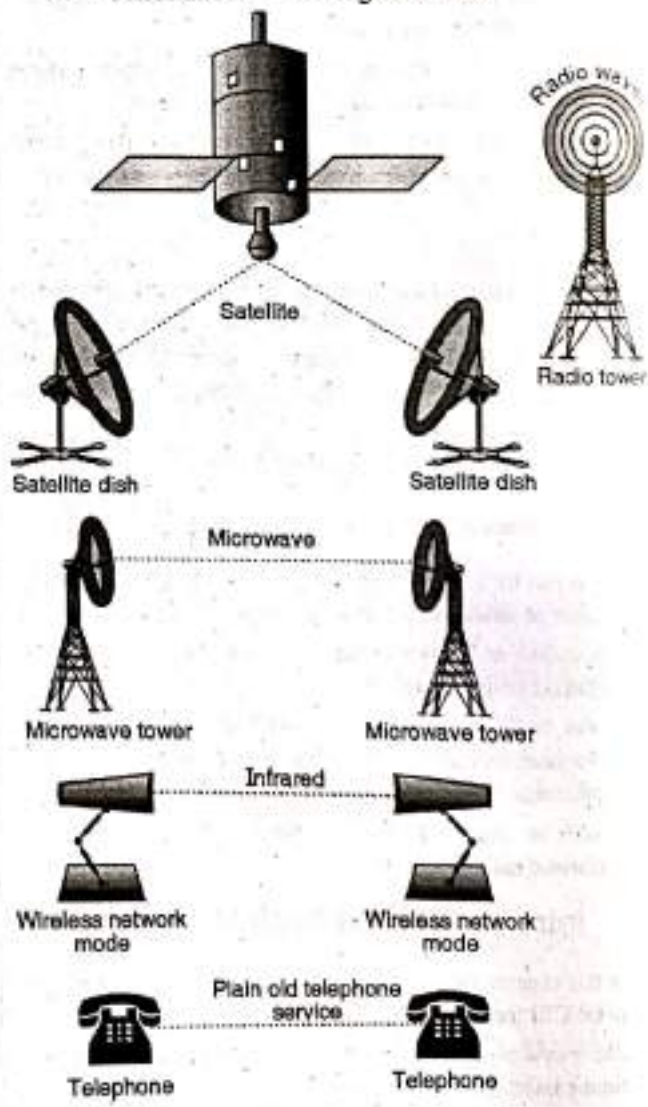
Q.1 What are the different guided and unguided transmission media ? **(May 17, 5 Marks)**

- We can classify the transmission media as shown in Fig. 2.5 into two categories.



(L-571) **Fig. 2.5.1 : Classification of transmission media**

- Media are roughly grouped into two classes :
  1. Guided media 2. Unguided media



(L-573) **Fig. 2.5.2 : Transmission media**

Scanned by CamScanner

2.5.2 Wired Media (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.
- In this type of media, the signal energy is contained and guided within a solid media.
- The examples of wired media are copper pair wires, coaxial cables and fiber optic cables.
- The wired media is used for point to point communication.

2.5.3 Wireless Media (Unguided Media) :

- The wireless media is also called as an unguided media.
- In the wireless media, the signal energy propagates in the form of unguided electromagnetic waves.
- The examples of wireless media are radio and infrared light.
- The wireless media is used for radio broadcasting in all the directions.
- The examples of guided and unguided media are a shown in Fig. 2.5.2.

2.5.4 Comparison of Wired and Wireless Media :

Comparison of wired and wireless media is given in Table 2.5.1.

Table 2.5.1 : 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.

2.5.5 Guided Media :

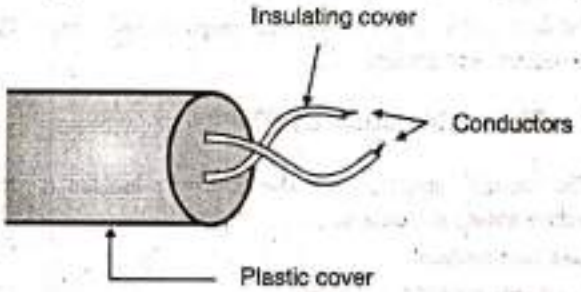
The most commonly used networking media are :

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

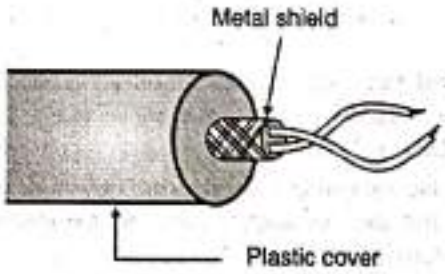
The selection of networking media depends on various factors such as cost, connectivity, bandwidth, performance in presence of noise, geographical coverage etc.

2.6 Twisted Pair Cables :

- The construction of twisted pair cable is as shown in Fig. 2.6.1. This is a very commonly used medium and it is cheaper than the co-axial cable or optical fiber cable.



(a) UTP



(b) STP

(L-574) **Fig. 2.6.1 : Construction of twisted pair cables**

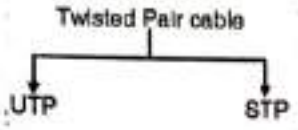
2.6.1 Types of Twisted Pair Cables :

- The two commonly used types of twisted pair cables are as follows :
  1. Unshielded twisted pair (UTP)

Scanned by CamScanner

2. Shielded twisted pair (STP)

- The construction of UTP and STP cables is shown in Fig. 2.6.1.



(G-97)

STP :

- STP cable as shown in Fig. 2.6.1(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 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.

2.6.2 Characteristics of STP :

1. The twisted conductors are shielded by a braided mesh to reduce noise interference.
2. Low cost medium
3. Used only for IBM computers
4. Support data rates upto several Mbps.

UTP :

- A twisted pair consists of two insulated conductor twisted together in the shape of a spiral as shown in Fig. 2.6.1. 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.

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.

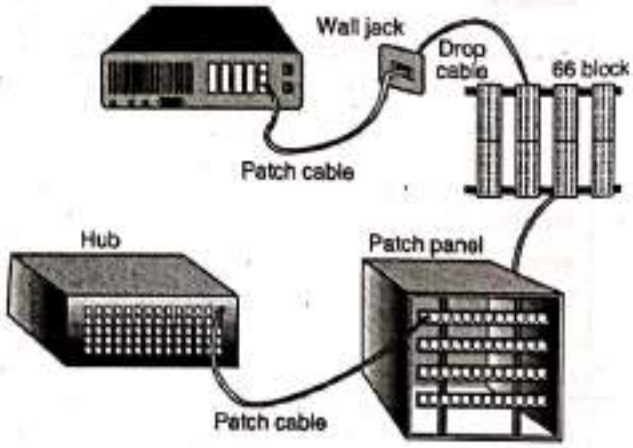
2.6.3 Categories of UTP :

- Table 2.6.1 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 2.6.1 : 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
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. 2.6.2.



(L-575) **Fig. 2.6.2 : A common UTP installation**

Scanned by CamScanner

2.6.4 Characteristics of UTP :

1. The wires are not shielded.
2. Noise and electromagnetic interference is high.
3. UTP is an economical medium.
4. Can support data rate of several Mbps.
5. Installation is easy.
6. Used in applications like analog and digital telephony, LAN etc.

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 :
  1. **Category 3 :** Characteristics of UTP cables and associated connecting hardware are specified upto 16 MHz.
  2. **Category 4 :** Under this category, the characteristics of UTP cables and associated connecting hardware have been specified for the data rates upto 20 MHz.
  3. **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.

2.6.5 Applications of Twisted Pair Cables :

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

1. Local area networks for connecting computers to each other.
2. In the ISDN (Integrated Services Digital Network).
3. In the digital subscriber line (DSL).
4. In the analog telephony (conventional telephone line) to carry voice and data signals.
5. 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.

2.6.6 Comparison of Twisted Pair Cables :

Sr. No.	Factors	UTP	STP
1.	Bandwidth	1 – 155 Mbps (typically 10 Mbps)	1 – 155 Mbps (typically 16 Mbps)
2.	Number of node 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

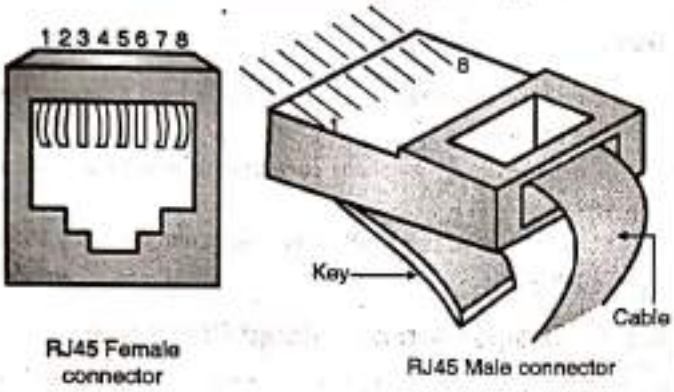
2.6.7 Connectors :

- 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.

Scanned by CamScanner

2.6.8 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. 2.6.3.
- This connector can be inserted in only one way.



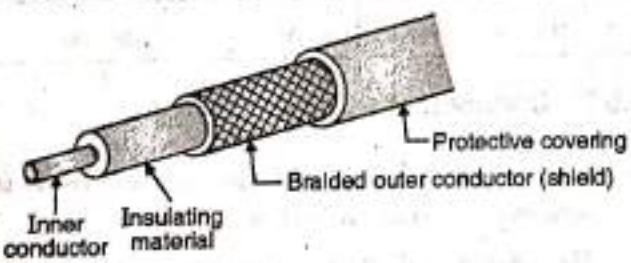
(G-340) **Fig. 2.6.3 : UTP RJ45 connector**

2.7 Co-axial Cables : MU : May 07

University Questions

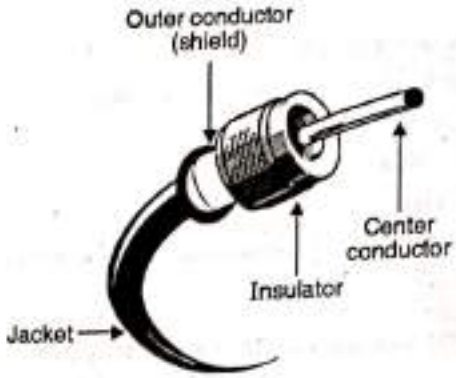
Q. 1 State different physical media properties, explain any one in detail. **(May 07, 10 Marks)**

- The construction of co-axial cable is as shown in Fig. 2.7.1. 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. 2.7.1 : 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. 2.7.2.



(L-577) **Fig. 2.7.2 : 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. 2.7.2 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.

2.7.1 Characteristics of a Co-axial Cable :

MU : May 07

University Questions

Q. 1 State different physical media properties, explain any one in detail. **(May 07, 10 Marks)**

- The important characteristics of a co-axial cable are as follows :
- Two types of cables having 75 Ω and 50 Ω 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.

Scanned by CamScanner

- 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).

Note : 50 Ω cable is commonly used for digital transmission and 75 Ω cable is used for analog transmission. Two types of co-axial cables based on the frequency they support - Baseband (0 – 4 kHz) and Broadband (above 4 kHz). Baseband co-axial is used for telephone networks and Broadband co-axial is used for cable TV. Co-axial cables have different sizes. They are classified by their size (RG) and by their resistance to direct or alternating electric currents. (measured in ohms, also called impedance).

2.7.2 Co-axial Cable Standards :

Table 2.7.1 shows the co-axial cable standards. The co-axial cables are categorised by their RG ratings where RG stands for Radio Government.

Table 2.7.1 : Categories of co-axial cables

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

2.7.3 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

2.7.4 Advantages of Co-axial Cable :

1. Excellent noise immunity due to the shield
2. Larger bandwidth than twisted pair cables
3. Losses are small
4. Can be used for high data rates
5. Less attenuation
6. They are easy to install.

2.7.5 Disadvantages :

1. Costlier than the twisted pair cables.
2. BNC connectors are required to be used for connection.

2.7.6 Baseband Co-axial Cable :

The baseband co-axial cable is the one that makes use of digital signaling. 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 50 Ω rather than 75 Ω 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 2.7.2.

Table 2.7.2 : IEEE 802.3 specifications for 10 Mbps baseband co-axial cable Bus LAN

Sr. 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

2.7.7 Broadband Co-axial Cable :

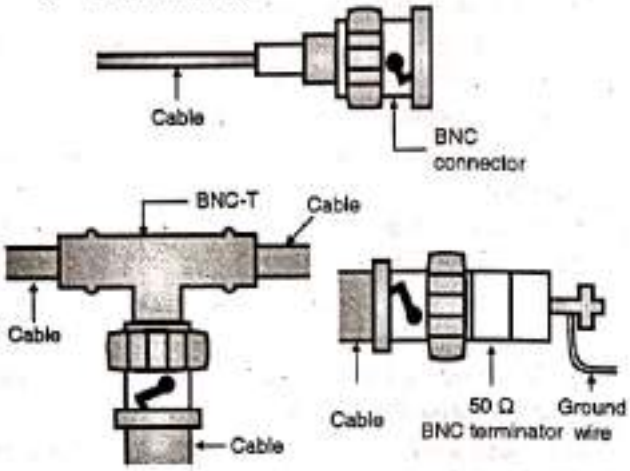
- This is the co-axial cable which is used in the cable TV system. It has higher bandwidth compared to the baseband cable.
- The type of signaling is analog at radio frequencies.
- This cable has certain disadvantages such as it is more expensive, more difficult to install and maintain as compared to 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.

2.7.8 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.

Scanned by CamScanner

- 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 Bayone-Neill-Concelman or BNC connectors.
- Fig. 2.7.3 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.



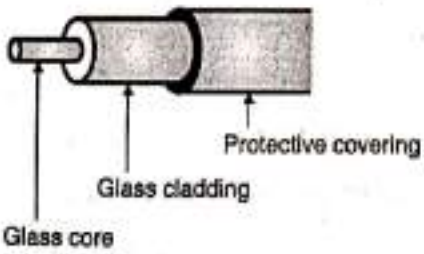
(G-341) **Fig. 2.7.3 : BNC connectors of different types**

- The BNC connector connects the end of the cable to a device such as a TV set.
- The BNC – T connector is used in Ethernet networks for branching out a cable for connection to a computer or other devices. A cable is connected to one leg of T and two more cables can be connected to the remaining two legs as shown in Fig. 2.7.3.
- The BNC terminator is used at the end of the cable as a termination. This avoids reflection of signal.

2.8 Optical Fiber Cables :

Construction :

- The construction of an optical fiber cable is as shown in Fig. 2.8.1.
- 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.

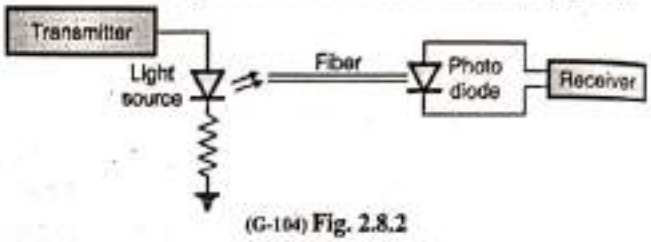


(G-103) **Fig. 2.8.1 : Construction of optical fiber cable**

- 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.

2.8.1 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. 2.8.2.

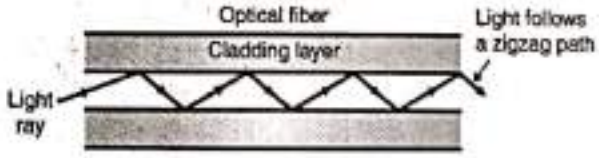


(G-104) **Fig. 2.8.2**

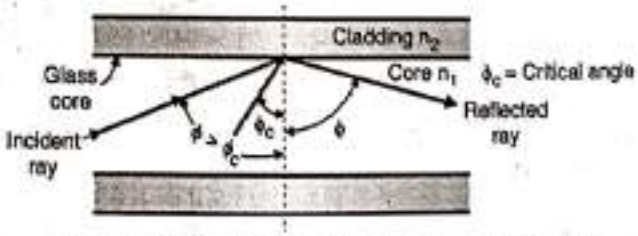
- The two light sources which are used popularly are :
  1. LED (light emitting diode)
  2. Injection laser diode (ILD)
- The LED is cheaper but has a disadvantage that it provides an unfocussed light which hits the core boundaries and gets diffused.
- So LED is preferred only for short distances.
- The laser diode can provide a very focused beam which can be used for a long distance communication.

2.8.2 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. 2.8.3(a).



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



(b) Reflection at the interface of core and cladding

(G-105) **Fig. 2.8.3**

- Fig. 2.8.3(b) illustrates the principle of light travel through the optical fiber.

Scanned by CamScanner

- 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".

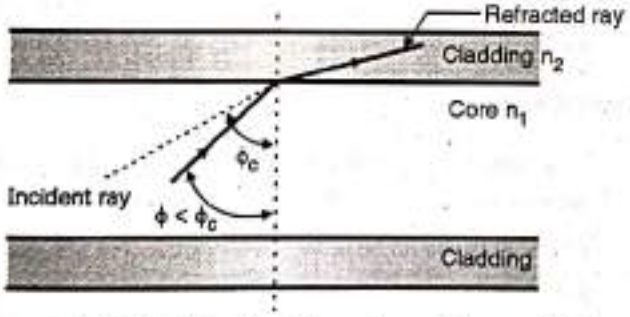
$$\sin \phi_c = \frac{n_2}{n_1}$$

This is as shown in Fig. 2.8.3.

Observations from Fig. 2.8.3(b) :

Some of the important observations from Fig. 2.8.3(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. 2.8.4. The refracted ray enters into the cladding and gets lost.

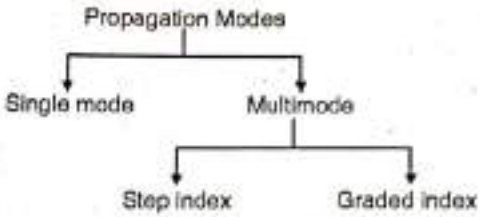


(G-106) Fig. 2.8.4 : Refraction takes place at the core cladding interface if $\phi < \phi_c$

2.8.3 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. 2.8.5.

- 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. 2.8.5 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.



(G-107) Fig. 2.8.5 : Refraction at the interface

- When the incident light ray enters the core of refractive index , it undergoes refraction and makes an angle θ_1 with the dotted line normal to the air-core interface as shown in Fig. 2.8.5. 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,

$$n_0 \sin \theta_0 = n_1 \sin \theta_1 \quad ...(2.8.1)$$

- Therefore the emerging angle θ_1 is given by,

$$\sin \theta_1 = \frac{n_0}{n_1} \sin \theta_0 \quad ...(2.8.2)$$

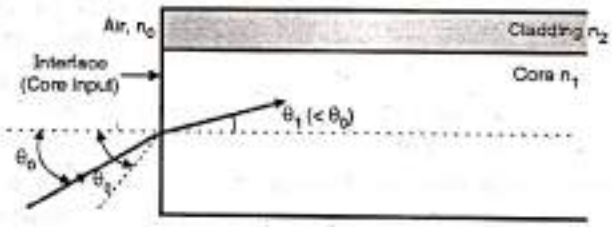
- As $n_0 < n_1$, $\frac{n_0}{n_1} < 1$ therefore the emerging angle will be less than the angle of incidence θ_0.

2.8.4 Modes of Propagation : MU : Dec. 14

University Questions

Q. 1 Explain the modes of propagating light along optical channels. What are the advantages over other guided media ? **(Dec. 14, 10 Marks)**

- The number of paths followed by light rays inside the optical cable is called as modes.
- Fig. 2.8.6 shows different modes of operation of an optical fiber.



(G-108) Fig. 2.8.6 : Propagation modes in optical fibers

- There are two types namely single mode and multimode's 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.

2.8.5 Single Mode Fibers : MU : Dec. 14

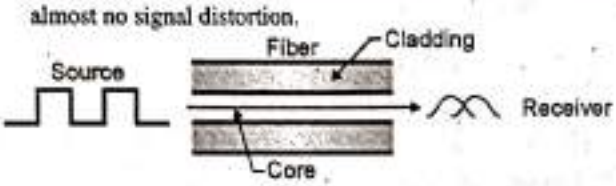
University Questions

Q. 1 Explain the modes of propagating light along optical channels. What are the advantages over other guided media ? **(Dec. 14, 10 Marks)**

- These are called as single mode fibers because they support on one mode of propagation (TE, TM or TEM).

Scanned by CamScanner

- 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. 2.8.7. This beam travel's almost horizontally and follows only one path from source to destination, as shown in Fig. 2.8.7. 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. 2.8.7 : Single mode fiber**

2.8.6 Multimode Fibers : MU : Dec. 14

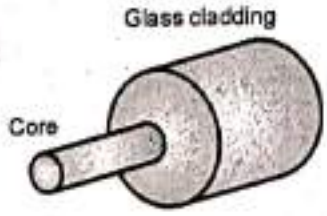
University Questions

Q. 1 Explain the modes of propagating light along optical channels. What are the advantages over other guided media ? **(Dec. 14, 10 Marks)**

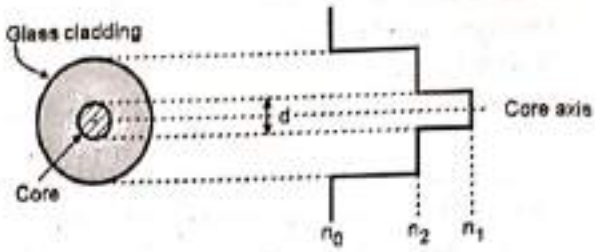
- These are called as multimode fibers because they support simultaneous propagation of many modes and the incident light follows different paths from the source to destination.
- Each mode has its own group velocity and each mode will follow its own path while travelling from the transmitter to receiver.
- 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 :

- The construction of an optical fiber with a core and glass cladding is as shown in Fig. 2.8.8(a).



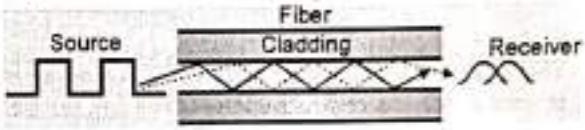
(a) Construction of a glass clad core type fiber



(b) Cross sectional view **(c) Index profile**

(G-110) **Fig. 2.8.8**

- 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. 2.8.8(c).
- Due to the sudden change in refractive index at the boundary of core and cladding, this fiber is called **step index** fiber.
- Fig. 2.8.9 illustrates the propagation of light over a step index fiber.
- Multiple beams will follow different zigzag paths as shown in Fig. 2.8.9. The number of reflections that a beam undergoes depends on the angle of incidence of that beam.

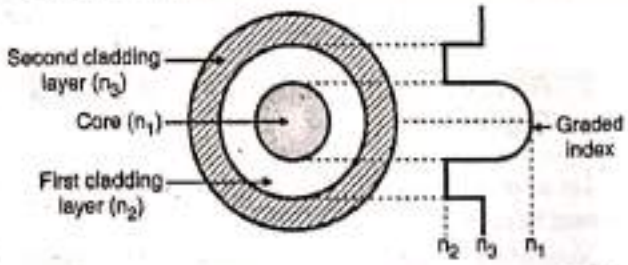


(G-111) **Fig. 2.8.9 : Multimode step index fiber**

- Hence, at the destination, all the beams do not reach simultaneously. This leads to diffusion of signal at the receiver.
- The step index multimode fibers are therefore not used for long distance communications.

Graded index fibers :

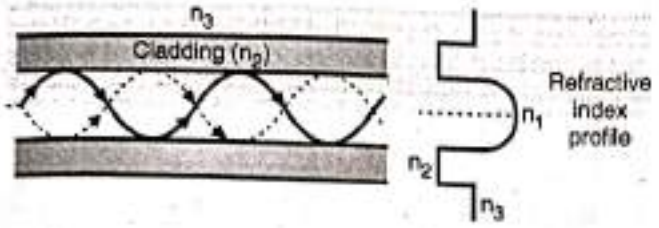
- As shown in Fig. 2.8.10, the refractive index of the fiber core does not remain constant throughout its bulk.
- Instead it is maximum at the center of the core and reduces gradually towards the walls of the core. In order to get this type of index profile the material in the fiber core is modified.



(G-112) **Fig. 2.8.10 : Refractive index profile of a graded index fiber**

- 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. 2.8.11.

Scanned by CamScanner



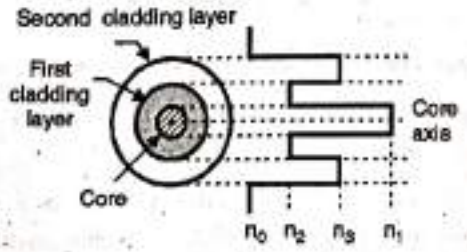
(G-113) **Fig. 2.8.11 : Propagation of light in a graded index fiber**

- 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.

2.8.7 Comparison of Step Index and Graded Index Fibers :

Table 2.8.1 : 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.
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**

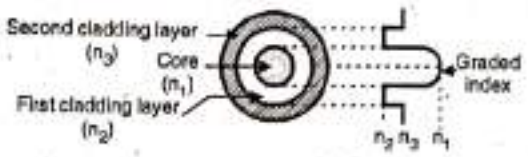


Fig. B

2.8.8 Comparison of Single Mode and Multimode Fibers :

Table 2.8.2 : 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.
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.

2.8.9 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.

Scanned by CamScanner

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 sparks.

2.8.10 Advantages of Optical Fibers :

MU : Dec. 14, Dec. 16, New Syll, : Dec. 18

University Questions

Q. 1 Explain the modes of propagating light along optical channels. What are the advantages over other guided media ? **(Dec. 14, 10 Marks)**

Q. 2 List the advantages of fiber optics as a communication medium. **(Dec. 16, 5 Marks)**

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

1. **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.

2. **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.

3. **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.

4. **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.

2.8.11 Disadvantages of Optical Fiber :

Some of the disadvantages of optical communication system are :

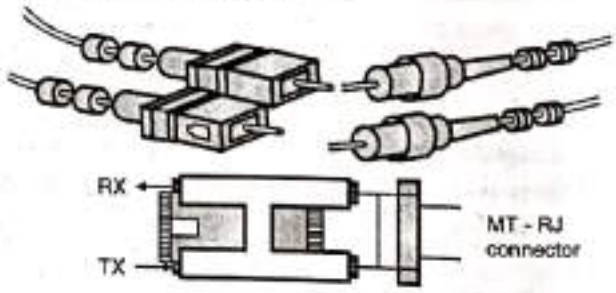
1. Sophisticated plants are required for manufacturing optical fibers.
2. The initial cost incurred is high.
3. Joining the optical fibers is a difficult job.

2.8.12 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).

2.8.13 Fiber Optic Cable Connectors :

- Fiber optic cables use three types of connectors as shown in Fig. 2.8.12. The types are :
  1. Subscriber channel (SC) connector.
  2. Straight tip (ST) connector
  3. MT – RJ connector.



(L-635) **Fig. 2.8.12 : Fiber optic cable connectors**

- The SC connector is used for cable TV. It uses a push/pull locking system.
- The ST connector is used for connecting a cable to networking devices. It uses a bayonet locking system and is more reliable than SC.

Scanned by CamScanner

- MT-RJ is a new connector. It has the same size as RJ 45.

2.8.14 Comparison of Wired Media :

MU : Dec. 06

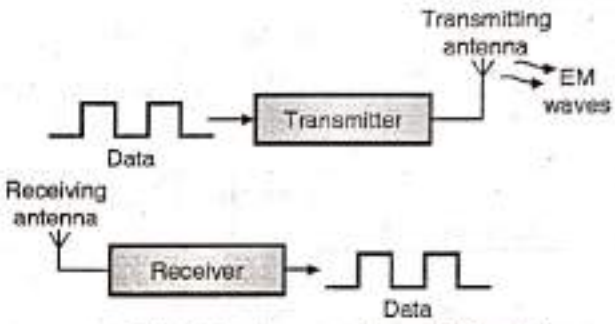
University Questions

Q. 1 Compare the performance characteristics of coaxial, twisted pair and fiber optic transmission media. **(Dec. 06, 10 Marks)**

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 conduction and radiation.	Power loss due to conduction	Power loss 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.

2.9 Unguided (Wireless) Media :

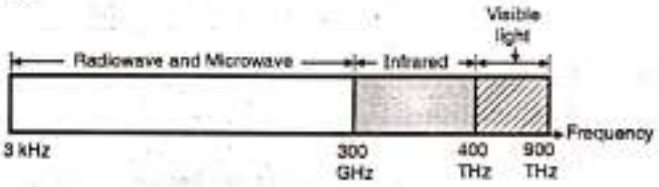
- As already defined, an unguided media (also called as wireless media) does not use a conductor or wire as a communication channel.
- Instead it uses the air or vacuum as medium to carry the information from transmitter to receiver.
- The transmitter first converts the data signal into electromagnetic 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. 2.9.1.



(G-117) **Fig. 2.9.1 : Concept of unguided media**

2.9.1 EM Spectrum for Wireless Media :

The electromagnetic spectrum used for wireless communication is shown in Fig. 2.9.2. The signal from sender to receiver travels in the form of electromagnetic radiation through air.



(L-597) **Fig. 2.9.2 : Electromagnetic spectrum for the wireless communication**

2.9.2 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.

2.9.3 Bands :

The electromagnetic spectrum is divided into several subbands. Table 2.9.1 gives various frequency bands, corresponding type of propagation and application.

Scanned by CamScanner

Table 2.9.1 : 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 μm
12.	Visible light	–	0.4 μm to 0.8 μm

2.9.4 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 2.9.2 gives you the details of entire usable frequency spectrum and its applications.

Table 2.9.2 : 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.

2.9.5 Infrared Signals :

- The EM signals having frequencies above 300 GHz are not referred as radio waves.

Scanned by CamScanner

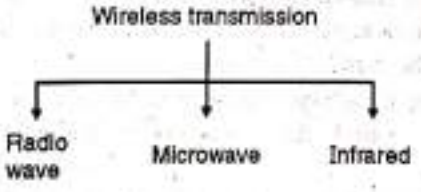
- The signal occupying the range between 0.1 mm and 700 nanometers (nm) are called infrared signals.
- These are used in various special types of communications. Some of them are as follows :
  1. In astronomy to detect stars and other heavenly bodies.
  2. In the guided weapon systems
  3. TV remote control.
  4. Wireless keyboards and mouse.

2.9.6 Visible Light :

- Light is a special type of electromagnetic radiation. It has wavelength in the range of 0.4 to 0.8 μm.
- Light is used for various kinds of communications.
- 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.

2.10 Types of Wireless Media :

- The wireless media is not in the form of an electrical or optical conductor. In most cases the earths atmosphere is used as the physical path to carry data from sender to receiver.
- Wireless media is used when it is not possible to use cable media due to distance or obstructions. There are three main types :
  1. Radiowave 2. Microwave 3. Infrared.

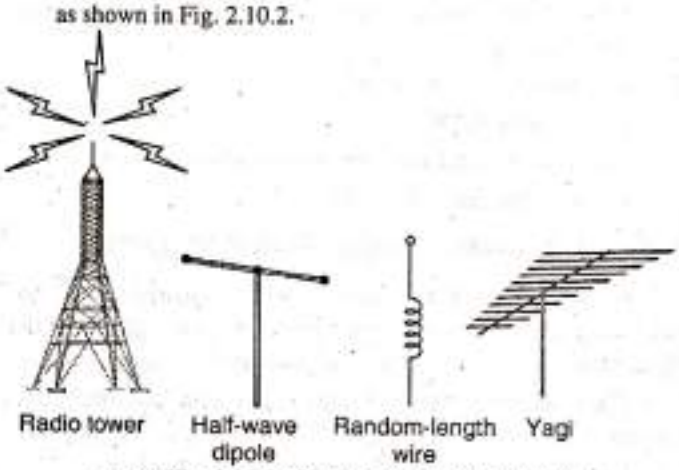


(L-598)Fig. 2.10.1 : Classification of wireless media

2.10.1 Radio Wave Transmission Systems :

- Radio waves have frequencies between 10 kHz and 1 gigahertz. The range of electromagnetic spectrum between 10 kHz and 1 GHz is called radio frequency (RF).

  Radio waves include the following types :
  1. Short wave used in AM radio.
  2. Very High Frequency (VHF) used in FM radio and TV.
  3. Ultra High Frequency (UHF) used in TV.
- The radio frequency bands are regulated and require a license from the regulatory body. Unregulated frequency bands are also present which operate at less than 1 watt transmitted power.
- Radio waves can broadcast omnidirectionally or directionally. Various kinds of antennas are used to broadcast these signals as shown in Fig. 2.10.2.



(L-599) Fig. 2.10.2 : Various types of antennas

- The power of the RF signal is determined by the antenna and transceiver.
- Each range has characteristics that affect its use in computer network. For computer network applications, radio waves fall into three categories :
  1. Low power, single frequency
  2. High power, single frequency
  3. Spread - spectrum.

Characteristics of the three types of radio :

The characteristics of the three types of radio wave are given in Table 2.10.1.

Table 2.10.1

Sr. No.	Factors	Low power single frequency	High power single frequency	Spread spectrum
1.	Frequency range	All radio frequencies	All radio frequencies	All radio frequencies (typically 902 to 928 MHz.)
2.	Bandwidth capacity	1 - 10 Mbps	1 - 10 Mbps	2 - 6 Mbps
3.	Attenuation	High	Low	High
4.	EMI	Poor	Poor	Fair
5.	Installation	Simple	High	Moderate
6.	Cost	Low	Higher	Moderate

- The various areas of applications and the corresponding distances involved are given in Table 2.10.2.

Scanned by CamScanner

Table 2.10.2

Sr. No.	System	Distance
1.	Paging	Tens of kilometres
2.	Cordless telephone	Tens of meters
3.	Cellular phone	Few hundred km
4.	Wireless LAN	100 m

- Some of the important applications of radio transmission systems are :
  1. Cellular communication
  2. Wireless LAN
  3. Point to point and point to multipoint radio systems
  4. Satellite communication

2.10.2 Microwave Transmission System :

It makes use of the lower gigahertz frequencies of the electromagnetic spectrum. These frequencies, are higher than the RF and they produce better throughput and performance.

There are two types of microwave data communication systems :

1. Terrestrial 2. Satellite.

Microwaves :

- Microwaves are basically unidirectional electromagnetic waves with a frequency range from 1 to 300 GHz.
- Microwaves use space wave propagation. The space wave propagation is also called as line of sight communication.
- Due to large bandwidth available it is possible to allot wider subbands. Therefore high data rates can be easily supported using microwave communication.

Terrestrial Microwave Systems :

- These systems use directional parabolic antennas to transmit and receive signals in the lower gigahertz range as shown in Fig. 2.10.3.

(L-600) **Fig. 2.10.3 : Terrestrial microwave system**

- The signals are highly focussed and the physical path must be line of sight.
- Relay towers are used to extend the range. Smaller terrestrial microwave systems can be used even within a building.
- Microwave LANs operate at low power using small transmitters that communicate with omnidirectional hubs. Hubs can then be connected to form an entire network.

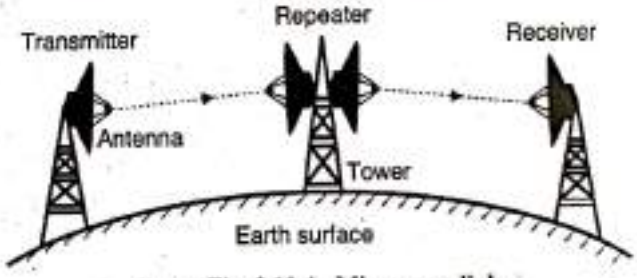
Characteristics of Terrestrial Microwave Systems :

Terrestrial microwave systems have the following characteristics :

1. The frequency range used is from 4 – 6 GHz and 21 to 23 GHz.
2. It supports a bandwidth from 1 to 10 Mbps.
3. Attenuation is dependent on frequency, signal strength, antenna size and atmospheric conditions.
4. The signals are affected by problems such as EMI effect, jamming etc.
5. Line of sight requirements make installation difficult.
6. Short distance systems can be inexpensive but long distance systems are relatively expensive.

RF Link (Microwave Link) :

- Long form of RF link is radio frequency link. This is actually a type of point to point wireless communication.



(L-601) **Fig. 2.10.4 : Microwave link**

- The radio frequencies used for RF links are in microwave range therefore, RF links are also called as microwave links. This is shown in Fig. 2.10.4.
- Although many wire communication systems use copper wires or optical fiber, some system prefer to use air as medium.
- This happens when infrared, lasers, microwaves and radio are used for the transmission of data, as they do not need any physical medium.
- For long distance communication, microwave radio transmission is successfully and popularly used as an alternative to co-axial cable.
- The signal transmission takes place in the form of electromagnetic waves which have wavelengths of few centimeters.
- Parabolic antennas can be mounted on the towers to send a beam of waves to another antenna, tens of kilometres away.
- The transmitting and receiving antennas are highly directional to enable a point to point communication.

Scanned by CamScanner

- This system is widely used for both telephone and television transmission. The higher the tower which holds the antenna, the greater is the range. With a 100 metre high tower, the distances of 100 km can be easily covered.

Advantages of microwave link :

Some of the important advantages are as follows :

1. Installation of towers and associated equipments is cheaper than laying down a cable of 100 km length.
2. Less maintenance as compared to cables.
3. Repeaters can be used. So effect of noise is reduced.
4. No adverse effects such as cable breakage etc.
5. Due to the use of highly directional antenna, these links do not make any interference with other communication systems.
6. Size of transmitter and receiver reduces due to the use of high frequency.

Disadvantages :

1. Signal strength at the receiving antenna reduces due to multipath reception.
2. The transmission will be affected by the thunderstorms, and other atmospheric phenomenons.

Applications of Microwave transmission :

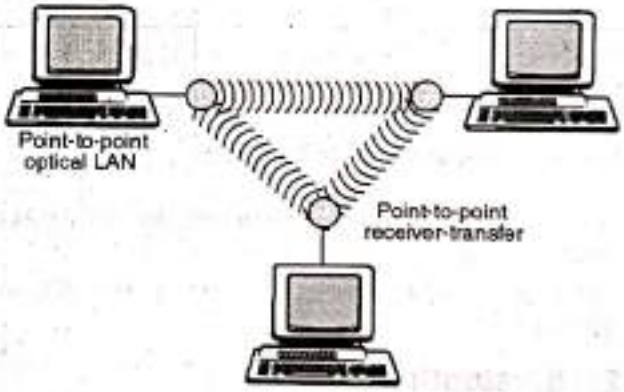
1. One-to-one communication
2. In cellular phones
3. In satellite networks
4. In the wireless LANs

2.11 Use of Infrared Light for Transmission :

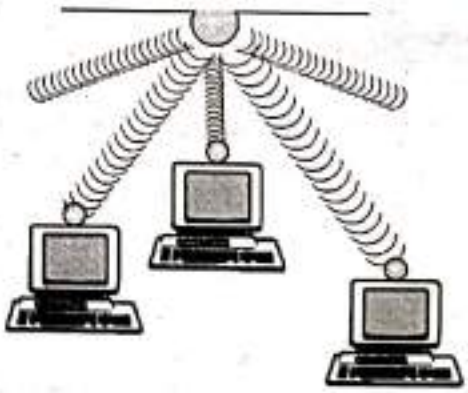
- The electromagnetic waves having frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm) are known as infrared waves.
- IR waves uses line-of sight propagation (space wave propagation).
- Infrared light is a communication medium whose properties are significantly different from those of the radio frequencies.
- A very important property of the infrared light is that it cannot penetrate walls. That means it can be easily contained within a room.
- Due to this property, the infrared light can be used with a much reduced interference. Also the same frequency band can be used in the equipments located in the adjacent rooms as well.
- The wavelength of the infrared light ranges from 850 nm and 900 nm, where the receivers with good sensitivity are available.
- Another advantage of infrared communication is the very large bandwidth which is available for use but has not been exploited to its full extent.
- The major disadvantage is that the sun generates radiation in the infrared band. This can cause a lot of interference with the IR communication.
- The infrared band can be used in development of very high speed wireless LANs in future.

2.11.1 Applications and Standards :

- A number of standards have been developed for an infrared data link (IRDA).
- The IRDA-C standard provides the standards for the bidirectional communications used in cordless devices such as mice, keyboards, joysticks and handheld computers.
- The IRDA-C standard operates at a bit rate of 75 kbits/sec and the distance range is upto 8 meters.
- Another standard called IRDA-D standard operates on the data rates from 115 kb/s to 4 Mb/s, with a distance range upto 1 metre.
- The IR data links can be designed as a wireless alternative to wired connection between computer and printer or keyboard, mouse etc.
- One advantage of infrared is that an FCC license is not required to use it.
- The only disadvantage of infrared signals is that they cannot penetrate walls or other objects and they are diluted by strong light sources.



(a) Point-to-point infrared media in a network



(b) Broadcast infrared media

(L-603) Fig. 2.11.1

Scanned by CamScanner

2.11.2 Comparison of Point to Point and Broadcast Infrared System :

Sr. No.	Factor	Point to Point	Broadcast
1.	Frequency range	100 GHz to 1000 terahertz	100 GHz to 1000 terahertz
2.	Bandwidth capacity	Data rates between 100 kbps to 16 mbps	Data rates less than 1 mbps
3.	Node capacity	2 (source to destination)	More than one
4.	Attenuation	Depends on quality of emitted light, its purity, atmospheric conditions and signal obstructions	Depends on quality of emitted light, its purity atmospheric conditions
5.	EMI	Affected by intense light	Affected by intense light
6.	Installation	Requires precise alignment	Fairly simple
7.	Cost	Moderately high if laser is used	High if laser is used.

2.11.3 Applications of Infrared :

1. Very high data rates can be supported, due to very high bandwidth (approximately 400 THz).
2. For communication between keyboard, mouse PCs and printers.

2.12 Bluetooth :

MU : Dec. 05, Dec. 06, May 07, May 08, Dec. 08, Dec. 10, May 11, Dec. 12, May 13

University Questions

Q. 1 Write short notes on : Bluetooth. **(Dec. 05, Dec. 06, May 11, May 13, 10 Marks)**

Q. 2 List blue tooth feature and explain network formation process. **(May 07, May 08, Dec. 08, Dec. 12, 10 Marks)**

Q. 3 Write short notes on : Bluetooth architecture. **(Dec. 10, 5 Marks)**

- Bluetooth is the name given to a new technology using short-range radio links, which could replace the cable(s) connecting portable and/or fixed electronic devices.
- Bluetooth replaces cables that connect one device to another with one universal radio link.
- Its key features are robustness, low complexity, low power and low cost.
- Designed to operate in noisy frequency environments, the Bluetooth radio uses a fast acknowledgement and frequency-hopping scheme to make the link more reliable.
- 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 which can connect devices such as telephones, computers, printers, cameras, etc. without using wires.
- A Bluetooth LAN is an Ad hoc network i.e. it does not use a base station. It is possible to connect the Bluetooth LAN to the Internet.
- This technology is implemented using the IEEE 802.15 standard.

2.12.1 Architecture : MU : Dec. 11, Dec. 13, May 17

University Questions

Q. 1 Write short notes on : Bluetooth architecture. **(Dec. 11, 7 Marks)**

Q. 2 Draw and explain the architecture and protocol stack of Bluetooth. **(Dec. 13, 10 Marks)**

Q. 3 Write short notes on : Bluetooth architecture. **(May 17, 10 Marks)**

1. Piconets and 2. Scatternets.

2.12.2 Piconets : MU : Dec. 13, May 17

University Questions

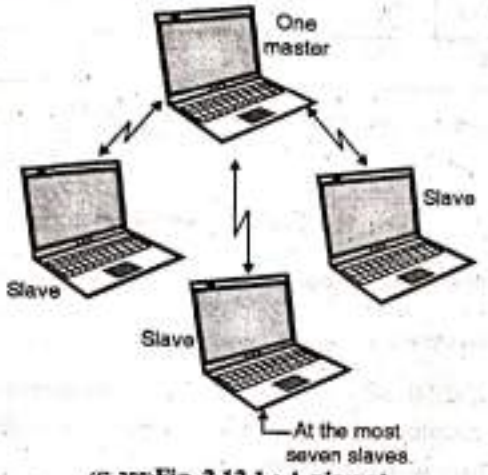
Q. 1 Draw and explain the architecture and protocol stack of Bluetooth. **(Dec. 13, 10 Marks)**

Q. 2 Write short notes on : Bluetooth architecture. **(May 17, 10 Marks)**

- 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. 2.12.1 shows a piconet. A master can also be called as a primary station and slaves are secondary station.

Scanned by CamScanner

- 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.



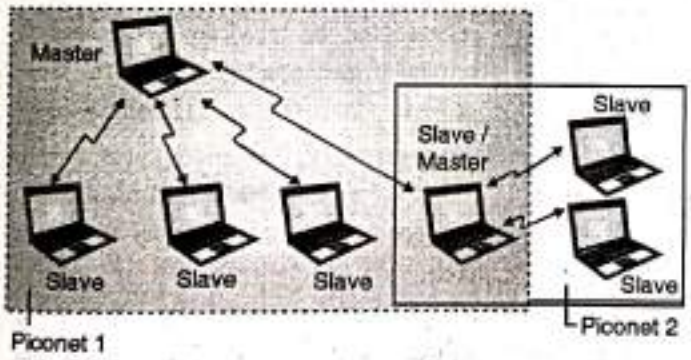
(G-388)**Fig. 2.12.1 : A piconet**

2.12.3 Scatternet : MU : May 17

University Questions

Q. 1 Write short notes on : Bluetooth architecture. **(May 17, 10 Marks)**

- A scatternet is obtained by combining piconets as shown in Fig. 2.12.2.



(G-389) **Fig. 2.12.2 : Scatternet**

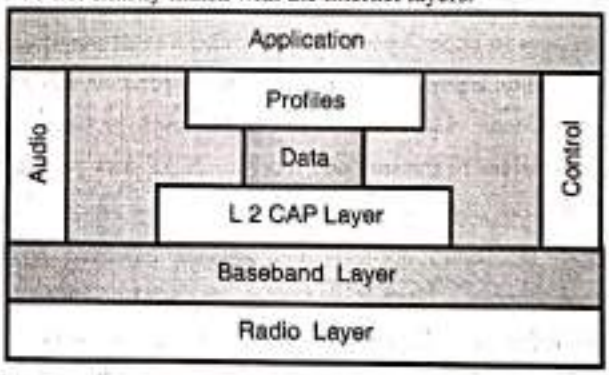
- Fig. 2.12.2 shows a scatternet consisting of two piconets. A slave in the first piconet can act as a master in the second piconet.
- It will receive the messages from the master in the first piconet by acting as a slave and then delivers the message to the slaves in the second piconet as shown in Fig. 2.12.2. So the same device acts as a slave in the first piconet and as master in the second piconet.

2.12.4 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.

2.12.5 Bluetooth Layers (Bluetooth Protocol Architecture) :

- The layers of Bluetooth are as shown in Fig. 2.12.3 and they do not exactly match with the internet layers.



(G-390)**Fig. 2.12.3 : Bluetooth layers**

1. Radio :

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.

2. Baseband :

- The baseband is the physical layer of the Bluetooth. It manages physical channels and links. In addition to that the other services like error correction, data whitening,

Scanned by CamScanner

hop selection and Bluetooth security etc. also are handled by this layer.

- The baseband layer lies 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 for carrying out link level routines like link connection and power control.
- Some other functions managed by the baseband layer are :
- To manage asynchronous and synchronous links, handles packets and carry out paging and inquiry to access and inquire Bluetooth devices in the area.
- The baseband transceiver applies a Time-Division Duplex (TDD) scheme. (i.e. transmits and receives alternately).
- Therefore apart from different hopping frequency (frequency division), the time is also slotted.

2.12.6 TDMA :

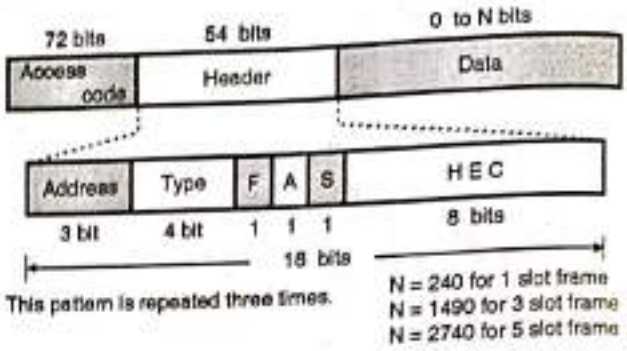
Bluetooth uses a form of TDMA that is called TDD-TDMA (Time Division Duplex-TDMA).

2.12.7 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.

2.12.8 Frame Format :

- A frame in the baseband layer can be one of the three types :
  1. One slot
  2. Three slot
  3. Five slot.
- The frame format of the three frame types is shown in Fig. 2.12.4.



(G-391) **Fig. 2.12.4 : Frame format**

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. 2.12.4).
- 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 can not 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.

2.12.9 Data (Payload) Field :

This field contains the data or control bits. It can be 0 to 2740 bits long. It contains data or control bits coming from the upper layers.

Scanned by CamScanner

2.12.10 Security Limitations In Bluetooth :

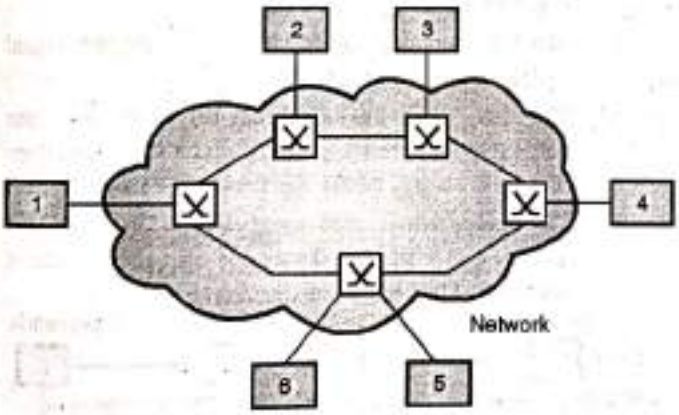
- Due to its wireless nature, experts express a security concern with Bluetooth.
- The issue can be addressed with three aspects: specific sequence of channel hopping known only to the sending and receiving devices, challenge-response authentication routine to verify the validity of the receiving unit, and the 128-bit key encryption standard for securing transmission between devices.

2.12.11 Bluetooth Advantages :

1. 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.
2. 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.

2.13 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 cannot be used.

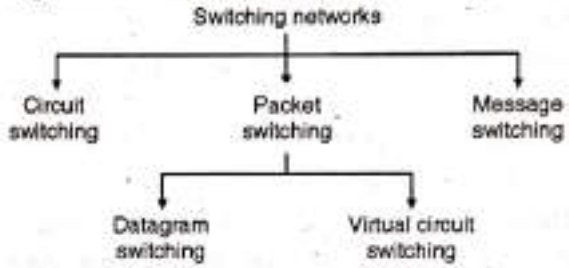


(L-616) **Fig. 2.13.1 : Switched network**

- 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. 2.13.1 shows a switched network.

2.13.1 Switching Methods :

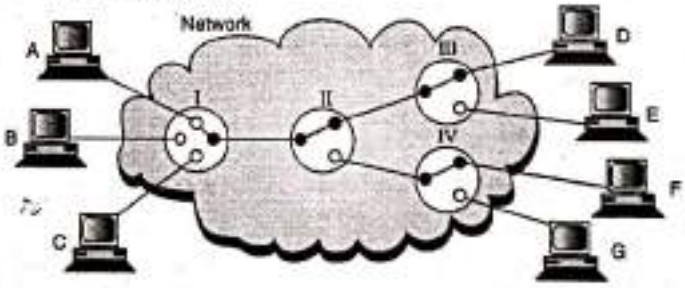
- The three basic methods of switching are :
  1. Circuit switching 2. Packet switching
  3. Message switching
- Out of these, the circuit and packet switching are commonly used today but the message switching has been phased out in general communication but is still used in the networking applications.
- Fig. 2.13.2 shows the classification of switching methods.



(L-617) **Fig. 2.13.2 : Classification of switching methods**

2.14 Circuit Switching Networks :

- 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 cannot 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.



(L-618) **Fig. 2.14.1 : Circuit-switched 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.
- 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

Scanned by CamScanner

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. 2.14.1.
- 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. 2.14.1, 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).

2.14.1 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. 2.14.1, 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) :

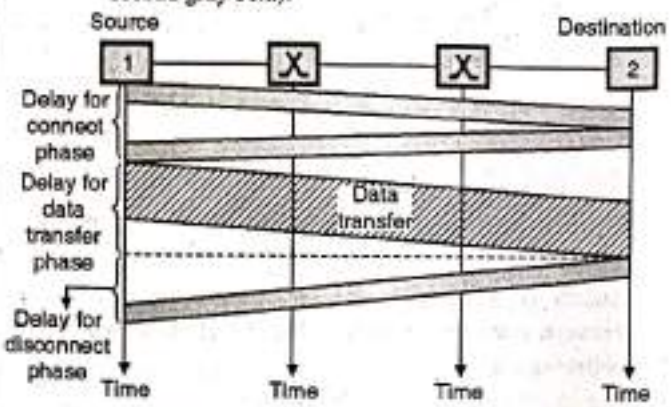
- After some time the connection between two users is terminated usually by the action of one or two stations.
- Circuit switching is inefficient in most of the applications.
- The entire channel capacity is dedicated for the duration of connection, even if the data is not being transferred.
- Once the circuit is established, the network is effectively transparent to the users with no delays involved.

2.14.2 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.

2.14.3 Delay :

- Eventhough the efficiency is low, the delay in this type of networks is very small.
- Fig. 2.14.2 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 :
  1. The propagation time related to the request message of the source computer (slope of the first gray box in Fig. 2.14.2).
  2. The time required for the transfer of request signal (height of the first gray box in Fig. 2.14.2).
  3. The time taken by the acknowledgement from the destination computer to propagate back to source (slope of the second gray box in Fig. 2.14.2).
  4. The propagation time required to transfer the acknowledgement from destination computer (height of second gray box.).



(L-619) Fig. 2.14.2 : Delay in circuit switching

Scanned by CamScanner

- 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. 2.14.2 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.

2.14.4 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.

2.14.5 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.

2.14.6 Circuit Switched Technology in Telephone Networks :

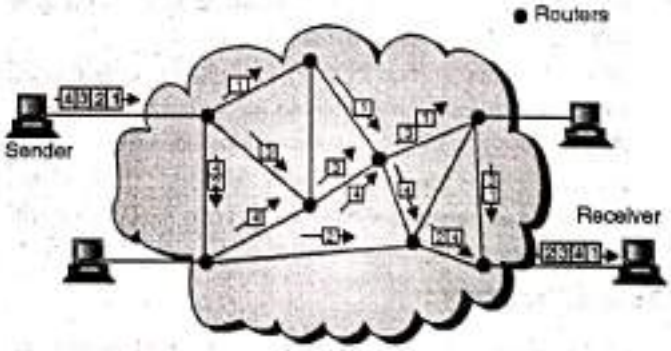
- The telephone companies previously used the circuit switching technology for switching and routing a call. This was a physical layer technology.
- However, today the tendency is to use other switching techniques. For example the telephone number is used as the global address and a signalling system (called SS7) is used for creating and disconnecting the connections.

2.15 Packet Switching :

- In packet switching, messages are broken up into packets. Each packets 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 :
  1. Bandwidth is reduced due to splitting data onto different routes in a busy circuit.
  2. 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 :
  1. Datagram packet switching
  2. Virtual circuit packet switching.

2.15.1 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 instructors.
- 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 packet are called as **datagrams.**
- Datagram packet switching is shown in Fig. 2.15.1.



(L-623) **Fig. 2.15.1 : Datagram packet switching**

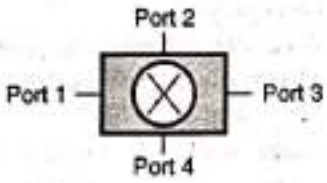
- In this circuit, four packets are to be delivered from the sender to receiver. The switches in the datagram network are called as **routers.**
- All the four packets (datagrams) belong to the same message in this circuit however actually they can get originated from any computer.
- The four datagrams, as shown in Fig. 2.15.1 may travel different paths to reach the destination. Due to this the packets may arrive out of order at the destination.

Scanned by CamScanner

- The delay associated with each packet will be different as a result of the different paths followed by them. The datagrams may get lost of 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.

2.15.2 Routing Table :

- In packet switched networks, each packet switch has a routing table. This table contains the destination address.
- The routing tables are is dynamic and their information is updated on periodic basis. The routing table consists of destination address and the corresponding output part over which the packet is to be forwarded as shown in Fig. 2.15.2.



Destination address	Output port
1323	1
4360	2
9140	3
6436	4

(L-624) **Fig. 2.15.2 : Router and Routing table**

Destination Address :

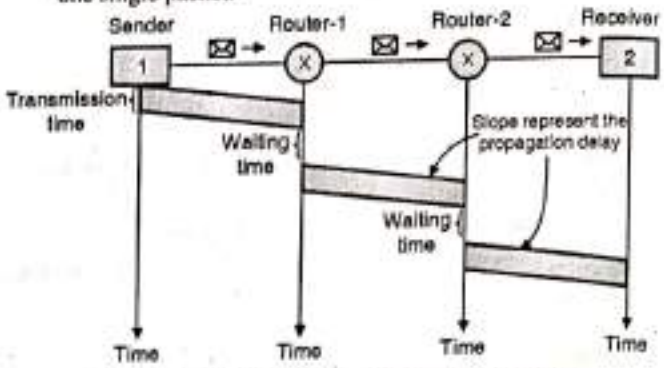
- Every packet in the datagram network consists of a header that contains the destination address where the packet is to be delivered and some additional information.
- When the router receives a packet, it examines the destination address of the packet and refers to its routing table to decide the port through which the packet is to be forwarded.
- For example in the routing table of Fig. 2.15.2, if the destination address on the received packet is 4360 then it will be forwarded through port 2.

2.15.3 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.

2.15.4 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.
- All the packets in a message take different paths. Hence the delay associated with each packet is different.
- Fig. 2.15.3 illustrates the delays in a datagram network for one single packet.



(L-625) **Fig. 2.15.3 : Delay in datagram network**

- In Fig. 2.15.3, 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. 2.15.3 and the two waiting times w_1 and w_2.

$$\therefore \text{ Total delay } = 3T + 3\tau + w_1 + w_2 \qquad \ldots(2.15.1)$$

- The datagram switching is used in Internet.

2.15.5 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 become 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 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.

Scanned by CamScanner

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.

2.15.6 Disadvantages of Packet Switching :

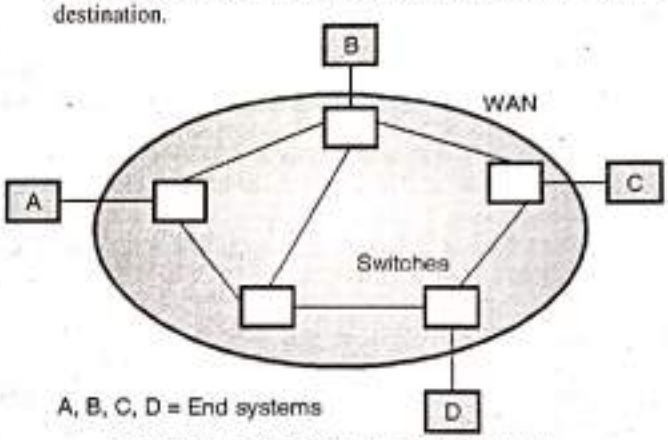
1. Increased delay due to following reasons :
   (a) Transmission delay = length of packet divided by incoming channel rate.
   (b) Variable delay due to processing and queuing.
2. The amount of overall packet delay can vary substantially (jitter) due to the following reasons :
   (a) Packets may vary 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.

2.15.7 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.

2.16 Virtual Circuit Packet Switching :

- 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. 2.16.1 shows the virtual circuit network. The network consists of switches which route the traffic from source to destination.



(L-626) **Fig. 2.16.1 : Virtual circuit network**

2.16.1 Addressing :

The virtual circuit networks use two types of addressing :

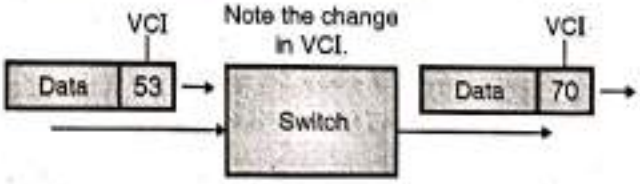
1. Global addressing
2. Local addressing (Virtual circuit Identifiers).

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. 2.16.2 but when the frame leaves that switch it contains another VCI (70 as shown).



(L-627) **Fig. 2.16.2 : VCI**

Scanned by CamScanner

2.16.2 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.

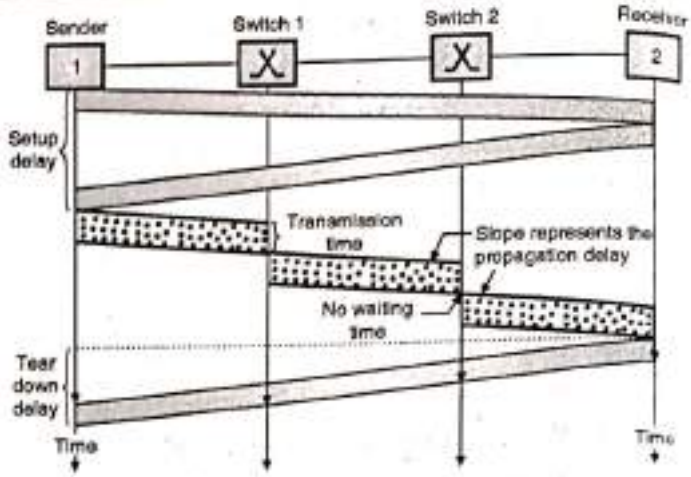
2.16.3 Efficiency :

- 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 effect. This increases the efficiency of the virtual circuit network.

2.16.4 Delay :

- Different delays in virtual circuit networks are illustrated in Fig. 2.16.3.
- 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. 2.16.3, 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.

$$\therefore \text{ Total delay} = 3T + 3\tau + \text{Set up phase delay} + \text{Tear down delay}$$



(L-632) **Fig. 2.16.3 : Delays in virtual circuits**

2.16.5 Circuit Switched Technology in WANs :

The virtual circuit networks are used in switched WANs such as Frame Relay and ATM networks.

2.16.6 Advantages of Virtual Circuit Packet Switching :

1. Virtual circuit packet switching uses abbreviated headers and hardware based table lookup, which allows fast processing and forwarding of packets.
2. In the virtual circuit packet switching, resources can be allocated during connection setup.
3. 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.
4. 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.
5. The efficiency of virtual circuit packet switching is high.

2.16.7 Disadvantages of Virtual Circuit Packet Switching :

1. 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.
2. In the case of fault occurs in the network, all affected connections must be set up again.
3. Connection setup is not possible, if the switch is unable to handle the volume of traffic allowed or link utilization exceeds certain thresholds.

Scanned by CamScanner

2.16.8 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
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

2.17 Comparison of Circuit and Packet Switching : MU : May 17

University Questions

Q. 1 Compare and contrast a circuit switching and a packet switching network. **(May 17, 5 Marks)**

Parameter	Circuit switching	Packet switching
Application	Telephone network for bi-directional, real time transfer of voice signals.	Internet for datagram and reliable stream service between computers.
End terminal	Telephone, modem.	Computer
Information type	Analog voice or PCM digital voice	Binary information
Transmission system	Analog and digital data over different transmission media	Digital data over different transmission media.
Addressing scheme	Hierarchical numbering plan	Hierarchical address space
Routing scheme	Route selected during call setup.	Each packet is routed independently.
Multiplexing scheme	Circuit multiplexing.	Packet multiplexing shared media access networks.

Review Questions

Q. 1 Name the layer which is associated with the transmission media.

Q. 2 Explain the classification of transmission media.

Q. 3 What is the difference between guided and unguided transmission media ?

Q. 4 State the types of guided media.

Q. 5 Explain the difference between UTP and STP.

Q. 6 What is the effect of twisting the wires in UTP cables ?

Q. 7 Give applications of co-axial cable.

Q. 8 State and explain the duties of physical layer.

Q. 9 What is the advantage of using shielding ?

Q. 10 Compare the guided transmission media.

Q. 11 State advantages of optical fiber cable.

Q. 12 State the three ways of wireless transmission.

Q. 13 Write a note on microwave communication.

Q. 14 State the applications of microwave communication.

Q. 15 Write a note on : Infrared transmission.

Q. 16 State applications of infrared transmission.

Q. 17 Compare twisted pair (UTP and STP).

Q. 18 Compare twisted pair, co-axial and fiber optic cable.

Q. 19 Which are the two types of microwave transmission systems ?

Q. 20 What are the characteristics of a terrestrial microwave system ?

Scanned by CamScanner

Q. 21 Compare point to point and broadcast infrared transmission system.

Q. 22 State and discuss various types of connectors.

Q. 23 _____ is the name given to a new technology using short-range radio links, intended to replace the cable(s) connecting portable and/or fixed electronic devices.

Ans. : Bluetooth.

Q. 24 A bluetooth network is called as a _____ or a small net.

Ans. : piconet

Q. 25 Every Bluetooth device consists of a built in short range _____.

Ans. : radio transmitter.

Q. 26 Each Bluetooth-enabled device contains a 1.5 - inch square transceiver chip operating in the ISM (industrial, scientific, and medical) radio frequency band of _____ GHz to _____ GHz.

Ans. : 2.40, 2.48.

Q. 27 The _____ is the physical layer of the Bluetooth.

Ans. : Baseband.

Q. 28 The baseband transceiver applies a _____ scheme.

Ans. : Time-Division Duplex (TDD).

Q. 29 The Logical Link Control and Adaptation Layer Protocol (L2CAP) is layered over the _____ protocol and resides in the data link layer.

Ans. : baseband.

Q. 30 Bluetooth hop frequency is _____ hops/second.

Ans. : 1600.

Q. 31 IEEE 802.11x hop frequency is _____ hops/second

Ans. : 2.5.

Q. 32 Bluetooth uses _____ modulation technique.

Ans. : GFSK (Gaussian Frequency Shift Keying)

Q. 33 What is switching ?

Q. 34 Explain the concept of circuit switching.

Q. 35 State advantages and drawback of circuit switching

Q. 36 Explain the concept of packet switching.

Q. 37 State merits and demerits of packet switching.

Q. 38 Compare circuit and packet switching.

2.18 University Questions and Answers (New Syllabus) :

Dec. 2018 [Total Marks : 04]

Q. 1 List the advantages of fiber optics as a communication medium. **(Section 2.8.10) (4 Marks)**

□□□

Scanned by CamScanner

CHAPTER 3

Module 3

Data Link Layer

Syllabus :

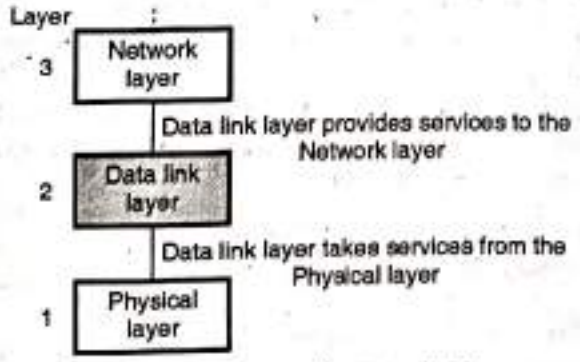
DLL design issues (Services, Framing, Error control, flow control) Error detection and correction (Hamming code, CRC, Checksum), Elementary data link layer protocols, Stop and wait, Sliding window (Go back-N, Selective repeat), HDLC.

3.1 Introduction :

- The physical layer deals with the transmission of signals over different transmission medias.
- A reliable and efficient communication between two adjacent machines can be achieved via the data link layer.
- This layer basically deals with frame formation, flow control, error control, addressing and link management.
- While sending data from source to destination errors may get introduced. The data communication circuits have only a finite data rate and there is non-zero propagation delay between the instant a bit is sent and the instant at which it is received.
- These limitations affect the efficiency of data transfer. The data link layer protocols used for communication take care of all these problems.
- Data link layer is the second layer in OSI reference model. It is above the physical layer.

3.1.1 Position of Data Link Layer :

- Fig. 3.1.1 shows the position of data link layer in the five layer Internet model. It is the second layer.



(L-663)**Fig. 3.1.1 : Position of data link layer**

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

3.2 Data Link Layer Design Issues (Functions of Data Link Layer) :

MU : Dec. 06, Dec. 07, May 10, May 11, May 16, May 17

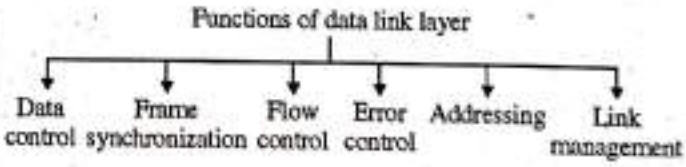
University Questions

Q. 1 Describe any five functions of data link layer with suitable examples. **(Dec. 06, Dec. 07, May 10, May 11, 10 Marks)**

Q. 2 Explain any four functions of data link layer with example. **(May 16, 10 Marks)**

Q. 3 Enumerate the main responsibilities of the data link layer. **(May 17, 5 Marks)**

- The data link layer is supposed to carry out many specified functions.
- For effective data communication between two directly (physically) connected transmitting and receiving stations the data link layer has to carry out a number of specific functions as follows :



(L-664)**Fig. 3.2.1 : 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

Scanned by CamScanner

each frame should be identified so that the frames can be recognized by the destination machine.

3. **Flow control :**

The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4. **Error control :**

The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

5. **Addressing :**

When many machines are connected together (LAN), the identity of the individual machines must be specified while transmitting the data frames. This is known as addressing.

6. **Control and data on same link :**

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

7. **Link management :**

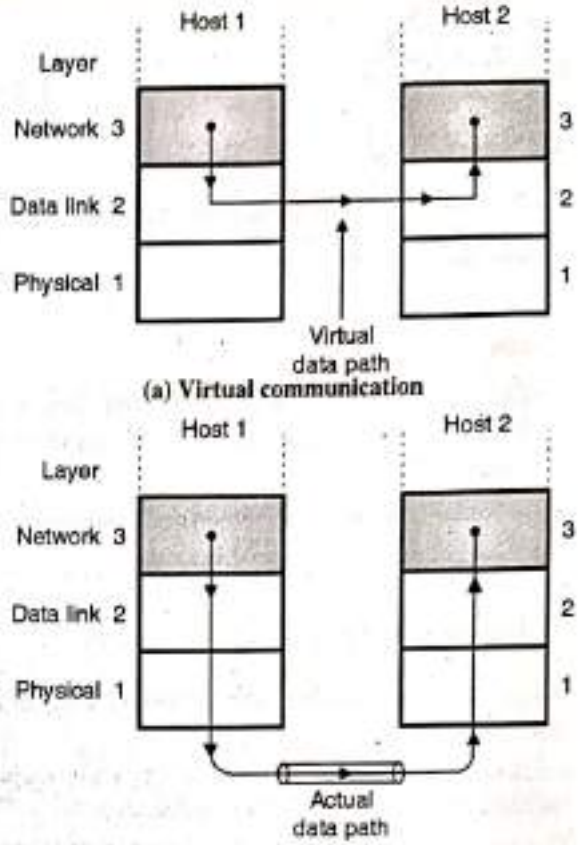
The communication link between the source and destination is required to be initiated, maintained and finally terminated for effective exchange of data. It requires co-ordination and co-operation among all the involved stations. Protocols or procedures are required to be designed for the link management.

3.3 Services Provided to Network Layer : MU : May 16

University Questions

Q. 1 Explain any four functions of data link layer with example. **(May 16, 10 Marks)**

- 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. 3.3.1(a). It is not the actual path.
- The actual path followed by the data from sending machine to destination is shown in Fig. 3.3.1(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. 3.3.1(a)) using a data link layer protocol.



(a) Virtual communication

(b) Actual data path

(L-665)Fig. 3.3.1

3.3.1 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.

3.3.2 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.

3.3.3 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.

Scanned by CamScanner

- 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.

3.3.4 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.

3.4 Framing :

MU : Dec. 09, Dec. 11, Dec. 14, May 16

University Questions

Q. 1 Explain framing, flow and error control in data link layer. **(Dec. 09, Dec. 11, 10 Marks)**

Q. 2 Why there is a need for framing ? **(Dec. 14, 10 Marks)**

The following encoding is used in a data link protocol :

A : 01000111; B :11100011; FLAG : 01111110; ESC:11100000

Show the bit sequence transmitted (in binary) for the four character frame :

A B ESC FLAG

When each of the following framing methods are used :

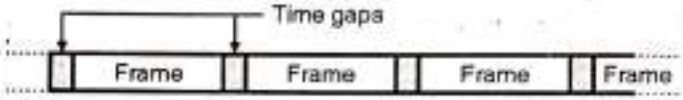
(a) Character count

(b) Flag bytes and byte stuffing

(c) Starting and ending flag bytes, with bit stuffing

Q. 3 Explain any four functions of data link layer with example. **(May 16, 10 Marks)**

- 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 there, 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. 3.4.1.



(G-178) **Fig. 3.4.1 : Framing**

- 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.

3.4.1 Framing Methods :

MU : Dec. 10, May 11, May 13, May 15, May 16, Dec. 17, New Syll. : Dec. 18

University Questions

Q. 1 Explain the different framing methods. **(Dec. 10, May 11, 5 Marks)**

Q. 2 Explain different framing methods. What are the advantages at variable length frames over fixed length frames ? **(May 13, 10 Marks)**

Q. 3 Explain in short different framing methods. **(May 15, May 16, 4 Marks)**

Q. 4 Explain in short different framing methods. **(Dec. 17, 5 Marks)**

- 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.

3.4.2 Character Count :

MU : Dec. 10, May 11, May 13, Dec. 14, May 15, May 16, Dec. 17, New Syll. : Dec. 18

University Questions

Q. 1 Explain the different framing methods. **(Dec. 10, May 11, 5 Marks)**

Q. 2 Explain different framing methods. What are the advantages at variable length frames over fixed length frames ? **(May 13, 10 Marks)**

Q. 3 Why there is a need for framing ? **(Dec. 14, 10 Marks)**

Scanned by CamScanner

The following encoding is used in a data link protocol :

A : 01000111; B :11100011; FLAG : 01111110; ESC:11100000

Show the bit sequence transmitted (in binary) for the four character frame :

A B ESC FLAG

When each of the following framing methods are used :

(a) Character count

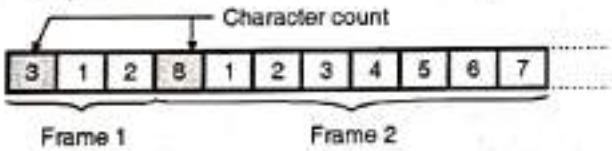
(b) Flag bytes and byte stuffing

(c) Starting and ending flag bytes, with bit stuffing

Q. 4 Explain in short different framing methods. **(May 15, May 16, 4 Marks)**

Q. 5 Explain in short different framing methods. **(Dec. 17, 5 Marks)**

- In this method, a field in the header is used to specify the number of characters in the frame.
- This number helps the receiver to know the exact number of characters present in the frame following this count.
- The character count method is illustrated in Fig. 3.4.2.



(L-668)**Fig. 3.4.2 : Character count method**

- The two frames shown in Fig. 3.4.2 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.

3.4.3 Starting and Ending Character with Character Stuffing :

MU : Dec. 10, May 11, May 13, May 15, May 16, Dec. 17, New Syll. : Dec. 18

University Questions

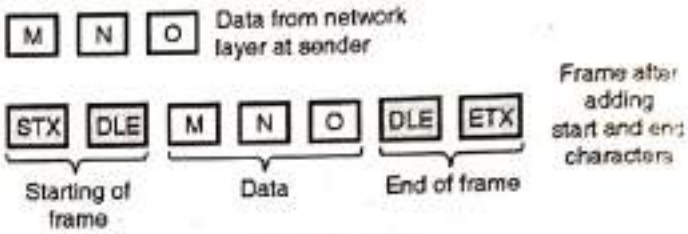
Q. 1 Explain the different framing methods. **(Dec. 10, May 11, 5 Marks)**

Q. 2 Explain different framing methods. What are the advantages at variable length frames over fixed length frames ? **(May 13, 10 Marks)**

Q. 3 Explain in short different framing methods. **(May 15, May 16, 4 Marks)**

Q. 4 Explain in short different framing methods. **(Dec. 17, 5 Marks)**

- 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. 3.4.3.



(L-669)**Fig. 3.4.3**

3.4.4 Character Stuffing :

MU : Dec. 10, May 11, May 13, Dec. 14, May 15, Dec. 17, New Syll. : Dec. 18

University Questions

Q. 1 Explain the different framing methods. **(Dec. 10, May 11, Dec. 17, 5 Marks)**

Q. 2 Explain different framing methods. What are the advantages at variable length frames over fixed length frames ? **(May 13, 10 Marks)**

Q. 3 Why there is a need for framing ? **(Dec. 14, 10 Marks)**

The following encoding is used in a data link protocol :

A : 01000111; B :11100011; FLAG : 01111110; ESC:11100000

Show the bit sequence transmitted (in binary) for the four character frame :

A B ESC FLAG

When each of the following framing methods are used :

(a) Character count

(b) Flag bytes and byte stuffing

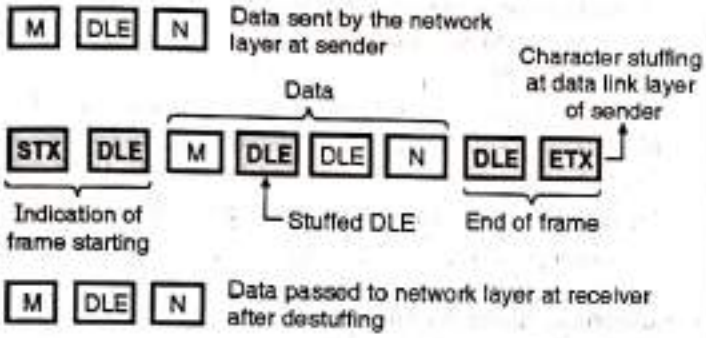
(c) Starting and ending flag bytes, with bit stuffing

Q. 4 Explain in short different framing methods. **(May 15, 4 Marks)**

- The problem 0with this system is that the characters DLE STX or DLE ETX can be a part of data as well.

Scanned by CamScanner

- 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.



(G-181) **Fig. 3.4.4 : Character stuffing**

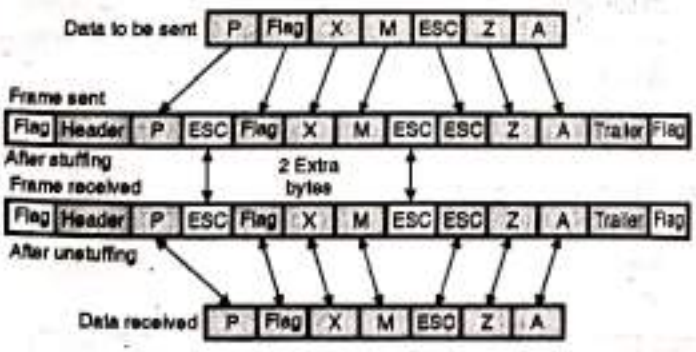
- Thus the DLE STX or DLE ETX used for framing purpose can be distinguished from the one in data because DLEs in the data always appear more than once.
- This is called character stuffing and it is shown in Fig. 3.4.4. Note that at the receiving end the destuffing is essential. Destuffing process is 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.

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. 3.4.5 demonstrates the concept of byte stuffing.



(G-182) **Fig. 3.4.5 : Byte-stuffing**

- Byte stuffing by the escape character will allow the presence of the flag is 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. 3.4.5.

3.4.5 Starting and Ending Flags, with Bit Stuffing :

MU : Dec. 10, May 11, May 13, Dec. 14, May 15, May 16, Dec. 17, New Syll. : Dec. 18

University Questions

Q. 1 Explain the different framing methods. **(Dec. 10, May 11, 5 Marks)**

Q. 2 Explain different framing methods. What are the advantages at variable length frames over fixed length frames ? **(May 13, 10 Marks)**

Q. 3 Why there is a need for framing ? **(Dec. 14, 10 Marks)**

The following encoding is used in a data link protocol :

A : 01000111; B :11100011; FLAG : 01111110; ESC:11100000

Show the bit sequence transmitted (in binary) for the four character frame :

A B ESC FLAG

When each of the following framing methods are used :

(a) Character count

(b) Flag bytes and byte stuffing

(c) Starting and ending flag bytes, with bit stuffing

Q. 4 Explain in short different framing methods. **(May 15, May 16, 4 Marks)**

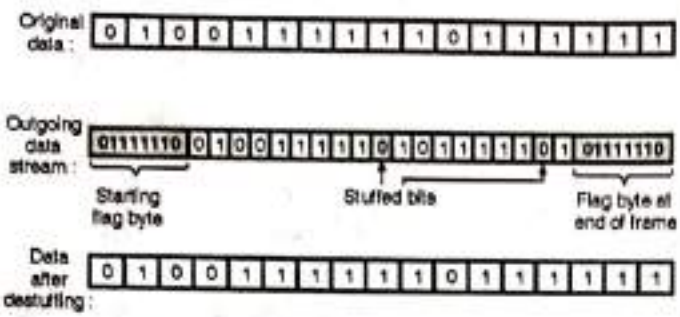
Q. 5 Explain in short different framing methods. **(Dec. 17, 5 Marks)**

- 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. 3.4.6.

Scanned by CamScanner



(G-183) **Fig. 3.4.6 : Bit stuffing and destuffing**

- 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. 3.4.6.
- Due to bit stuffing, the possible problem if the data contains the flag byte pattern (0111 1110) is eliminated.

3.4.6 Physical Layer Coding Violations :

MU : Dec. 10, May 11, May 13, May 16, Dec. 17

University Questions

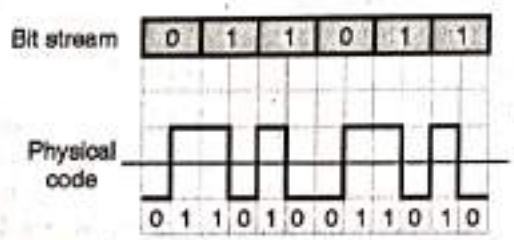
Q. 1 Explain the different framing methods. **(Dec. 10, May 11, 5 Marks)**

Q. 2 Explain different framing methods. What are the advantages at variable length frames over fixed length frames ? **(May 13, 10 Marks)**

Q. 3 Explain in short different framing methods. **(May 16, 4 Marks)**

Q. 4 Explain in short different framing methods. **(Dec. 17, 5 Marks)**

- 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. 3.4.7. 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. 3.4.7. 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. 3.4.7**

Which method of framing is used practically ?

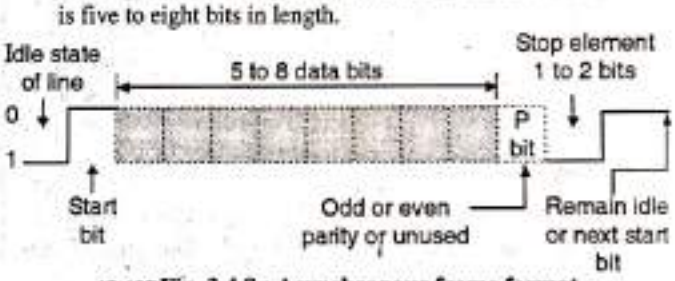
- Many data link protocols use the combination of the character count technique with one of the other techniques so as to have an extra safety.

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. 3.4.8. 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.

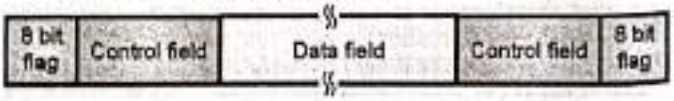


(G-185) **Fig. 3.4.8 : Asynchronous frame format**

- 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. 3.4.9.



(G-186) **Fig. 3.4.9 : Synchronous frame format**

Scanned by CamScanner

- 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.
- As shown in the Fig. 3.4.9, 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.

3.5 Error Control :

MU : Dec. 09, Dec. 11, May 16

University Questions

Q. 1 Explain framing, flow and error control in data link layer. **(Dec. 09, Dec. 11, 10 Marks)**

Q. 2 Explain any four functions of data link layer with example. **(May 16, 10 Marks)**

- 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.

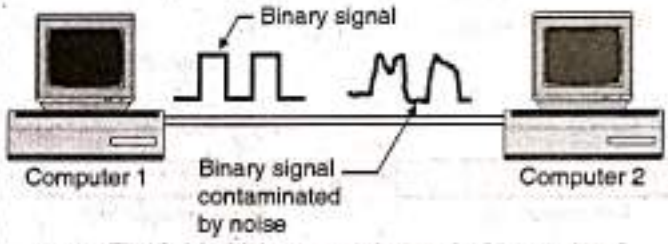
3.5.1 Function of a Timer :

New Syll. : MU : Dec. 18

- 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.

3.6 Error Detection and Correction :

- When transmission of digital signals takes place between two systems such as computers as shown in Fig. 3.6.1, 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.



(L-302) **Fig. 3.6.1 : Noise contaminates the binary signal**

- These error can become a serious threat to the accuracy of the digital system. Therefore it is necessary to detect and correct the errors.

Types of errors :

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

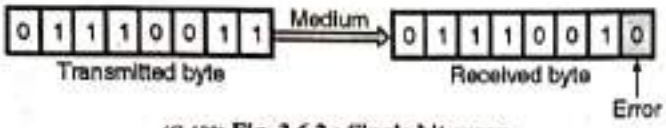
1. Content errors
2. Flow integrity errors.

- 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.

Scanned by CamScanner

Single bit error :

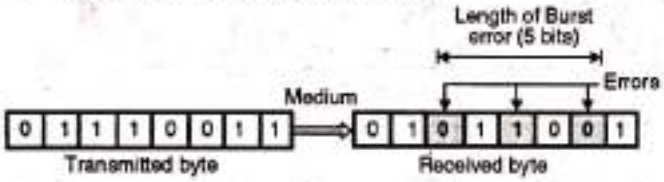
- The term single bit error suggests that only one bit in the given data unit such as byte is in error.
- That means only one bit in a transmitted byte will change from 1 to 0 or 0 to 1, as shown in Fig. 3.6.2.



(G-188) **Fig. 3.6.2 : Single bit error**

Burst errors :

- If two or more bits from a data unit such as a byte change from 1 to 0 or from 0 to 1 then burst errors are said to have occurred.
- Refer Fig. 3.6.3 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. 3.6.3.



(G-189) **Fig. 3.6.3 : Burst errors**

Disadvantages of coding :

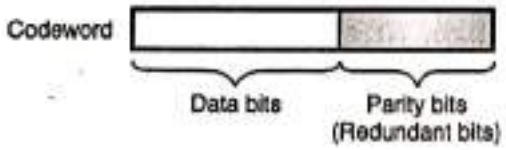
Some of the disadvantages of the coding technique are :

1. An increased transmission bandwidth is required in order to transmit the encoded signal. This is due to the additional bits (redundancy) added by the encoder.
2. Use of coding make the system complex.

3.6.1 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. 3.6.4.



(L-303) **Fig. 3.6.4 : 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.

$$\therefore \quad \text{Code rate } (r) = \frac{k}{n} \qquad ...(3.6.1)$$

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.

$$\therefore \quad \text{Code efficiency} = \text{Code rate} = \frac{k}{n} \qquad ...(3.6.2)$$

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 :

Code word No.1 :	1	1	1	1	0	1	0	0
	↕		↕		↕		↕	
Code word No.2 :	0	1	0	1	1	1	1	0

(G-190(b))

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.

Scanned by CamScanner

- The error detection and correction capabilities of a coding technique depend on the minimum distance as shown in the Table 3.6.1.

(L-899) **Table 3.6.1 : 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 > 1 errors per word	$d_{min} \geq (s + t + 1)$

Ex. 3.6.1 : Find the Hamming weight of the following code vector :

x = 1 1 0 1 0 1 0 0

Soln. :

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

3.6.2 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. 3.6.5.

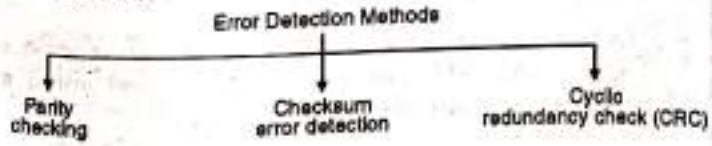
Transmitted codeword	1 0 1 0 1 1 0 0	1 1 1 0 1 0 1 1	0 0 1 0 0 1 0 1
Received codeword	1 1 1 0 1 1 0 0 (error)	0 1 1 1 1 0 1 1 (error)	1 0 1 1 0 0 0 1 (error)
Number of errors	1	2	3
Distance	1	2	3

(L-305) **Fig. 3.6.5**

- 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.

3.6.3 Error Detection Methods :

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

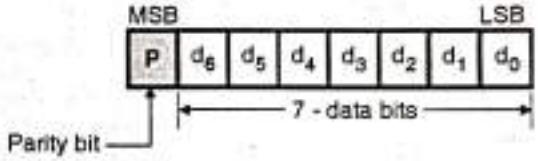


(L-308)

- 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.

3.6.4 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. 3.6.6, 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.

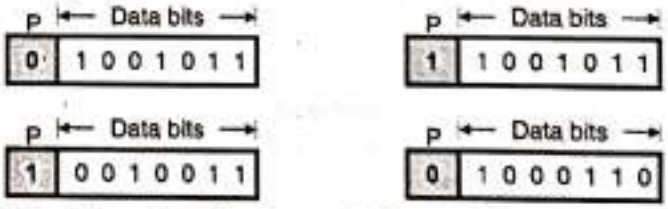


(L-309) **Fig. 3.6.6 : Format of a transmitted word with parity bit**

- 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.
- For odd parity this bit is set to 1 or 0 at the transmitter such that the number of "1 bits" in the entire word is odd.
- For even parity this bit is set to 1 or 0 such that the number of "1 bits" in the entire word is even. This is illustrated in Fig. 3.6.7.



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

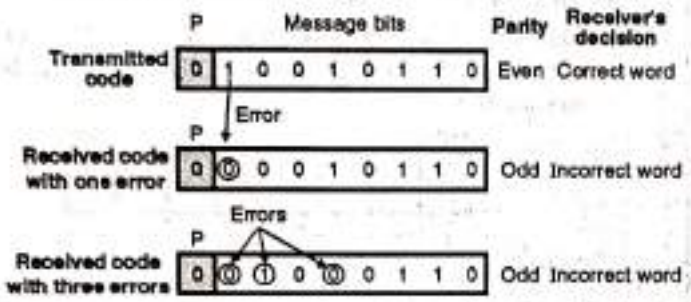
(L-310) **Fig. 3.6.7**

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.

Scanned by CamScanner

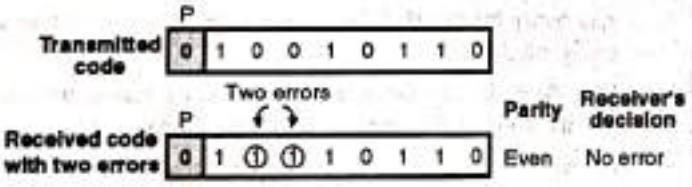
- That means if it is known that the parity of the transmitted signal is always going to be "even" and if the received signal has an odd parity then the receiver can conclude that the received signal is not correct. This is as shown in Fig. 3.6.8.
- If a single error or an odd number of bits change due 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. 3.6.8.
- 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. 3.6.8 : The receiver detects the presence of error if the number of errors is odd i.e. 1, 3, 5 ....**

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. 3.6.9 and the receiver will fail to detect the presence of errors.



(L-312) **Fig. 3.6.9 : The receiver cannot detect the presence of error if the number of errors is even i.e. 2, 4, 6 ....**

Conclusions :

1. Double or any even number of errors in the received word will not change the parity. Therefore even number of errors will be unnoticed.
2. 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 :

1. Thus the simple parity checking method has its limitations. It is not suitable for detection of multiple errors (two, four, six etc).
2. The other limitation of parity checking method is that it cannot reveal the location of erroneous bit. It cannot correct the error either.

Ex. 3.6.2 : Write the ASCII code of word "HOLE" using even parity.

Soln. :

Table P. 3.6.2 shows the ASCII code of word HOLE using even parity.

Table P. 3.6.2

	P	7	6	5	4	3	2	1
H	0	1	0	0	1	0	0	0
O	1	1	0	0	1	1	1	1
L	1	1	0	0	1	1	0	0
E	1	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 an external interference such as lightning which lasts for a duration of several bits.
- So the noise or interference produced by the lightening 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 samecode word.
- 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. 3.6.10. The final carry is ignored.

```
Word A : 1 0 1 1 0 1 1 1
         +
Word B : 0 0 1 0 0 0 1 0
         ---------------
Sum    : 1 1 0 1 1 0 0 1
```

(L-898) **Fig. 3.6.10 : 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.

Scanned by CamScanner

- 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. 3.6.2A : Find the checksum of the following message.

10110001, 10101011,
00110101, 10100001

Soln. :

Ignored

Carries	(1)0 1 0 1 1 1 1 0
Data bytes	+ 1 0 1 1 0 0 0 1 + 1 0 1 0 1 0 1 1 + 0 0 1 1 0 1 0 1 + 1 0 1 0 0 0 0 1
Checksum byte	**0 0 1 1 0 0 1 0**

(G-1943)

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

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.

3.6.5 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. 3.6.11.
- The parity bits are produced for each row and column of such block of data.
- The two sets of parity bits so generated are known as :
  1. Longitudinal Redundancy Check (LRC) bits
  2. Vertical Redundancy Check (VRC) bits.
- The LRC bits indicate the parity of rows and VRC bits indicate the parity of columns as shown in Fig. 3.6.11.

Characters		C	O	M	P	U	T	E	R	
7 bit ASCII codes (Message bits)	b_1	1	1	1	0	1	0	1	0	1
	b_2	1	1	0	0	0	0	0	1	1
	b_3	0	1	1	0	1	1	1	0	1
	b_4	0	1	1	0	0	0	0	0	0
	b_5	0	0	0	1	1	1	0	1	0
	b_6	0	0	0	0	0	0	0	0	0
VRC bits (even parity)	b_7	1	1	1	1	1	1	1	1	0
	→	1	1	0	0	0	1	1	1	1

These bits will make the parity of each column even

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

(L-315) **Fig. 3.6.11 : Vertical and longitudinal parity check bits**

The Vertical Redundancy Check (VRC) Bits :

- As shown in Fig. 3.6.11 the VRC bits are parity bits associated with the ASCII code of each character. Each VRC bit will make the parity of its corresponding column "an even parity". For example consider column 1 corresponding to character "C". The ASCII code for the character C is,

Character	C
b_1	1
b_2	1
b_3	0
b_4	0
b_5	0
b_6	0
b_7	1
VRC bit →	1

← Column - 1 of the data block

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

(G-1944)

- Therefore the 8th bit which is a VRC bit is made "1" to make the parity even. Similarly the other VRC bits are found as shown in Fig. 3.6.11.

Scanned by CamScanner

The Longitudinal Redundancy Check (LRC) Bits :

- The LRC bits are parity bits associated with the rows of the data block of Fig. 3.6.11. Each LRC bit will make the parity of the corresponding row, an even parity. For example, consider row 1 of Fig. 3.6.11.

Row 1 :	b_1	1	1	1	0	1	0	1	0	1

← LRC bit to make parity even

(G-1945)

How to locate the bit in error ?

- Even a single error in any bit will result in a noncorrect "LRC" in one of the rows and an incorrect VRC in one of the columns. The bit which is common to the row and column is the bit in error.
- However there is still a limitation on the Block parity code, which is that, multiple errors in rows and columns can be only detected but they cannot be corrected. This is because, it is not possible to locate the bits which are in error. This will be clear when you will solve the following example.

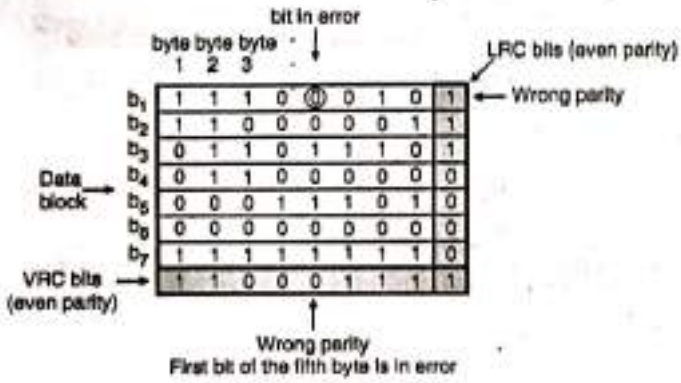
Ex. 3.6.3 : The following bit stream is encoded using VRC, LRC and even parity. Locate and correct the error if it is present.

11000011 11110011
10110010 00001010
00101010 00101011
10100011 01001011
11100001

Soln. :

1. Fig. P. 3.6.3 shows the received data block alongwith the LRC and VRC bits.
2. 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.



b_1	1	1	1	0	1	0	1	0	1
b_2	1	1	0	0	0	0	0	1	1
b_3	0	1	1	0	1	1	1	0	1
b_4	0	1	1	0	0	0	0	0	0
b_5	0	0	0	1	1	1	0	1	0
b_6	0	0	0	0	0	0	0	0	0
b_7	1	1	1	1	1	1	1	1	0
VRC	1	1	0	0	0	1	1	1	1

(G-199) **Fig. P. 3.6.3**

3.6.6 Cyclic Redundancy Check (CRC) :

MU : May 09, Dec. 12, May 13

University Questions

Q. 1 What is CRC ? Write the algorithm for computing checksum and explain with suitable example. **(May 09, 10 Marks)**

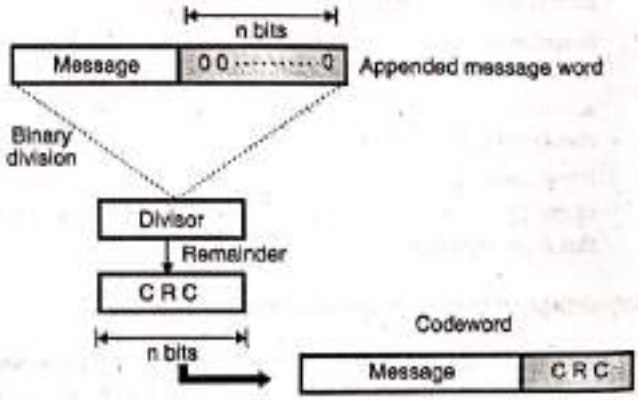
Q. 2 What is CRC ? **(Dec. 12, 5 Marks)**

Q. 3 Explain with the suitable example CRC algorithm for computing checksum. **(May 13, 10 Marks)**

- 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. 3.6.12.



(L-819) **Fig. 3.6.12 : CRC generator**

Scanned by CamScanner

- 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.

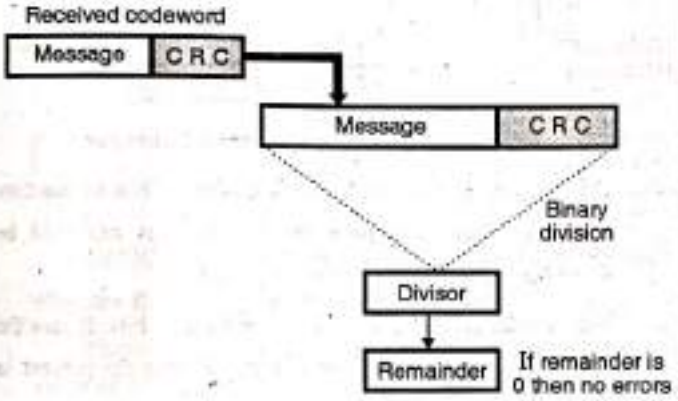
Step 2 : Divide the newly generated data unit in step 1 by the divisor (generator). This is a binary division.

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. 3.6.12.

CRC checker :

- Fig. 3.6.13 shows the CRC checker.



(L-820) **Fig. 3.6.13 : CRC checker**

- The codeword received at the receiver consists of message and CRC. (Fig. 3.6.13)
- 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.

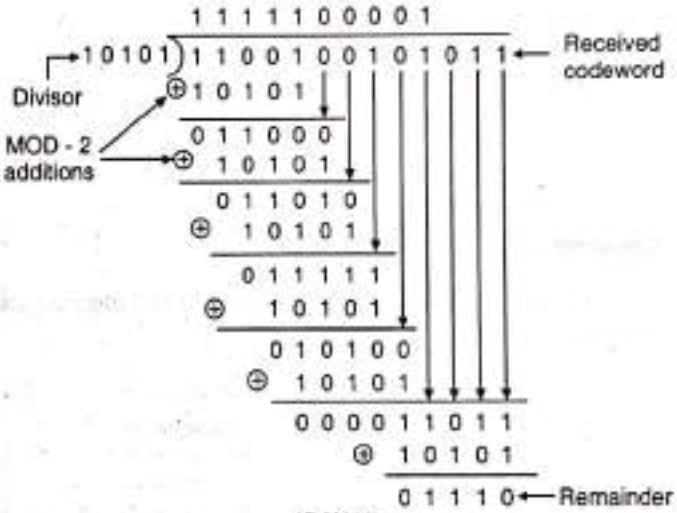
Ex. 3.6.4 : The codeword is received as 1100 1001 01011. Check whether there are errors in the received codeword, if the divisor is 10101. (The divisor corresponds to the generator polynomial).

Soln. :

- 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



(G-201(a))

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. 3.6.5 : Generate the CRC code for the data word of 1100 10101. The divisor is 10101.

Soln. :

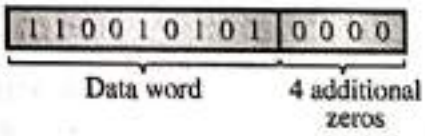
Given : Data word : 110010101

Divisor : 10101.

The number of data bits = m = 9

The number of bits in the codeword = n = 5

Dividend = Data word + (n – 1) zeros.



(G-801(a))

Scanned by CamScanner

Carry out the division as follows :

```
                 1 1 1 1 1 0 0 1 1 1        ← Quotient
Divisor → 1 0 1 0 1 ) 1 1 0 0 1 0 1 0 1 0 0 0 0   ← Dividend
                      1 0 1 0 1
                      ⊕ ⊕ ⊕ ⊕ ⊕
                      0 1 1 0 0 0
                        1 0 1 0 1
                        0 1 1 0 1 1
                          1 0 1 0 1
                          0 1 1 1 0 0
                            1 0 1 0 1
                            1 0 0 1 1
                            1 0 1 0 1
                                1 1 0 0 0
                                1 0 1 0 1
                                  1 1 0 1 0
                                  1 0 1 0 1
                                    1 1 1 1 0
                                    1 0 1 0 1
                                      1 0 1 1  ← Remainder
```

(G-801(b))

Codeword :

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

∴	1100101010000	Dividend
+	1011	Remainder
	1100101011011	Codeword

(G-2290)

∴ Codeword = | 1 1 0 0 1 0 1 0 1 | 1 0 1 1 |

Data word Remainder

(G-1761)

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.

3.6.7 Error Correction : MU : Dec. 12

University Questions

Q. 1 Explain the error detection and error correction algorithms. **(Dec. 12, 10 Marks)**

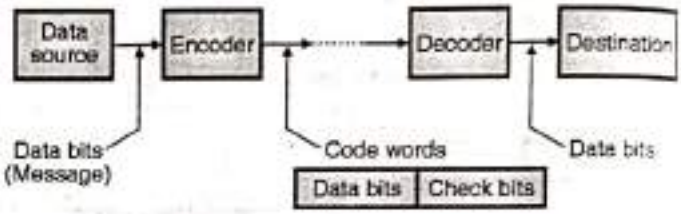
We are going to discuss two completely different approaches for the error control. They are :

1. Forward error correction (FEC)
2. 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. 3.6.14.
- 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.

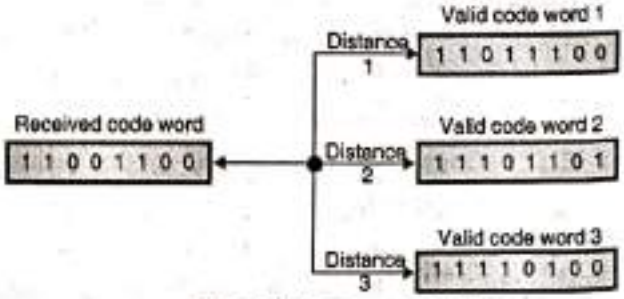


(L-306) **Fig. 3.6.14 : Error correction technique**

- The encoder of Fig. 3.6.14, 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.

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. 3.6.15.



(L-307) **Fig. 3.6.15 : Concept of FEC**

Scanned by CamScanner

- In Fig. 3.6.15, the valid code word 1 has the minimum distance (1), hence it is the most likely correct code word.

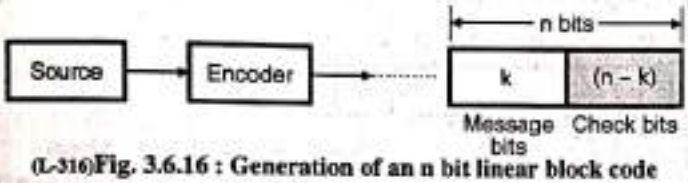
Error correction techniques :

Some of the FEC techniques are as follows :

1. Linear block codes.
2. Convolutionnl coding.
3. Hamming codes.
4. Cyclic codes.

3.6.8 Linear Block Codes :

- The generation of block codes is illustrated in Fig. 3.6.16. To generate an (n, k) block code, the encoder accepts the information in the form of block of successive "k" bits.
- At the end of each such block (of k message bits) it adds (n – k) parity bits as shown in Fig. 3.6.16. As these bits do not contain any information, they are called as "redundant" bits.
- It is important to note that the (n – k) parity bits are related algebraically related to the "k" message bits. The n bit code word is thus produced as shown in Fig. 3.6.16.



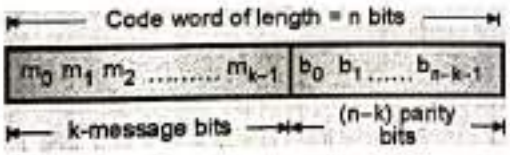
(L-316)**Fig. 3.6.16 : Generation of an n bit linear block code**

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. 3.6.17.



(G-206) **Fig. 3.6.17 : Structure of the codeword for a linear block code**

3.6.9 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 :

1. Block length : $n = 2^m - 1$
2. Number of message bits : $k = 2^m - m - 1$ ...(3.6.3)
3. Number of parity bits : $(n - k) = m$.

   Where $m \geq 3$. i.e. minimum number of parity bits is 3.
4. The minimum distance $d_{min} = 3$.
5. The code rate or code efficiency

$$= \frac{k}{n} = \frac{2^m - m - 1}{2^m - 1} = 1 - \frac{m}{2^m - 1} \quad ...(3.6.4)$$

If m >> 1 then code rate r = 1.

Error detection and correction capabilities of Hamming code :

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

1. The number of errors that can be detected per word = 2.

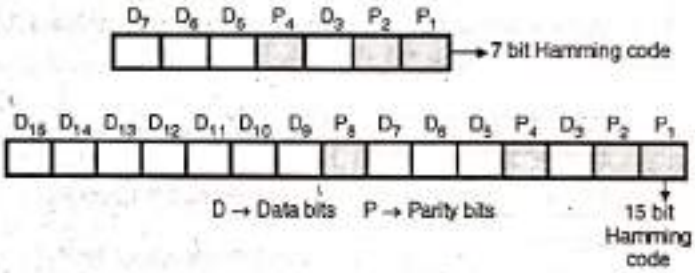
   since $d_{min} \geq (s + 1)$ $\therefore$ $3 \geq s + 1$ $\therefore$ $s \leq 2$
2. The number of errors that can be corrected per word = 1

   since $d_{min} \geq (2t + 1)$ $\therefore$ $3 \geq (2t + 1)$ $\therefore$ $t \leq 2$

Thus with $d_{min} = 3$ it is possible to detect upto 2 errors and it is possible to correct upto only 1 error.

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. 3.6.18.
- The 7-bit Hamming code is used commonly, but the concept can be extended to any number of bits.

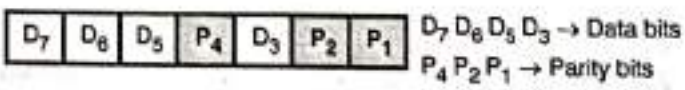


(G-1946) **Fig. 3.6.18 : Hamming code words**

Note that the parity bits are inserted at each 2^n bit where n = 0, 1, 2, 3 ..... . Thus P_1 is at $2^0 = 1$, i.e. at first bit, P_2 is at $2^2 = 2$ P_4 is as 2^2 and P_8 is at 2^3 as shown in Fig. 3.6.18.

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. 3.6.19.



(G-1947) **Fig. 3.6.19 : Code word pattern for Hamming code**

2. The D bits in Fig. 3.6.19 are data bits, whereas P bits are parity bits. The parity bits P_1, P_2, P_4 are adjusted in a particular way as explained below.

Minimum number of parity bits :

- Table 3.6.2(a) gives a listing of minimum number of parity bits needed for various ranges of "m" information bits.

Scanned by CamScanner

Table 3.6.2(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 3.6.2(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.

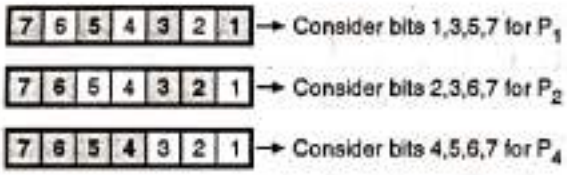
Table 3.6.2(b)

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 P_1 :

P_1 is adjusted to 0 or 1 so as to establish even parity over bits 1,3,5 and 7 i.e. P_1, D_3, D_5 and D_7.



(G-2291)

Selection of P_2 :

P_2 is adjusted to 0 or 1 so as to set even parity over bits 2,3,6 and 7 (P_2, D_3, D_6 and D_7).

Selection of P_4 :

P_4 is adjusted to 0 or 1 so as to set even parity over bits 4,5,6 and 7 (P_4, D_5, D_6 and D_7).

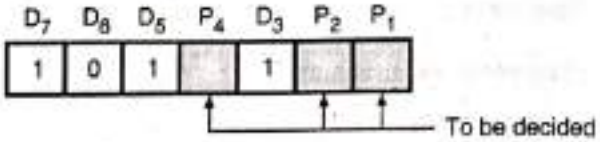
The selection of parity bits will be clear after solving the following example.

Ex. 3.6.6 : 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 :

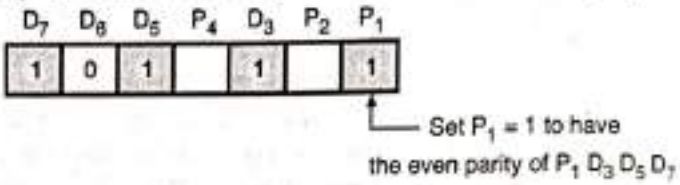
The seven bit Hamming code format is shown in Fig. P. 3.6.6 : Given bit word = 1 0 1 1



(G-1948) **Fig. P. 3.6.6**

Step 2 : Decide P_1 :

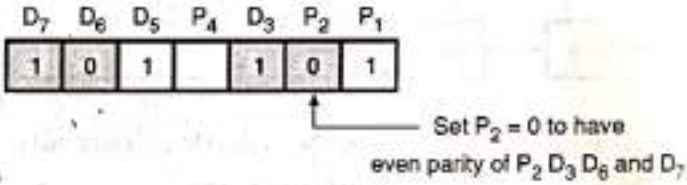
P_1 sets the parity of bits P_1, D_3, D_5 and D_7. As D_7, D_5, D_3 = 1 1 1 we have to set P_1 = 1 in order to have the even parity.



(G-1949)

Step 3 : Decide P_2 :

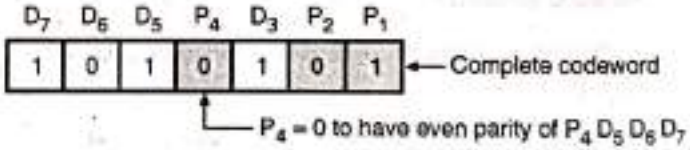
P_2 is set to have the even parity of P_2 D_3 D_6 and D_7. But D_3 D_6 D_7 = 1 0 1 hence set P_2 = 0.



(G-1950)

Step 4 : Decide P_4 :

P_4 is set to have the even parity of P_4 D_5 D_6 and D_7. But D_5 D_6 D_7 = 1 0 1, hence set P_4 = 0.

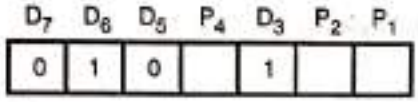


(G-1951)

Ex. 3.6.7 : Encode the data bits 0 1 0 1 into a seven bit even parity Hamming code.

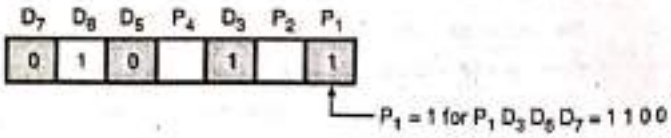
Soln. :

Step 1 :



(G-1952)

Step 2 : Select P_1 for P_1 D_3 D_5 D_7 :



(G-1953)

Scanned by CamScanner

Step 3 : Select P_2 for $P_2 D_3 D_6 D_7$:

D_7	D_6	D_5	P_4	D_3	P_2	P_1
0	1	0		1	0	1

$P_2 = 0$ for $P_2 D_3 D_6 D_7 = 0\ 1\ 1\ 0$

(G-1954)

Step 4 : Select P_4 :

D_7	D_6	D_5	P_4	D_3	D_2	D_1
0	1	0	1	1	0	1

Set $P_4 = 1$ to have $P_4 D_5 D_6 D_7 = 1\ 0\ 1\ 0$

(G-1955)

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

0	1	0	1	1	0	1

← Complete codeword

(G-1956)

Detection and correction of errors :

1. The Hamming coded data is now transmitted. At the receiver it is decoded to get the data back.
2. The bits (1, 3, 5, 7) , (2, 3, 6, 7) and (4, 5, 6, 7) are checked for even parity.
3. If all the 4-bit groups mentioned above possess the even parity then the received code word is correct i.e. it does not contain errors.
4. But if the parity is not even (i.e. it is odd) then error exists. Such an error can be located by forming a three bit number out of the three parity checks. This process becomes clear by solving the example given below.

Ex. 3.6.8 : 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. :

	D_7	D_6	D_5	P_4	D_3	P_2	P_1
Received codeword :	1	0	1	1	0	1	1

(G-1957)

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

$P_4\ D_5\ D_6\ D_7 = 1\ 1\ 0\ 1 \rightarrow$ Odd parity.

$\therefore$ 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 :

$\therefore P_2\ D_3\ D_6\ D_7 = 1\ 0\ 0\ 1 \rightarrow$ Even parity so no error.

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

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

$\therefore P_1\ D_3\ D_5\ D_7 = 1\ 0\ 1\ 1 \rightarrow$ 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 :

Error word E =

P_4	P_2	P_1

1's position

2's position

4's position

(G-1958)

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

E =

1	0	1

$E = (5)_{10}$

(G-1959)

Hence bit 5 of the transmitted codeword is in error.

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

Incorrect bit

(G-1960)

Step 5 : Correct the error :

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

Correct codeword = [1 0 0 1 0 1 1]

Ex. 3.6.9 : A seven bit Hamming code is received as 1 1 1 0 1 0 1. What is the correct code ?

Soln. :

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

← Received codeword

(G-1961)

Scanned by CamScanner

1. Check bits 4, 5, 6, 7 → Odd parity, hence error ∴ $P_4 = 1$
2. Check bits 2, 3, 6, 7 → Odd parity, hence error ∴ $P_2 = 1$
3. Check bits 1, 3, 5, 7 → Even parity, hence no error ∴ $P_1 = 0$

(G-1968)

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

∴ Error word E = | 1 | 1 | 0 |
P_4 P_2 P_1

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

∴ Correct codeword :

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	1	0	1	0	1

Inverted bit

(G-1962)

Ex. 3.6.10 : Write the steps to generate the Hamming code. Prepare hamming code for bit pattern 1010. 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 3.6.9 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. 3.6.10(a).

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	1		0		

To be decided

(G-1963) **Fig. P. 3.6.10(a)**

Step 2 : Decide P_1, P_2 and P_4 :

- P_1 sets the parity of P_1, D_3, D_5 and D_7. As $D_7 D_5 D_3 = 110$, $P_1 = 0$ so as to have the even symmetry.
- P_2 is set to have the even parity of P_2, D_3, D_6 and D_7. But $D_3 D_6 D_7 = 001$. Hence $P_2 = 1$.
- P_4 is set to have the even parity of P_4 D_5 D_6 and D_7. But $D_5 D_6 D_7 = 101$ so $P_4 = 0$.
- The codeword is shown in Fig. P. 3.6.10(b).

1	0	1	0	0	1	0

Complete codeword

(G-1964) **Fig. P. 3.6.10(b)**

The error detection and correction :

The 7th bit is in error. So the received codeword is as shown in Fig. P. 3.610(c).

Received codeword :

D_7	D_6	D_5	P_4	D_3	P_2	P_1
0	0	1	0	0	1	0

Error

(G-1965) **Fig. P. 3.6.10(c)**

Step 3 : Error detection and correction :

1. Analyze bits 4, 5, 6, 7
   $P_4 D_5 D_6 D_7 = 0100 \rightarrow$ odd parity so error exists here.
   ∴ Put $P_4 = 1$ in the 4's position of error word.
2. Analyze bits 2, 3, 6, 7
   $P_2 D_3 D_6 D_7 = 1000 \rightarrow$ odd parity so error exists here.
   ∴ Put $P_2 = 1$ in the 2's position of error word.
3. Check the bits 1, 3, 5, 7
   $P_1 D_3 D_5 D_7 = 0010 \rightarrow$ odd parity so error exists.
   ∴ Put $P_1 = 1$ in the 1's position of error word.
4. The error word is shown in Fig. P. 3.6.10(d).

Error word E = | P_4 | P_2 | P_1 | = | 1 | 1 | 1 |

(G-1966) **Fig. P. 3.6.10(d) : Error word**

The decimal equivalent of error word is $(7)_{10}$. Hence bit 7 in the received codeword is in error.

Ex. 3.6.11 : 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 3.6.6.**
- The generator polynomial actually acts as the divisor in the process of CRC generation.

∴ Data word : 110101011

Divisor : $x^4 + 0x^3 + 0x^2 + x + 1 = 10011$

1 1 0 1 0 1 0 1 1	0 0 0 0
Data word	4 additional zeros

(G-216)

The number of data bits = m = 9

The number of bit in the codeword = N

Dividend = Data word + (N – 1) number of zeros.

Scanned by CamScanner

Carry out the division as follows :

```
                 1 1 0 0 0 0 1 1 1
10011 ) 1 1 0 1 0 1 0 1 1 0 0 0 0
        1 0 0 1 1
Mod 2 → ⊕ ⊕ ⊕ ⊕ ⊕
addition  0 1 0 0 1 1
            1 0 0 1 1
            0 0 0 0 0 0 1 1 0 0
                  1 0 0 1 1
                  1 1 1 1 1
                  1 0 0 1 1
                  0 1 1 0 0 0
                    1 0 0 1 1
                    0 1 0 1 1 0
                      1 0 0 1 1
                      0 0 1 0 1 ← Remainder
```

(G-216(a))

Codeword : The codeword is given by :

Codeword = | 1 1 0 1 0 1 0 1 1 | 0 1 0 1 |

← Dataword → ← Remainder →

(G-216(b))

Internationally used CRC polynomials :

The three polynomials which are used internationally are :

$$\text{CRC 12} = x^{12} + x^{11} + x^{3} + x^{2} + x^{1} + 1$$

$$\text{CRC 16} = x^{16} + x^{15} + x^{2} + 1$$

$$\text{CRC} - \text{CCITT} = x^{16} + x^{12} + x^{5} + 1$$

3.6.10 Solved Examples :

Ex. 3.6.12 : If the frame is 1101011011 and generator is $x^4 + x + 1$ what would be the transmitted frame.

May 05, Dec. 09, 5 Marks, May 11, 10 Marks

Soln. :

Given : Data word : 1 1 0 1 0 1 1 0 1 1

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 :

Dividend | 1 1 0 1 0 1 1 0 1 1 | 0 0 0 0 |

← Data word → ← 4 additional zeros →

(G-216(c))

Step 2 : Carryout the long division :

```
Generator                                   Dividend
                 1 1 0 0 0 0 1 0 1 0
10011 ) 1 1 0 1 0 1 1 0 1 1 0 0 0 0 ←
        1 0 0 1 1
        ⊕⊕⊕⊕⊕
          0 1 0 0 1 1
            1 0 0 1 1
            0 0 0 0 0 1 0 1 1 0
                  1 0 0 1 1
                  0 0 1 0 1 0 0
                    1 0 0 1 1
                    0 0 1 1 1 0 ←
                                Remainder
```

(G-216(d))

Step 3 : Write the transmitted frame :

The transmitted frame is obtained by writing the data word followed by the remainder.

```
∴   1 1 0 1 0 1 1 0 1 1 0 0 0 0 ← Dividend
                        1 1 1 0 ← Remainder
+
  → 1 1 0 1 0 1 1 0 1 1 1 1 1 0
Transmitted frame
```

(G-1967)

∴ The transmitted codeword is as follows :

| 1 1 0 1 0 1 1 0 1 1 | 1 1 1 0 |

← Dataword → ← Remainder →

(G-216(e))

Ex. 3.6.13 : What is the remainder obtained by dividing $x^7 + x^5 + 1$ by the generator polynomial $x^3 + 1$?

Soln. :

Given : Dividend : $x^7 + x^5 + 1 = x^7 + 0x^6 + x^5 + 0x^4 + 0x^3 + 0x^2 + 0x + 1$

$= 10100001$

Divisor : $x^3 + 1 = x^3 + 0x^2 + 0x + 1 = 1001$

The long division is as follows :

```
          1 0 1 1 0
1001 ) 1 0 1 0 0 0 0 1
       1 0 0 1
       0 0 1 1 0 0
         1 0 0 1
         0 1 0 1 0
           1 0 0 1
           0 0 1 1 1 ← Remainder
```

(G-216(f))

The remainder is 00111 = $x^2 + x + 1$ in the polynomial form.

Scanned by CamScanner

Ex. 3.6.14 : 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

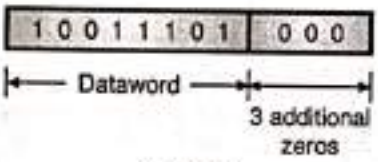
Generator polynomial :

$x^3 + 1 = x^3 + 0x^2 + 0x + 1 = 1001 = n$

Step 1 : Obtain the dividend :

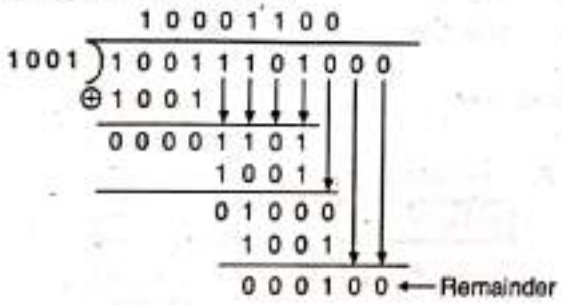
Dividend = Data word + 3 zeros.

The dividend is as follows :



(G-216(g))

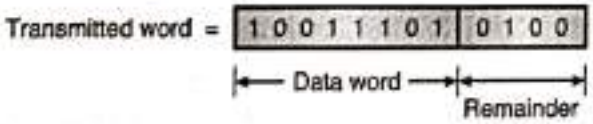
Step 2 : Carry out the division :



(G-216(h))

Step 3 : Obtain the actually transmitted bit stream :

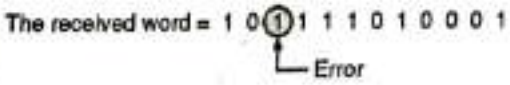
The transmitted word is obtained by writing the data word followed by the remainder as follows :



(G-216(i))

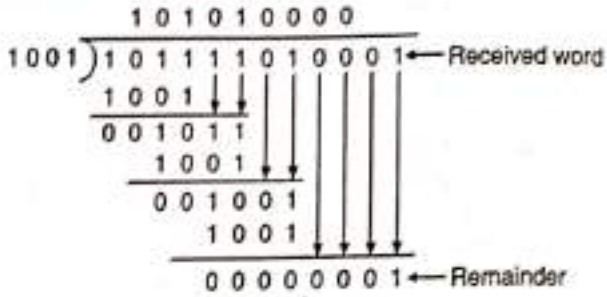
Error detection :

Step 4 : Write the erroneous received word :



(G-2292)

At the receiver, this word is divided by the same divider used at the transmitter i.e. 1001.

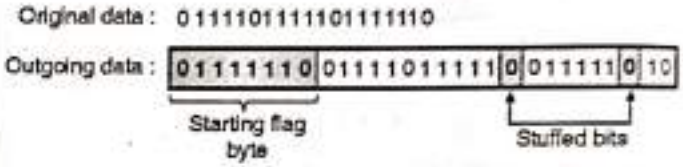


(G-216(j))

A non zero remainder indicates that there is an error in the received codeword.

Ex. 3.6.15 : A bit string 0111101111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing ?

Soln. : The original bit stream and the stream after bit stuffing are shown in Fig. P. 3.6.15.



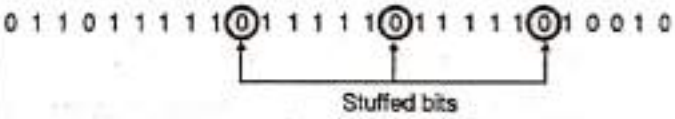
(G-217) **Fig. P. 3.6.15**

Ex. 3.6.16 : Apply bit stuffing

011011111111111111110010

Soln. :

The outgoing data after bit stuffing is shown in Fig. P. 3.6.16.



(G-218) **Fig. P. 3.6.16**

Ex. 3.6.17 : 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	P_8	1	0	0	P_4	1	P_2	P_1

(G-218(a))

Scanned by CamScanner

Step 2 : Select P_1 for $P_1\ D_3\ D_5\ D_7\ D_9\ D_{11}\ D_{13}$:

Parity needs to be even parity

D_{13}	D_{11}	D_9	D_7	D_5	D_3	
1	1	1	1	0	1	P_1

(G-218(b))

For even parity P_1 should be 1. $\therefore$ **$P_1 = 1$**

Step 3 : Select P_2 :

To select P_2 we have to consider the bits in positions 2, 3, 6, 7, 10 and 11

$\therefore$ 10101P_2 $\rightarrow$ $P_2 = 1$ $\therefore$ **$P_2 = 1$**

Step 4 : Select P_4 :

For P_4, we have to consider the bits in the following positions 4, 5, 6, 7, 12, 13 and select the value of P_4 for even parity.

$\therefore$ 11100P_4 $\therefore$ **$P_4 = 1$**

Step 5 : Select P_8 :

To select P_8, consider the bit in following positions 8, 9, 10, 11, 12, 13 and select P_8 for even parity.

$\therefore$ 11101P_8 $\therefore$ **$P_8 = 0$**

So the codeword is as follows :

					P_8				P_4		P_2	P_1
1	1	1	0	1	0	1	0	0	1	1	1	1

Codeword

(G-218(c))

Ex. 3.6.18 : Consider an error detecting CRC with the generator 10101. Assume the CRC bits follows the data bits in any transmission :

1. Compute the transmitted bit sequence for the data bit sequence 01101101.
2. The string of bits 110011001100 is received. Is it acceptable, and if so what is the data bit sequence.

Dec. 03, 10 Marks

Soln. :

Part I : Transmitted bit sequence :

Given : Data bit sequence : 01101101

Generator : 10101

Step 1 : Append 4 zeros to the data bit sequence :

Dividend = Data word + 4 zeros

= | 01101101 | 0000 |

Data bit sequence — 4 Zeros

(G-801(o))

Step 2 : Carry out division :

```
                 1 1 1 1 1 0 1 1 1
1 0 1 0 1 ) 0 1 1 0 1 1 0 1 0 0 0 0
            ⊕ 1 0 1 0 1
              1 1 0 0 0
            ⊕ 1 0 1 0 1
              0 1 1 0 1 1
            ⊕   1 0 1 0 1
              0 1 1 1 0 0
            ⊕   1 0 1 0 1
              0 1 0 0 1 1
            ⊕   1 0 1 0 1
              0 0 1 1 0 0 0
            ⊕     1 0 1 0 1
                0 1 1 0 1 0
              ⊕   1 0 1 0 1
                0 1 1 1 1 0
              ⊕   1 0 1 0 1
                  0 1 0 1 1 ← Remainder
```

(G-801(p))*

Step 3 : Codeword :

Codeword = Dividend + Remainder

= | 01101101 | 1011 |

Part II :

Received word : 110011001100

Carry out the division as follows :

```
                 1 1 1 1 1 1 0 0
1 0 1 0 1 ) 1 1 0 0 1 1 0 0 1 1 0 0
            ⊕ 1 0 1 0 1
              0 1 1 0 0 1
            ⊕   1 0 1 0 1
              0 1 1 0 0 0
            ⊕     1 0 1 0 1
              0 1 1 0 1 0
            ⊕     1 0 1 0 1
              0 1 1 1 1 1
            ⊕     1 0 1 0 1
              0 1 0 1 0 1
            ⊕     1 0 1 0 1
              0 0 0 0 0 0 0 ← Remainder
```

(G-801(q))

Since the remainder is 0, the received codeword is acceptable and does not contain errors. So it is acceptable.

Scanned by CamScanner

Received codeword = | 1 1 0 0 1 1 0 0 | 1 1 0 0 |

(G-801(r))

Ex. 3.6.19 : Consider an error detecting CRC with the generator 10101.

1. Compute the transmitted bit sequence for the data bit sequence 1101101.
2. The string of bits 110011001100 is received. Is acceptable, and if so what is the data bit sequence.

Dec. 05, 10 Marks

Soln. :

Part I : Transmitted bit sequence :

Given : Data bit sequence : 1101101

Generator : 10101

Step 1 : Obtain the dividend :

Dividend = Data word followed by 4 zeros.

= 1101101 0000

Step 2 : Carry out division :

```
                1 1 1 0 1 1 1
1 0 1 0 1 ) 1 1 0 1 1 0 1 0 0 0 0
            ⊕ 1 0 1 0 1
              0 1 1 1 0 0
              ⊕ 1 0 1 0 1
                0 1 0 0 1 1
                ⊕ 1 0 1 0 1
                  0 0 1 1 0 0 0
                  ⊕ 1 0 1 0 1
                    0 1 1 0 1 0
                    ⊕ 1 0 1 0 1
                      0 1 1 1 1 0
                      ⊕ 1 0 1 0 1
                        1 0 1 1  ← Remainder
```

(G-801(t))

Step 3 : Transmitted bit sequence :

The transmitted bit sequence is obtained by adding remainder to the dividend.

∴ Transmitted code word = | 1 1 0 1 1 0 1 | 1 0 1 1 |

Data bits Remainder

(G-801(u))

Part II :

The received bit sequence is 1100 1100 1100. Divide it by the same generator used in part I.

```
                1 1 1 1 1 1 0 0
1 0 1 0 1 ) 1 1 0 0 1 1 0 0 1 1 0 0
            ⊕ 1 0 1 0 1
              0 1 1 0 0 1
              ⊕ 1 0 1 0 1
                0 1 1 0 0 0
                ⊕ 1 0 1 0 1
                  0 1 1 0 1 0
                  ⊕ 1 0 1 0 1
                    0 1 1 1 1 1
                    ⊕ 1 0 1 0 1
                      0 1 0 1 0 1
                      ⊕ 1 0 1 0 1
                        0 0 0 0 0 0 0  ← Remainder
```

(G-801(v))

Since the remainder is zero, there are no errors in the received bit sequence. Hence it is acceptable. The received sequence is,

| 1 1 0 0 1 1 0 0 | 1 1 0 0 |

← Bit sequence → ← Remainder →

(G-801(w))

∴ Received bit sequence = 11001100 ...Ans.

Ex. 3.6.20 : An 8-bit byte with binary value 10101111 is to be encoded using an even-parity Hamming code. What is the binary value after encoding ?

Dec. 10, 5 Marks, Dec. 11, May 12, 10 Marks

Soln. : Data number : 10101111

Step 1 :

- Number of message bits are 8. 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 in Fig. P. 3.6.20.

D_{12}	D_{11}	D_{10}	D_9		D_7	D_6	D_5		D_3		
1	0	1	0	P_8	1	1	1	P_4	1	P_2	P_1

Fig. P. 3.6.20

Step 2 : Select P_1 for P_1 D_3 D_5 D_7 D_9 D_{11} :

Parity needs to be even parity.

D_{11}	D_9	D_7	D_5	D_3	
0	0	1	1	1	P_1

Fig. P. 3.6.20(a)

For even parity P_1 should be 1.

∴ P_1 = 1

Step 3 : Select P_2 for P_2 D_3 D_6 D_7 D_{10} D_{11} :

D_{11}	D_{10}	D_7	D_6	D_3	
0	1	1	1	1	P_2

Fig. P. 3.6.20(b)

Scanned by CamScanner

$\therefore \quad P_2 = 0$

Step 4 : Select P_4 for $P_4\ D_5\ D_6\ D_7\ D_{12}$:

D_{12}	D_7	D_6	D_5	
1	1	1	1	P_4

Fig. P. 3.6.20(c)

$\therefore \quad P_4 = 0$

Step 5 : Select P_8 for $P_8\ D_9\ D_{10}\ D_{11}\ D_{12}$:

D_{12}	D_{11}	D_{10}	D_9	
1	0	1	0	P_8

Fig. P. 3.6.20(d)

$\therefore \quad P_8 = 0$

So codeword is as follows,

					P_8				P_4		P_2	P_1
Codeword :	1	0	1	0	0	1	1	1	0	1	0	1

Fig. P. 3.6.20(e)

Ex. 3.6.21 : Compute the Hamming code for the data - 1001101. **Dec. 13, 5 Marks**

Soln. :

Step 1 : **Codeword format :**

11	10	9	8	7	6	5	4	3	2	1
1	0	0	P_8	1	1	0	P_4	1	P_2	P_1

(G-2278) **Fig. P. 3.6.21 : Codeword format**

Step 2 : **Find : P_1, P_2, P_4, P_8 :**

Assume even parity.

1. **P_1 :**

   Consider bits 1,3,5,7,9,11 They are,

   10101 P_1 $\therefore$ For even parity $P_1 = 1$

2. **P_2 :**

   Consider bits 2,3,6,7,10,11 They are,

   10111 P_1 $\therefore$ For even parity $P_2 = 0$

3. **P_4 :**

   Consider bits 4,5,6,7 They are,

   110 P_4 $\therefore$ For even parity $P_4 = 0$

4. **P_8 :**

   Consider bits 8,9,10,11 They are,

   1 0 0 P_8 $\therefore$ For even parity $P_8 = 1$

Step 3 : **Write the codeword :**

Code word =

1	0	0	1	1	1	0	0	1	0	1

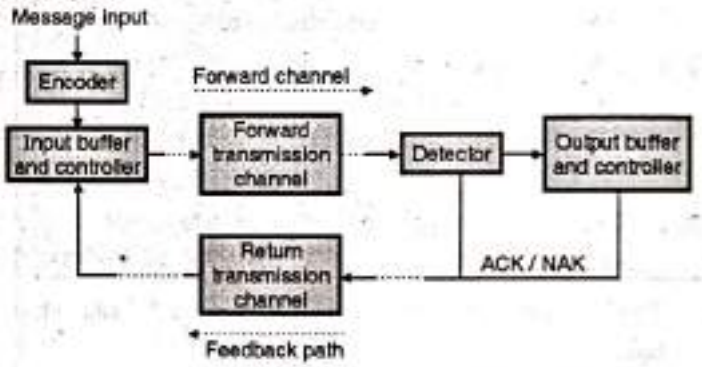
(G-2279)

3.6.11 ARQ Technique :

- There are two basic systems of error detection and correction. The first on 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. 3.6.20.



(L-372) **Fig. 3.6.20 : Block diagram of the basic ARQ system**

Operation of ARQ system :

- The encoder produces codewords for each message signal at its input. Each codeword at the encoder output is stored temporarily and transmitted over the forward transmission channel.
- At the destination a decoder will decode the code words and 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.

Scanned by CamScanner

- 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.

3.7 Flow Control :

MU : Dec. 09, Dec. 11, Dec. 14, May 16

University Questions

Q. 1 Explain framing, flow and error control in data link layer. **(Dec. 09, Dec. 11, 10 Marks)**

Q. 2 Why is flow control needed ? What are the mechanisms ? Explain how the Go-Back-N and Selective Repeat ARQ differ from each other. **(Dec. 14, 10 Marks)**

Q. 3 Explain any four functions of data link layer with example. **(May 16, 10 Marks)**

- 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.

3.8 Elementary Data Link Protocols :

In this section we are going to discuss some elementary data link layer protocols.

3.8.1 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.

Scanned by CamScanner

3.8.2 A Simplex Stop and Wait Protocol :

MU : Dec. 03, May 07, Dec. 08, Dec. 09

University Questions

Q. 1 Explain stop and wait sliding window protocol.

(Dec. 03, 10 Marks)

Q. 2 Explain stop and wait sliding window protocols with suitable examples.

(May 07, Dec. 08, Dec. 09, 10 Marks)

- 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.

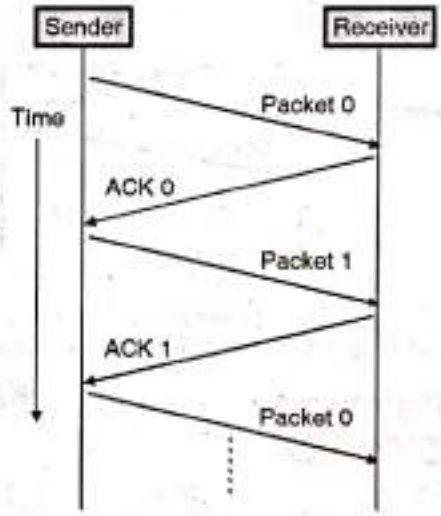
3.8.3 A Simplex Protocol for Noisy Channel :

- 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 :

  1. Normal operation and 2. 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 that numbers in each ACKs.



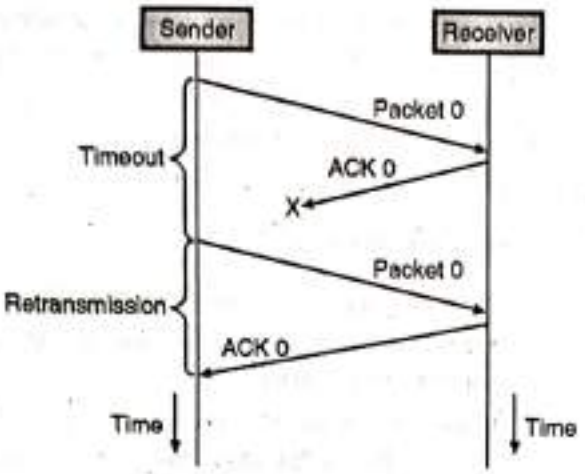
(G-220)Fig. 3.8.1 : Positive acknowledgement with retransmission

2. Time out :

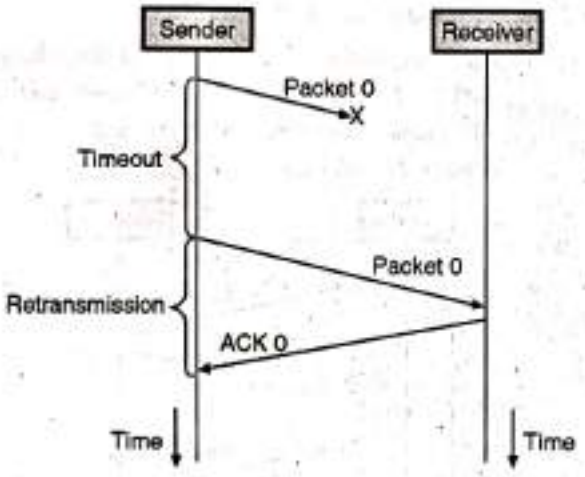
- If the sender does not receive **ACK** for previous sent frame after a certain period of time, the sender *times out* and *retransmit* that frame again.
- There are two cases when the sender does not receive ACK; one is when the ACK is lost and the other is when the frame itself is not received i.e. it got lost. These two possible cases are illustrated in Fig. 3.8.2.
- To support this feature, the sender keeps timer for each frame.

Scanned by CamScanner

- We have already discussed that a timer is introduced in the data link layer.



(a) Sender does not receive acknowledgement



(b) Frame is lost

(G-221)**Fig. 3.8.2 : Timeout and retransmission**

3.8.4 Piggybacking : MU : Dec. 07

University Questions

Q. 1 Describe in brief piggybacking. **(Dec. 07, 4 Marks)**

- 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 :

1. The disadvantage of piggybacking is the additional complexity.
2. If the data link layer waits too long before transmitting acknowledgement, then retransmission of frame would take place.

3.9 Sliding Window Protocols : MU : Dec. 03, May 05, May 07, Dec. 08, Dec. 09

University Questions

Q. 1 Explain stop and wait and sliding window protocol. **(Dec. 03, 10 Marks)**

Q. 2 Explain stop and wait and sliding window protocols with suitable examples. **(May 05, May 07, Dec. 08, Dec. 09, 10 Marks)**

- The next three protocols are more robust and bi-directional protocols.
- All these protocols are special type of protocol called **Sliding Window Protocols.**
- They show a different performance in terms of their efficiency, complexity and buffer requirements.

Sequence number :

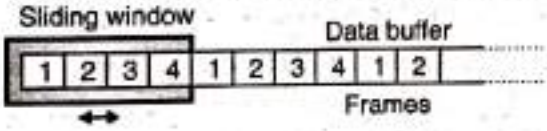
- One of the important features of all the sliding window protocols is that each outbound frame contains a sequence number, ranging from 0 to some maximum value. The maximum value is generally equal to $(2^n - 1)$.
- The value of n can be arbitrary.

Sliding windows :

- Sliding windows are basically the imaginary boxes at the transmitter and receiver.

Scanned by CamScanner

- 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. 3.9.1(a).

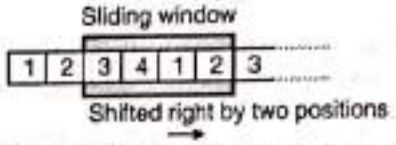


(G-222)**Fig. 3.9.1(a) : Sliding window**

- In Fig. 3.9.1(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. 3.9.1(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. 3.9.1(b) and sends 5th and 6th frames (i.e. frames 1 and 2 of the next lot).

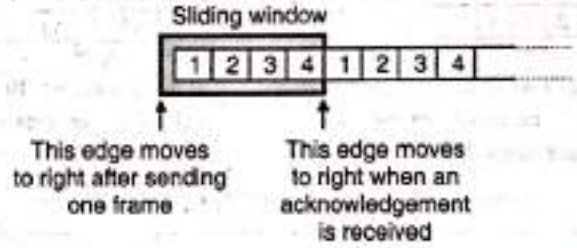


(G-223)**Fig. 3.9.1(b) : Illustration of sliding window mechanism**

- 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 staring 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 carriers 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 the takes this data.

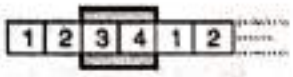
Movement of sender's window :

- Fig. 3.9.1(c) shows the sender's window.



(G-224)**Fig. 3.9.1(c) : Sender sliding window**

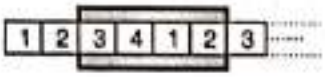
- If the senders window size is 4 and frames 1 and 2 are sent but acknowledgement has not been received so far, then as shown in Fig. 3.9.1(d), the sender's windows will only contain two frames i.e. 3 and 4.



(G-225)**Fig. 3.9.1(d) : Sender's window after sending first two frames but no acknowledgement**

Scanned by CamScanner

- Now if the sender receives acknowledgement bearing number 3 then it understands that the receiver has correctly received frames 1 and 2.
- The senders window now expands and includes the next two frames as shown in Fig. 3.9.1(e).

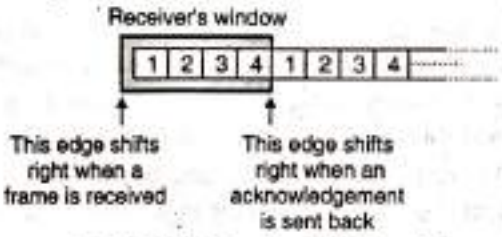


(G-226)**Fig. 3.9.1(e) : Sender's window after receiving acknowledgement bearing number-3**

- In this way the left edge of senders window will shift right when the data frames are sent and the right edge of the senders window will shift right when the acknowledgement is received.

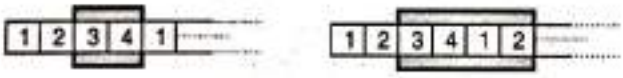
Movement of receiver's windows :

- Fig. 3.9.1(f) shows the receiver's window. Its left edge shifts right on receiving each data frame, where as its right edge shifts right when an acknowledgement is sent.



(G-227)**Fig. 3.9.1(f) : Receiver's sliding window**

- If we take the same example that we discussed for the sender's window then the position of receivers windows are as shown in Fig. 3.9.1(g) and (h).



(g) Two frames (1 and 2) received but no acknowledgement sent **(h) After sending the acknowledgement**

(G-228)**Fig. 3.9.1 : Movement of receiver window**

Ex. 3.9.1 : 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 :

1. Before A send any frame.
2. After A send frame 0, 1, 2 and receive ACK (acknowledgement) from B for 0 and 1.

Soln. :

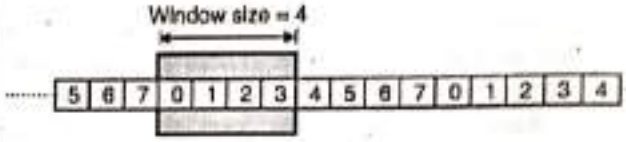
- The number of sequence number bits = m = 3.

  ∴ The sequence numbers will be 0, 1, 2, 3 ...., 6, 7. We can repeat these numbers. So the sequence will be,

  0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, ...

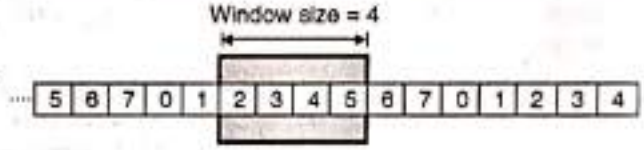
- The size of the window is 4.

Fig. P. 3.9.1(a) shows the sender window (at A) before sending any frame.



(G-229) **Fig. P. 3.9.1(a) : Before A sends any frame**

Fig. P. 3.9.1(b) shows that the window slides 2 positions because acknowledgement for frames 0 and 1 have been received.



(G-230) **Fig. P. 3.9.1(b) : After sliding two frames**

Ex. 3.9.2 : 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. :

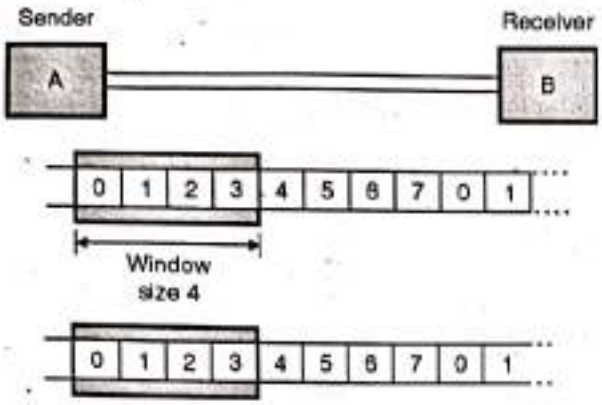
- The number of sequence bits = m = 3.

  ∴ 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. 3.9.2.

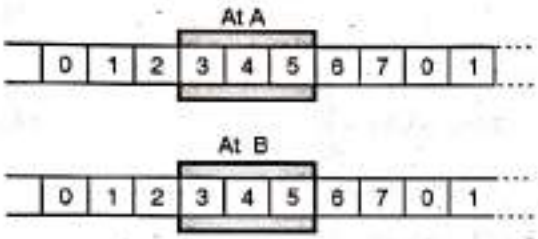
Scanned by CamScanner

Case 1 : Initial position :



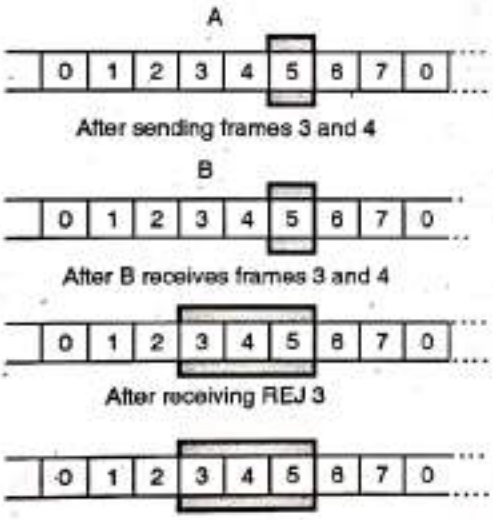
(G-231) **Fig. P. 3.9.2(a)**

Case 2 : After A sends frames 0, 1, 2 and B acknowledge 0, 1 :



(G-232) **Fig. P. 3.9.2(b)**

Case 3 : A sends frames 3 and 4 and then receives REJ 3 from B :



(G-233) **Fig. P. 3.9.2(c)**

3.9.1 A One Bit Sliding Window Protocol (Stop and Wait ARQ) :

MU : May 04, May 05, Dec. 05, May 10

University Questions

Q. 1 Explain a one - bit sliding window protocol in detail. **(May 04, May 10, 10 Marks)**

Q. 2 Explain stop and wait and sliding window protocol with example and suitable diagrams. **(May 05, 10 Marks)**

Q. 3 Explain n-bit sliding window protocol. **(Dec. 05, 6 Marks)**

- This protocol is called one bit protocol because the maximum window size here i.e. n is equal to 1.
- It uses the stop-and-wait technique which we have discussed earlier. The sender sends one frame and waits to get its acknowledgement.
- The sender transmits its next frame only after receiving the acknowledgement for the earlier frame.
- So one bit sliding window protocol is also called as **stop and wait protocol.**
- The sequence of events taking place when a frame is transmitted and received is as follows :

1. The data link layer of the sending machine fetches the first packet from its network layer.
2. It builds the frame for it and sends it to receiver.
3. The receiver data link layer checks the received frame for duplication.
4. If ok, it passes the frame to its network layer.

(G-234)

The operation of protocol :

- The operation of this protocol is based on the ARQ (automatic repeat request) principle.
- So the sliding window protocols are also called as ARQ protocols.
- In this method the transmitter transmits one frame of data and waits for an acknowledgement from the receiver.
- If it receives a positive acknowledgement (ACK) it transmits the next frame. If it receives a negative acknowledgement (NAK) it retransmits the same frame.

Features added for retransmission :

For retransmission, four features are added to the basic flow control mechanism.

1. The transmitter stores the copy of last frame transmitted until an acknowledgement for that frame is received from the destination.
2. For distinctly identifying different types of frames both data and ACK frames are numbered alternately 0 and 1. The first data frame sent is numbered as 0. This frame is

Scanned by CamScanner

acknowledged by an ACK 1 frame. After receiving ACK1 the sender sends next data frame having a number 1.

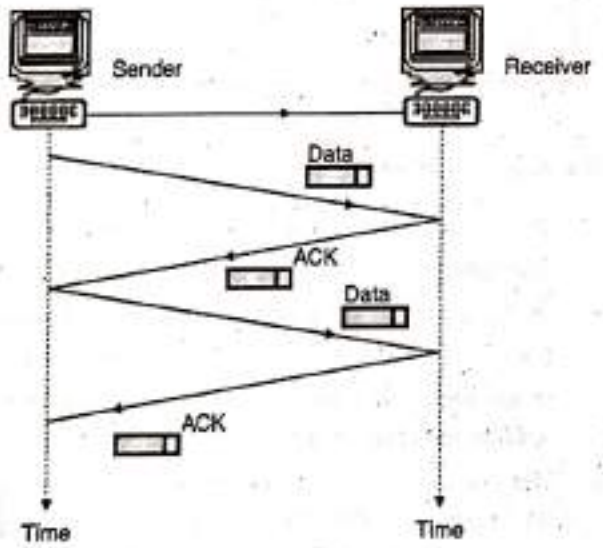
3. If an error occurs while transmission, the receiver sends a NAK frame back to the transmitter for retransmission of the corrupted frame. NAK frames which are not numbered tell the transmitter to retransmit the last frame transmitted.
4. The transmitter has a timer to take care of the frame ACK which are lost. After a specified time if the transmitter does not receive a ACK or NAK frame it retransmits the last frame.

When is the retransmission necessary ?

- The retransmission of frame is essential under the following events :
  1. If the received frame is damaged.
  2. If the transmitted frame is lost.
  3. If the acknowledgement from the receiver is lost.
- Let us see the operation of the protocol under these circumstances one by one.

Operation under normal condition :

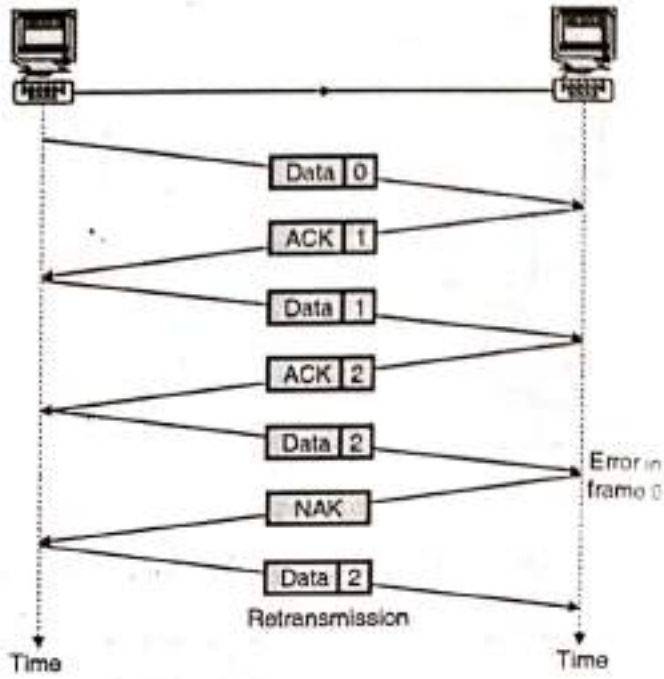
- Fig. 3.9.2 illustrates the protocol operation when everything is normal.
- No frame is lost so retransmission is not necessary.



(G-235)**Fig. 3.9.2 : Stop and wait under normal condition**

Stop and wait ARQ for damaged frame :

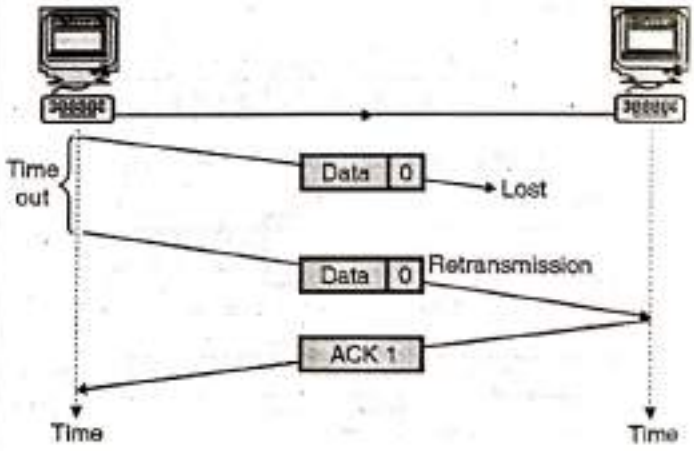
- As seen in Fig. 3.9.3(a) the transmitter transmits data frame numbered 0. The receiver returns an ACK 1 indicating that the data frame numbered 0 is received without any error.
- The next data frame i.e. data 1 is sent. The corresponding acknowledgement ACK2 is received.
- The process goes on in this 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.



(G-236)**Fig. 3.9.3(a) : Stop and wait ARQ damaged frame**

Stop and wait ARQ for lost data frame :

- Fig. 3.9.3(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.



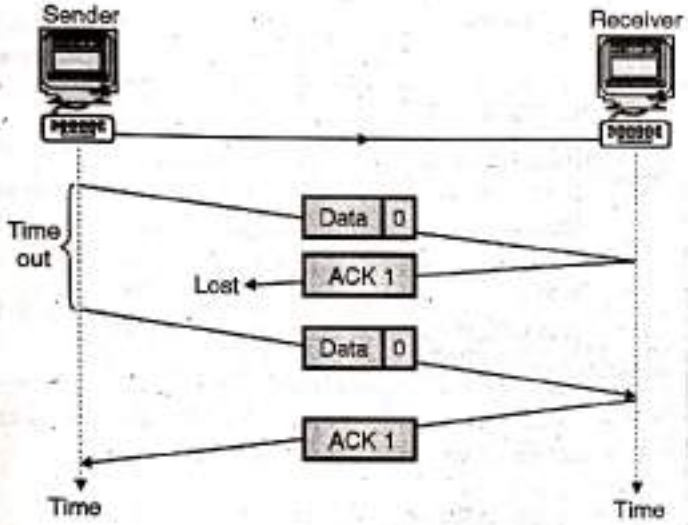
(G-237)**Fig. 3.9.3(b) : Stop and wait ARQ, lost data frame**

Stop and wait ARQ for lost acknowledgement :

- Fig. 3.9.3(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.

Scanned by CamScanner

- 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.



(G-238)**Fig. 3.9.3(c) : Stop and wait ARQ, lost ACK frame**

Note : Stop-and Wait ARQ was used in IBM's Binary Synchronous Communications (Bisync) Protocol. It is also used in Xmodem, a popular file transfer protocol for modem.

Disadvantages of stop and wait protocol :

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.

3.9.2 A Protocol using GO Back n :

MU : Dec. 03, Dec. 04, Dec. 10, May 11, Dec. 11, Dec. 14, May 15, Dec. 17

University Questions

Q. 1 Which protocol Go-Back-N or selective-repeat makes more efficient use of network bandwidth ? Why ? **(Dec. 03, 10 Marks)**

Q. 2 Explain sliding window protocol. Draw the sender and receiver windows for a system using Go-Back-N sliding window system given that :

1. Frame 0 is sent ; Frame 0 is ACK
2. Frames 1 and 2 are sent ; Frames 1 and 2 are ACK.
3. Frames 3, 4, 5 are sent. Frame 4 is ACK. Timer for frame 5 expires.
4. Frames 5, 6, 7 are sent, Frames 4 through 7 are ACK.

(Dec. 04, 10 Marks)

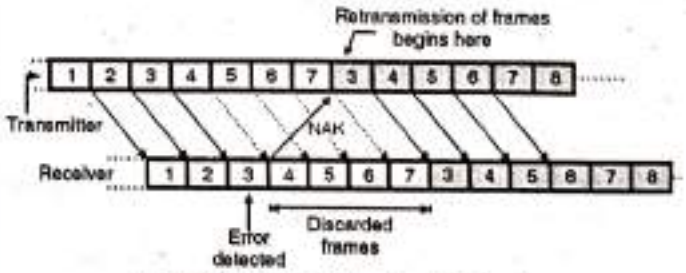
Q. 3 Explain sliding window protocol using go-back N technique. **(Dec. 10, May 11, Dec. 11, May 15, Dec. 17, 10 Marks)**

Q. 4 Why is flow control needed ? What are the mechanisms ? Explain how the Go-Back-N and Selective Repeat ARQ differ from each other. **(Dec. 14, 10 Marks)**

- In this stop and wait protocol it was assumed that the transmission time required for a frame to arrive at the receiver plus the transmission time for the acknowledgement to come back is negligible.
- But in some practical situations, this assumption is not correct.
- In the systems like satellite system the round trip time can be as long as 500 mS (propagation delay). This will reduce the efficiency of the protocol.
- Therefore an improved protocol known as **GO-Back-n ARQ** has been developed.
- It is a method used to overcome the inefficiency of the stop and wait ARQ by allowing the transmitter to continue sending enough frames so that the channel is kept busy while the transmitter waits for acknowledgements.
- In this method if one frame is damaged or lost, all frames are sent since the last frame acknowledged are retransmitted.

Principle of GO-back-n ARQ :

- Refer Fig. 3.9.4 to understand the principle of GO-Back-n ARQ.



(G-239)**Fig. 3.9.4 : Go back n ARQ system**

- The major difference between this and the previous system is that the sender does not wait for ACK signal for the transmission of next frame.

Scanned by CamScanner

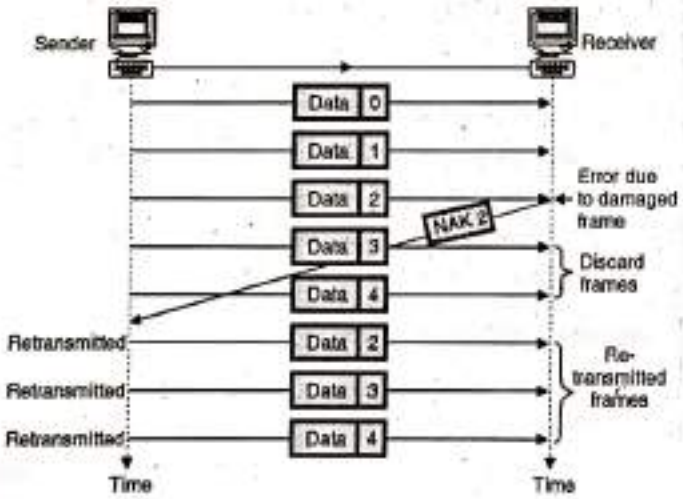
- It transmits the frames continuously as long as it does not receive the "NAK" signal. NAK is the negative acknowledgement signal sent by the receiver to the transmitter.
- When the receiver detects an error in the third frame as shown in Fig. 3.9.4, the receiver sends a NAK signal back to sender.
- 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.

Operation when the frame is lost :

- This condition is illustrated in Fig. 3.9.5(a).

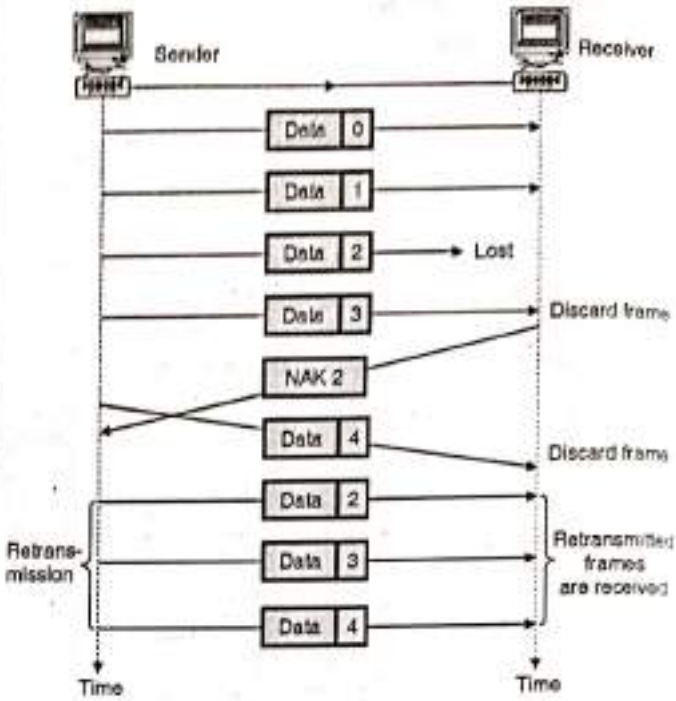


(G-240)**Fig. 3.9.5(a) : Go-back-n, damaged data frame**

- The second data frame is damaged, so the error is detected and receiver send NAK-2 signal back.
- On receiving this signal, the transmitter starts retransmission from frame 2.
- All the frames received after frame 2 are discarded by the receiver.

Operation when a frame is lost :

- As shown in Fig. 3.9.5(b) the case of lost frame is also treated in the same manner as that of the damaged frame.

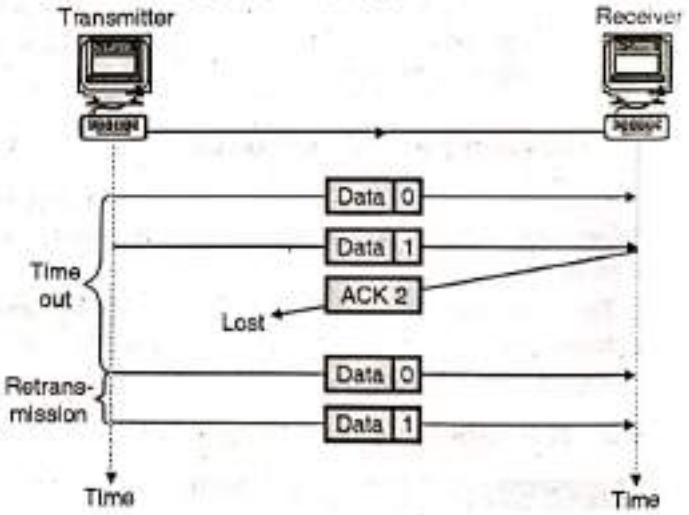


(G-241)**Fig. 3.9.5(b) : Go-back-n, lost data frame**

- The receiver, if it does not receive a particular data frame it sends a NAK to the transmitter and the transmitter retransmits all the frames sent since the last frame acknowledged.

Operation when the acknowledgement is lost :

- Fig. 3.9.5(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.



(G-242)**Fig. 3.9.5(c) : Go-back-n, lost ACK 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.

Scanned by CamScanner

- 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 :

1. It transmits all the frames if one frame is damaged or lost.
2. It transmits frames continuously as long as it does not receive the NAK signal.
3. 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.
4. The error can get introduced if the NAK is lost.

3.9.3 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.

3.9.4 Selective Repeat ARQ :

MU : Dec. 03, May 13, Dec. 14, Dec. 15, May 17

University Questions

Q. 1 Which protocol Go-Back-N or selective-repeat makes more efficient use of network bandwidth ? Why ? **(Dec. 03, 10 Marks)**

Q. 2 Explain sliding windows protocol with selective repeat. **(May 13, 10 Marks)**

Q. 3 Why is flow control needed ? What are the mechanisms ? Explain how the Go-Back-N and Selective Repeat ARQ differ from each other. **(Dec. 14, 10 Marks)**

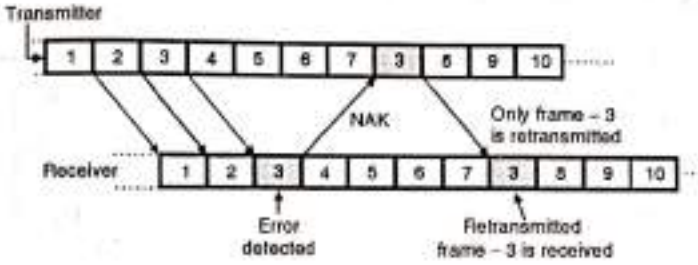
Q. 4 What is the maximum window size allowed for selective repeat ARQ ? Explain why with appropriate scenario. **(Dec. 15, 10 Marks)**

Q. 5 With the help of suitable example explain sliding window protocol with selective repeat. Compare its performance to sliding window with Go-back-n technique. **(May 17, 10 Marks)**

In this method only the specified damaged or lost frame is retransmitted. A selective repeat systems differs from the go-back-n method in the following ways :

1. The receiver can do sorting of data frames and is also able to store frames received after it has sent the NAK until the damaged frame has been replaced.
2. The transmitter has a searching mechanism that allows it to choose only those frames 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. 3.9.6.



(G-243)**Fig. 3.9.6 : Selective repeat ARQ system**

- In this system as well, the transmitter does not wait for the ACK signal for the transmission of the next frame. It transmits the frames continuously till it receives the "NAK" signal from the receiver.
- The receiver sends the "NAK" signal back to the transmitter as soon as it detects an error in the received frame. For example the receiver detects an error in the third frame, as shown in Fig. 3.9.6.
- By the time this "NAK" signal reaches the transmitter, it had transmitted the frames upto 7 as shown in Fig. 3.9.6.
- 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. 3.9.6.
- 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.

Scanned by CamScanner

3.9.5 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 :

$$\eta = \frac{t_f}{t_f + 2t_p} \quad \text{...(3.9.1)}$$

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.

Let $A = t_p / t_f$

$\therefore \quad \eta = 1/(1+2A)$

Propagation time is equal to distance (d) of the link divided by velocity of propagation (v).

$\therefore \quad t_p = d/v$

Transmission time is equal to the length of the frame (bits), divided by rate R.

$\therefore \quad t_f = L/R$

$\therefore \quad A = \frac{d/v}{L/R} = \frac{Rd}{Lv}$

3.9.6 Comparison of Sliding Window Protocols : MU : May 17

University Questions

Q. 1 With the help of suitable example explain sliding window protocol with selective repeat. Compare its performance to sliding window with Go-back-n technique. **(May 17, 10 Marks)**

Table 3.9.1 : Comparison of sliding window protocols

Sr. No.	Parameter	Stop and wait	Go back n ARQ	Selective repeat ARQ
1.	Window size	1.	Sending window size : $(2^m - 1)$	Sending window size : 2^{m-1}
2.	Operating principle	Transmits one frame at a time and waits for its ACK signal. Transmits the next frame only if ACK is obtained.	It transmits frames continuously till it receives the NAK signal.	Same as Go back n protocol.
3.	Communication type (Direction wise).	Communication is one way (simplex) for the data frames though the ACK frames are allowed to travel in the opposite direction.	Communication is one way (simplex) for the data frames though the NAK frames are allowed to travel in the opposite direction.	Same as Go back n protocol
4.	Retransmission takes place if	1. Received frame is damaged. 2. Transmitted frame is lost 3. ACK is lost	1. Received frame is damaged. 2. Transmitted frame is lost. 3. NAK is lost.	Same as Go back n protocol

Scanned by CamScanner

Sr. No.	Parameter	Stop and wait	Go back n ARQ	Selective repeat ARQ
5.	Retransmission	Only the damaged or lost frame is retransmitted.	On reception of the NAK signal, the transmitter retransmits all the frames from the one for which the NAK is obtained.	On reception of NAK, only the damaged or lost frame is retransmitted.
6.	Principle of pipelining.	Not used	Used	Used.
7.	Efficiency	Least efficient and slow	Moderately efficient due to pipelining	Most efficient due to pipelining.
8.	Complexity	Less complex	Moderately complex.	Highly complex.

Ex. 3.9.3 : 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. :

$$t_f = \frac{\text{Frame size}}{\text{Bit rate}} = \frac{4800}{9600} = 0.5 \text{ sec}$$

$$t_p = \frac{2000}{200000} = 0.01 \text{ sec}$$

We know, $A = t_p / t_f$

$\therefore$ $A = 0.01 / 0.5 = 0.02$

Since, $\eta = 1 / (1 + 2A) = 1 / (1 + 2 \times 0.02) = 0.96$

$\therefore$ $\% \eta = 96 \%$ ...Ans.

Ex. 3.9.4 : 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 mS, Efficiency $\eta \geq 50$ % i.e. $0.5 \leq \eta \leq 1$

To find : Range of frame size.

Step 1 : **Calculate value of t_f :**

$$\eta = \frac{t_f}{t_f + 2t_p}$$

For $\eta = 0.5$ we get, $0.5 = \dfrac{t_f}{t_f + (2 \times 20 \times 10^{-3})}$

$\therefore 0.5\, t_f + 20 \times 10^{-3} = t_f$

$\therefore t_f = 40 \times 10^{-3}$ sec.

Note that t_f = Transmission time for 1 frame

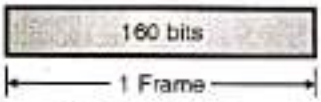
Step 2 : **Calculate the frame size :**

R = Data rate = 4 kbps = 4000 bps

$\therefore N = R \times t_f$

where N = Frame size

$\therefore N = 40 \times 10^{-3} \times 4 \times 10^{3} = 160$ bits ...Ans.



(G-244) **Fig. P. 3.9.4 : 1 frame size**

Ex. 3.9.5 : A channel has a bit rate of 4.8 kbits/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) = ?

$$\text{Efficiency} = \frac{L}{(L + BT)}$$

$$0.5 = \frac{L}{(L + 4.8 \times 10^{3} \times 20 \times 10^{-3})} = \frac{L}{(L + 96)}$$

$0.5\,(L + 96) = L$

$0.5L + 48 = L$

$\therefore L = \dfrac{48}{0.5} = 96$ bits. ...Ans.

Scanned by CamScanner

How to improve the throughput efficiency ?

- If the data signalling rate (R) is increased, then the time taken to transmit each block (B/R) will be reduced.
- However as delay remains unchanged, the throughput efficiency will decrease.
- To compensate for this it will be necessary to use longer blocks for higher data rates (R).
- Longer blocks however will have a greater probability of error, therefore an optimum block length is must be obtained for any particular system.
- Throughput efficiency also depends on the type of system used.
- For a half duplex system the transmission efficiency is very poor. An alternative method which gives greater efficiency is to use a continuous mode of transmission instead of block by block transmission.
- In this system the data blocks are transmitted without interruption unless a negative acknowledgement signal (NAK) is received by the transmitting end.
- When NAK is transmitted back to the transmitter it will retransmit the error block. The continuous transmission method avoids the dead time but needs more storage or buffering.

3.10 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 :

1. Asynchronous protocols – treat each character in a bit stream independently.
2. Synchronous protocols – take the whole bit stream and divides it into characters of equal size.

3.11 High Level Data Link Control (HDLC) Protocol :

MU : Dec. 07, May 08, May 11, Dec. 13, Dec. 16

University Questions

Q. 1 What is HDLC ? Explain the frame formats of I-frame, U-frame and S-frame. **(Dec. 07, 10 Marks)**

Q. 2 Explain HDLC protocol. **(May 08, Dec. 13, 10 Marks)**

Q. 3 Write short notes on : HDLC. **(May 11, Dec. 16, 5 Marks)**

- The high level data link control (HDLC) protocol was developed by ISO.
- It is the most widely accepted data link layer protocol. It has the advantages of flexibility, adaptability, reliability and efficiency of operation.
- HDLC is a bit oriented data link control protocol, and it is designed to satisfy many of data control requirements.
- For the HDLC protocol the following three types of stations have been defined :
  1. Primary station 2. Secondary station
  3. Combined station

1. Primary station :

A primary station takes care of the data link management. When communication between the primary and secondary stations takes place, the primary station would connect and disconnect the data link. The frames sent by a primary station are called commands.

2. Secondary station :

A secondary station operates under the control of a primary station. When communication between primary and secondary stations takes place, the frames sent by the secondary station takes place are called responses.

3. Combined station :

A combined station can act as primary as well as secondary stations. Therefore it can send both commands and responses.

Operating modes for data transfer :

- In HDLC both synchronous and asynchronous modes of communication are permitted.
- The meaning of the words synchronous and asynchronous is different from that of a physical layer.
- Following modes of operation are possible for data transfer :
  1. Normal response mode (NRM)
  2. Asynchronous response mode (ARM)
  3. Asynchronous balanced mode (ABM)
- The first two modes of operation are suitable for an unbalanced type of data transfer between one primary and the other secondary stations whereas the third one is suitable for a balanced type of data transfer.

Normal Response Mode (NRM) :

This mode is suitable for point-to-point as well as point-to-multipoint configurations. Here the primary station will control the overall data link management. It is a synchronous mode of communication.

Asynchronous Response Mode (ARM) :

- This mode is used for communication between primary and secondary stations. As the name indicates it is an asynchronous mode of communication.
- In ARM the secondary station can transmit response (frame) without taking permission from the primary station.
- This is not allowed in NRM. Therefore NRM is a more disciplined mode than ARM. The responsibility of link management function still lies with the primary station.

Scanned by CamScanner

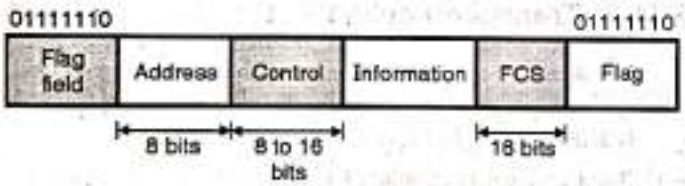
Asynchronous Balanced Mode (ABM) :

- 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.

3.11.1 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. 3.11.1(a) and Fig. 3.11.1(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. 3.11.1(a). It is also used to fill the idle time between consecutive frames.



(a) Information transfer frame

(b) Supervisory and unnumbered frames

(G-250)**Fig. 3.11.1**

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.

3.11.2 Frame Types in HDLC : MU : Dec. 07

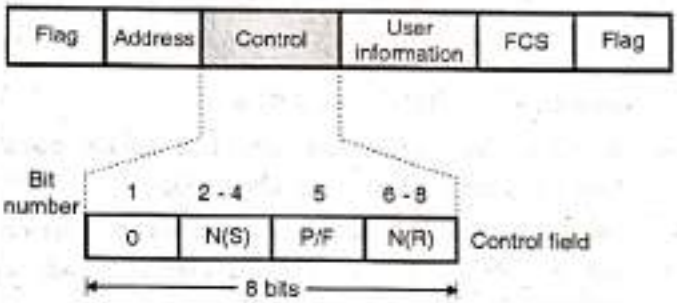
University Questions

Q. 1 What is HDLC ? Explain the frame formats of I-frame, U-frame and S-frame. **(Dec. 07, 10 Marks)**

- There are three types of frames defined in HDLC as follows :
  1. The I-frame or information frame.
  2. The S-frame or supervisory frame.
  3. The U-frame or the unnumbered frame.

The I-frame :

- Fig. 3.11.2 shows the format of the information frame or I-frame.



(G-251)**Fig. 3.11.2 : I-frame format**

- It is supposed to carry the user data from the network layer. It is also possible to include the flow and error control information which is also called piggybacking.

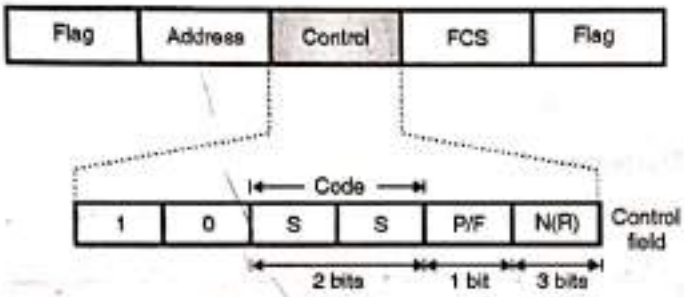
Explanation :

- Concentrate on the control field of the I-frame.
- As shown in the Fig. 3.11.2 if the first bit in the control field is 0 it is identified as an information frame (I-frame).
- The next three bits (2 to 4) are called N (S) and their job is to define the sequence number of the frame.
- Since there are only 3 bits, we can define only eight combinations ($2^3 = 8$). Therefore a sequence number is between 0 and 7 only.
- The value of N(S) field corresponds to the value of control variable S as discussed for the three ARQ mechanisms.
- The next bit (5th) is the poll/final (P/F) bit. It can have two possible values 0 or 1 out of which only the logical 1 is meaningful. Logic 0 in this position has no meaning.
- When P/F = 1, it means poll when a frame is sent by a primary station to secondary. .
- When P/F = 1, it means final when a frame is sent by a secondary station to primary.
- The last three bits (6 to 8) define the N(R) field. It is used for piggybacking. The 3 bits in the N(R) field will represent the value of ACK when piggybacking is used.

Scanned by CamScanner

The S-Frames :

- Fig. 3.11.3 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.

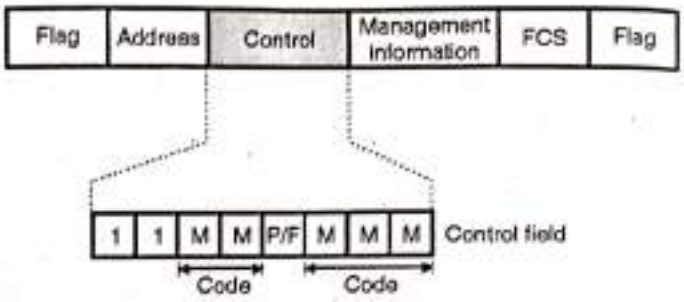


(G-252)**Fig. 3.11.3 : S-frame format**

- 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. 3.11.3.
- The next two bits define the code field marked SS. There are four possible combinations of these bits. They indicate different types of S-frames.
- There are 4 types of supervisory frames corresponding to the four possible value of the S bits in the control field.
  1. SS = 00 → corresponds to receive ready (RR) frames which are used to acknowledge frames when no I frames are available to piggyback the acknowledgement.
  2. SS = 01 → corresponds to Reject (REJ) frames which are used by the receiver to send a NAK when error has occurred.
  3. SS = 10 → corresponds to a Receive Not Ready (RNR) frame and it is used for flow control.
  4. SS = 11 → corresponds to a Selective Repeat Frame which indicates to the transmitter that it should retransmit the frame indicated in the N(R) subfield.
- The fifth bit in the control field is P/F bit the function of which is as discussed earlier, and the next 3 bits called N(R) correspond to the ACK or NAK value.

U-frames :

- The format of U-frame i.e. the unnumbered frame is shown in Fig. 3.11.4.
- These frames are used for exchanging the session management and control information between the communicating devices.



(G-253)**Fig. 3.11.4 : Format of U-frame**

- A 11 in the first two bits of the control field identifies an unnumbered (U) frame as shown in Fig. 3.11.4.
- 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. 3.11.4) are divided into two sections. Two bits before P/F bit and three bits after the P/F bits.
- These five code bits can create upto $2^5 = 32$ different types of U-frames.
- The unnumbered frame types are used for functions such as initialization, status reporting and resetting.
- The Information frame and supervisory frames implement the error and flow control functions of the data link layer.
- The combination of the I-frames and supervisory frames allows HDLC to implement stop-and-wait, Go-back-n and selective repeat ARQ.

3.11.3 Transparency in HDLC :

- The data field of HDLC frame is capable of carrying text and non-text information. The examples of non-text information is audio, video, graphics etc.
- But a problem is introduced for some message types during the transmission.
- If the data field of an HDLC frame contains the pattern 01111110 which is reserved for the flag field, then the receiver will treat that sequence as the end flag.
- Naturally the remaining bits are interpreted as the bits from next frame.
- This is called as lack of data transparency.

3.11.4 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 (01111110) 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.

Scanned by CamScanner

- 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.

3.12 Why Is CRC In Data Link Protocols In Trailer and not in Header ?

MU : May 15

University Questions

Q. 1 Why does the data link protocol always put the CRC in a trailer rather than in a header ? **(May 15, 4 Marks)**

- 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.

3.13 Solved Examples :

Ex. 3.13.1 : 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 kbps = 64×10^3 bps.
Frame size N = 512 bytes = 512×8 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,

$$t_f = \frac{\text{Frame size}}{\text{Bit rate}} = \frac{N}{R} = \frac{512 \times 8}{64 \times 10^3}$$

$$\therefore \quad t_f = 64 \times 10^{-3} \text{ sec}$$

Step 2 : **Calculate A :**

$$A = \frac{t_p}{t_f}$$

But t_p = Propagation delay = 270 mS for satellite channel

$$\therefore \quad A = \frac{270 \times 10^{-3}}{64 \times 10^{-3}} = 4.2187$$

Step 3 : **Maximum throughput :**

$$\eta_{max} = \frac{W}{1 + 2A}$$

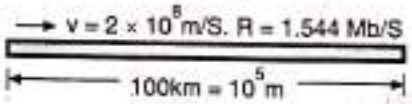
where W = Window size.

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. 3.13.2 : A 100 km long cable runs at T_1 data speed. The propagation speed in cable is 2/3 of the speed of light. How many bits fit in the cable ?

Soln. :

Given : L = 100 km = 1×10^5 m,
Data rate of T_1 = 1.544 Mb/s
Speed v = $2/3 \times 3 \times 10^8$ m/s = 2×10^8 m/s.



(G-262(a)) **Fig. P. 3.13.2**

To find : Number of bits fitting in the cable.

Number of bits in 1 sec. = 1.544×10^6 bits

Distance covered in 1 sec = 2×10^8 m

∴ Number of bits corresponding to 10^5 m cable is given by,

$$X = \frac{1.544 \times 10^6}{2 \times 10^8} \times 10^5 = 772 \text{ bits}$$ **...Ans.**

Ex. 3.13.3 : 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 :

$$t_f = \frac{\text{Frame size}}{\text{Bit rate}} = \frac{1000}{1 \times 10^6} = 1 \times 10^{-3} \text{s i.e. 1 mS.}$$

t_p = 270 mS propagation delay for a satellite channel

Scanned by CamScanner

$$\therefore A = \frac{t_p}{t_f} = \frac{270}{1} = 270$$

$$\therefore \eta = \frac{1}{1+2A} = \frac{1}{1+2(270)} = 1.848 \times 10^{-3}$$

$$= 0.1848\% \quad \text{...Ans.}$$

2. **For continuous ARQ with W = 7 :**

$$\eta = \frac{W}{1+2A} = \frac{7}{1+(2\times 270)} = 1.2936\% \quad \text{...Ans.}$$

3. **Continuous ARQ with W = 127 :**

$$\eta = \frac{127}{1+(2\times 270)} = 23.4696\% \quad \text{...Ans.}$$

Ex. 3.13.4 : Calculate link utilization efficiency for stop-and-wait protocol, if bit rate = 19.2 kbps, Frame size = 960 bits and propagation time = 0.06 sec. for window size = 3 and 7.

Soln. :

Given : Bit rate R = 19.2 kbps $= 19.2 \times 10^3$ bps

Frame size N = 960 bits

Propagation time t_p = 0.06 sec.

Window size W = 3 and 7.

To find : Link utilization efficiency (η).

Step 1 : Calculate t_f :

Transmission time for 1 frame is t_f is given by,

$$t_f = \frac{\text{Frame size (N)}}{\text{Bit rate (R)}}$$

$$= \frac{960}{19.2 \times 10^3}$$

$$\therefore t_f = 0.05 \text{ sec}$$

Step 2 : Calculate A :

$$A = \frac{t_p}{t_f} = \frac{0.06}{0.05} = 1.2$$

Step 3 : Calculate efficiency :

When W = 3,

$$\eta = \frac{W}{1+2A} \quad \text{Where W = Window size}$$

$$\therefore \eta = \frac{3}{1+(2\times 1.2)} = 0.8823 \quad \text{...Ans.}$$

when W = 7

$$\eta = \frac{W}{1+2A}$$

$$\therefore \eta = \frac{7}{1+(2\times 1.2)} = 2.05 \quad \text{...Ans.}$$

Ex. 3.13.5 : 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

$0.5 \le \eta \le 1$

To find : Frame size

Step 1 : Calculate value of t_f :

$$\eta = \frac{t_f}{t_f + 2t_p} \quad \text{where } t_f = \text{Time for one frame}$$

$$\therefore 0.5 = \frac{t_f}{t_f + (2\times 10\times 10^{-3})}$$

$$\therefore t_f = 0.02 \text{ sec}$$

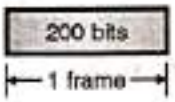
$$\therefore t_f = 20 \text{ msec}$$

Step 2 : Calculate the frame size (N) :

$$R = 10 \text{ kbps} = 10000 \text{ bps}$$

$$\therefore N = R \times t_f = 10\times 10^3 \times 20 \times 10^{-3}$$

$$\therefore N = 200 \text{ bits} \quad \text{...Ans.}$$



(G-263) **Fig. P. 3.13.5**

Ex. 3.13.6 : Imagine the length of a 10Base-5 cable is 2500 meters. If the speed of propagation in a thick co-axial cable is 60% of the speed of light, how long does it take for a bit to travel from the beginning to the end of the cable ? Ignore any propagation delay in the equipment.
(Speed of light = 3×10^8 meters / sec)

Soln. :

Given : L = 2500 m, Speed of propagation V = 60 % of C = 18×10^7 m /sec. C = 3×10^8 meters /sec.

We know that ;

$$\text{number of bits} = \frac{L}{V} = \frac{2500}{18 \times 10^7}$$

$$= 13.9 \ \mu\text{secs.} \quad \text{...Ans.}$$

Scanned by CamScanner

Ex. 3.13.7 : Given the dataword 1010101010 and the divisor 10111.

1. Show the generation of codeword at the sender site (Using binary division).
2. Show the generation of dataword at receiver site (assuming no errors).

Soln. :

Step 1 : Generation of codeword :

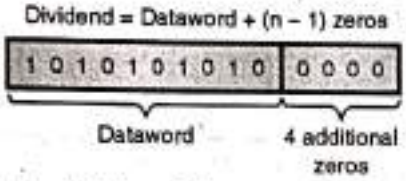
Given : Data word : 1010101010

Divisor : 10111

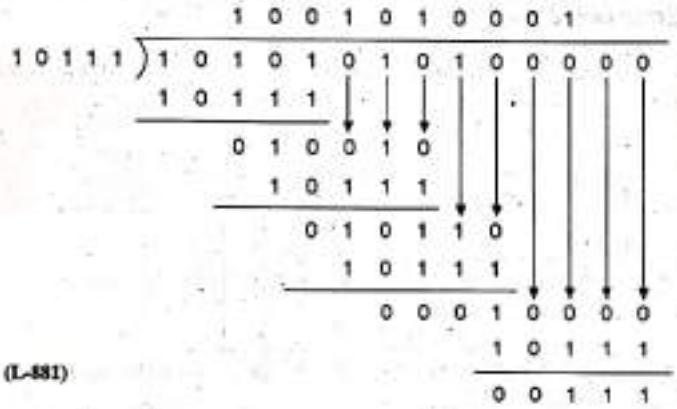
The number of data bits m = 10

The number of bits in the codeword n = 5

(L-883)



Carry out the division as follows :

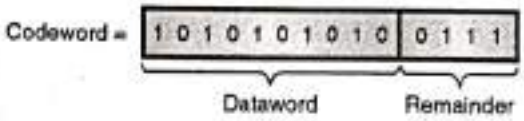


(L-881)

Codeword :

The codeword is given by,

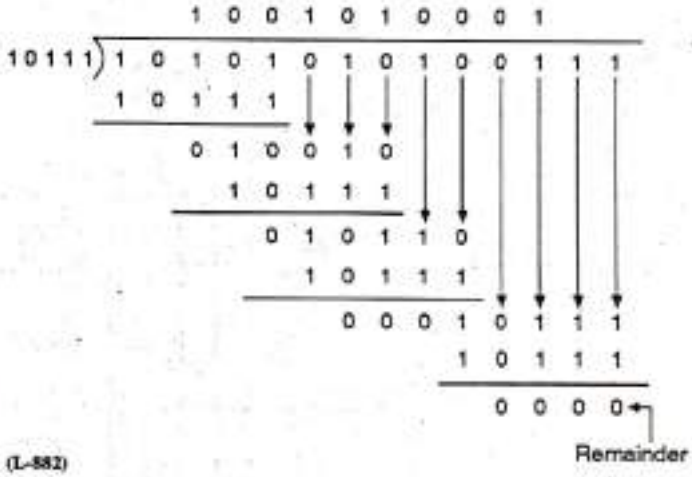
(L-884)



Step 2 : Generation of dataword from the codeword :

Codeword = 1 0 1 0 1 0 1 0 1 0 0 1 1 1

Divisor = 1 0 1 1 1



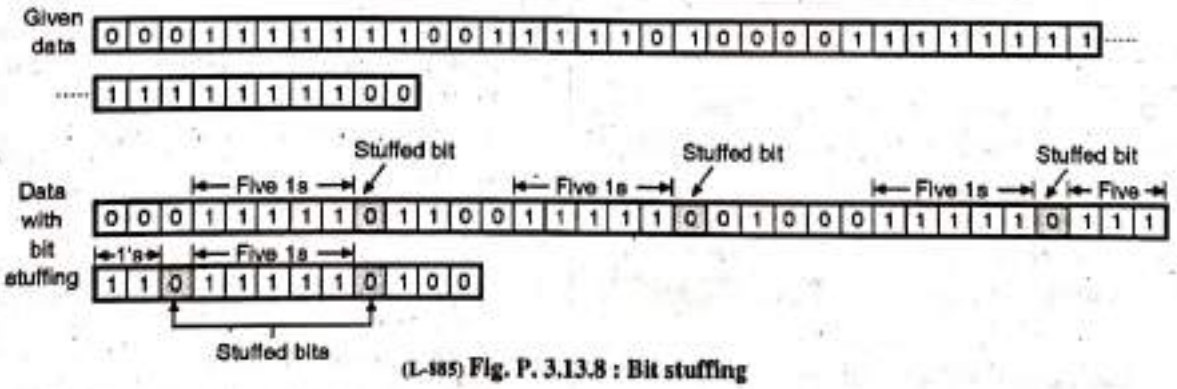
(L-882)

Ex. 3.13.8 : Bit-stuff the following frame payload :

"00011111110011111010000111111111111111100". And discuss limitations of bit stuffing.

Soln. :

– The original and bit stuffed payload are shown in Fig. P. 3.13.8. Note that a zero is inserted after every group of successive 1's.



(L-885) **Fig. P. 3.13.8 : Bit stuffing**

Limitations of bit stuffing :

1. The stuffed bits do not contain any information.
2. Due to bit stuffing, the code rate becomes unpredictable. It becomes dependent on the data being transmitted.

Scanned by CamScanner

Ex. 3.13.9 : Given the data word "101001111" and the divisor "10111", show the generation of cyclic redundancy check (CRC) codeword at the sender site.

Soln. :

Data word : 101001111

Divisor : 10111

The number of data bits = m = 9

The number of bits in codeword = n = 5

Dividend = Dataword + (n – 1) zeros

= 1 0 1 0 0 1 1 1 1 | 0 0 0 0

Dataword | 4 additional zeros

(L-886)

Carry out the division as follows :

```
                0 1 0 0 0 1 1 1 1
1 0 1 1 1 ) 1 0 1 0 0 1 1 1 1 0 0 0 0
            1 0 1 1 1
            -----------
            0 0 0 1 1 1 1 1
                1 0 1 1 1
                -----------
                0 1 0 0 0 1
                  1 0 1 1 1
                  -----------
                  0 0 1 1 0 0 0
                      1 0 1 1 1
                      -----------
                      0 1 1 1 1 0
                        1 0 1 1 1
                        -----------
                        0 1 0 0 1 0
                          1 0 1 1 1
                          -----------
                          0 0 1 0 1 ← Remainder
```

(L-887)

Codeword :

The codeword is given by,

Codeword : 1 0 1 0 0 1 1 1 1 | 0 1 0 1

Dataword | Remainder

(L-888)

Ex. 3.13.10 : Consider a message represented by the polynomial $M(x) = x^5 + x^4 + x$. Consider a generating polynomial $G(x) = x^3 + x^2 + 1$ (1101). Generate a 3 bit CRC and show what will be the transmitted frame. How is error detected by CRC ? **May 17, 10 Marks**

Soln. :

Given : Data word : $x^5 + x^4 + x = 110010$

Generator polynomial : $x^3 + x^2 + 1 = 1101$

Step 1 : Obtain the dividend :

Dividend = Dataword + 3 zeros.

The dividend is as follows :

1 1 0 0 1 0 | 0 0 0

Dataword | 3 zeros

(G-1976)

Step 2 : Carry out the division :

```
          1 0 0 1
1 1 0 1 ) 1 1 0 0 1 0 0 0 0
          1 1 0 1
          -----------
          0 0 0 1 1 0 0
              1 1 0 1
              -----------
              0 0 0 1 0 0 ← Remainder
```

(G-1977)

Step 3 : Obtain the transmitted frame :

Transmitted word = 1 1 0 0 1 0 | 1 0 0

Dataword | Remainder

(G-1978)

Error detection :

At the receiver, this word is divided by the same divider used at the transmitter i.e. 1101.

```
          1 0 0 1
1 1 0 1 ) 1 1 0 0 1 0 1 0 0
          1 1 0 1
          -----------
          0 0 0 1 1 0 1
              1 1 0 1
              -----------
              0 0 0 0 0 ← Remainder
```

(G-1979)

A zero remainder indicates that there is no error in the received codeword.

3.14 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 :
  1. Serial Line Internet Protocol (SLIP)
  2. 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 (OXDB, OXDC) is sent in its place.

Scanned by CamScanner

- If OXDB 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 :
  1. It does not have any error detection or correction facility.
  2. SLIP supports only IP. So it cannot be used over the networks which do not use IP.
  3. 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.
  4. SLIP does not provide any authentication. So neither party knows whom it is talking to.
  5. It is not an approved Internet standard. So many versions exist which makes networking difficult.

3.15 Point-to-Point Protocol (PPP) :

MU : Dec. 09

University Questions

Q. 1 Write short notes on : Point-to-Point Protocol (PPP). **(Dec. 09, 6 Marks)**

- 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.

3.15.1 Services Provided by PPP :

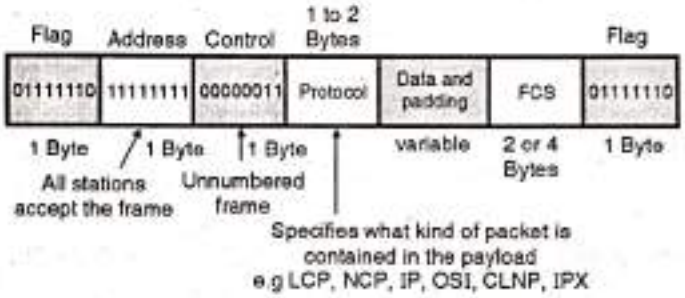
- Following are some of the services provided by PPP :
  1. To define the frame format.
  2. It defines how the link between two devices is to be established and how the data exchange should take place.
  3. It decides the encapsulation of network layer data into the data link frame.
  4. It defines 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).

3.15.2 Frame Format of PPP : MU : Dec. 15

University Questions

Q. 1 Write in brief about : PPP frame format. **(Dec. 15, 5 Marks)**

- The PPP protocol uses an HDLC like frame format as shown in Fig. 3.15.1.



(G-256)**Fig. 3.15.1 : Frame format of PPP**

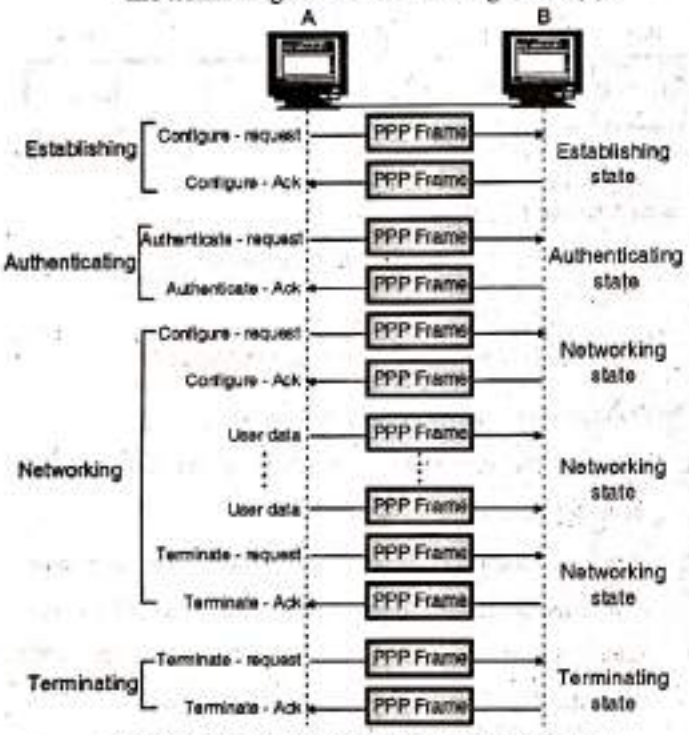
The descriptions of various fields is as follows :

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

Scanned by CamScanner

Protocol (LCP) and the Network Control Protocol (NCP).

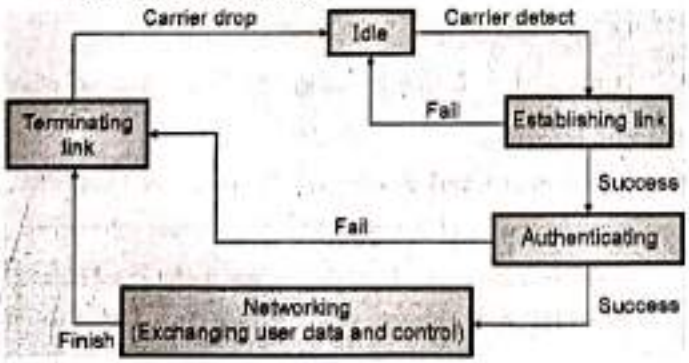
- The Link Control Protocol (LCP) is used to carry out various tasks such as to set-up, configure, test, maintain and terminate a link connection.
- After authentication has been completed a Network Control Protocol (NCP) is used.
- The NCP consists of multiple control protocols. It help in the encapsulation 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. 3.15.2(a).



(G-257)Fig. 3.15.2(a) : States of PPP connection

3.15.3 Transition Phases :

- The PPP connection goes through different phases. These states and their interrelation is shown in the transition state diagram of Fig. 3.15.2(b).



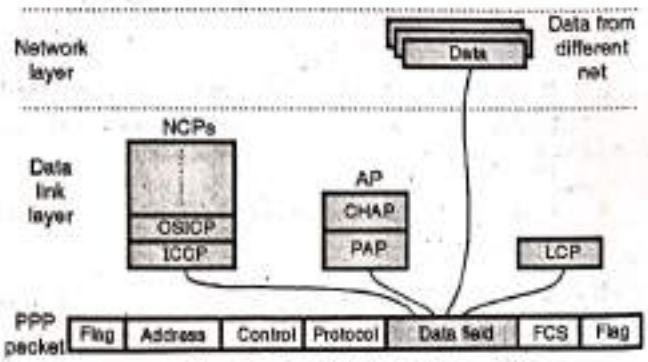
(G-258)Fig. 3.15.2(b) : Flow diagram for PPP connection

Figs. 3.15.2(a) and (b) shows the following states of a PPP connection :

1. **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.
2. **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.
3. **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.
4. **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.
5. **Terminating :** The user sends the terminate packet to terminate the link. With the reception of the terminate Ack packet, the link in terminated.

3.15.4 Multiplexing :

- PPP is a data link layer protocol. However it uses a set of other protocols in order to carry out the following operations .
  1. Link-establishment
  2. Authenticating the involved parties
  3. Carry the network layer data.
- Following three sets of protocols are defined to make the PPP more powerful in its operation :
  1. The Link Control Protocol (LCP)
  2. Two Authentication Protocols. (APs)
  3. Many Network Control Protocols (NCPs).
- As shown in Fig. 3.15.3, 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-259)Fig. 3.15.3 : Multiplexing in PPP

Scanned by CamScanner

3.15.5 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. 3.15.4 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.

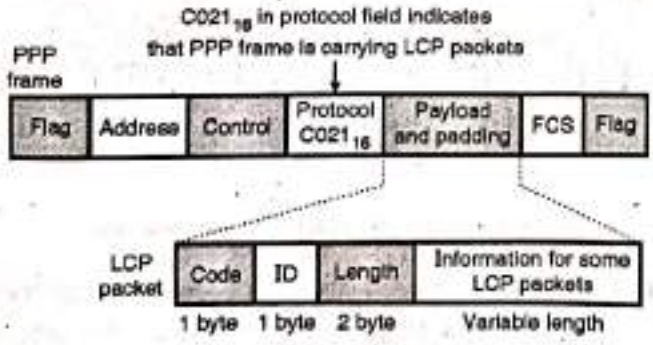
(G-260) **Fig. 3.15.4 : Protocol stack**

3.15.6 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.

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. 3.15.5.



(G-261) **Fig. 3.15.5 : LCP packet**

- Various fields in LCP packet are as follows :
  1. **Code :** It is a one byte length field which defines the type of LCP packet.
  2. **ID :** It is a one byte length field which holds a value used for matching a request with the reply.
  3. **Length :** It is a two byte long field which is used for defining the length of entire LCP packet.
  4. **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 :
  1. Configuration packets
  2. Link termination packets
  3. Link monitoring and debugging packets.

3.15.7 Authentication Protocols :

- Meaning of authentication is to validitate 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.

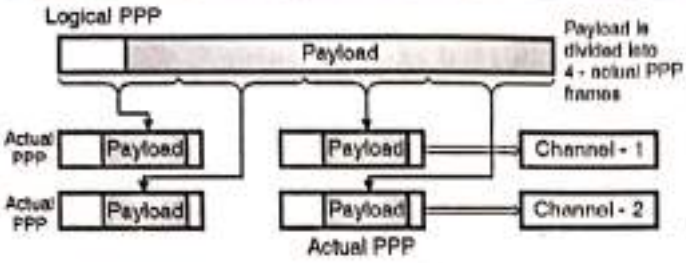
3.15.8 Network Control Protocol (NCP) :

- 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.

3.15.9 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. 3.15.6.

Scanned by CamScanner



(G-262)Fig. 3.15.6

3.15.10 Difference between SLIP and PPP :

Sr. 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.

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 ?

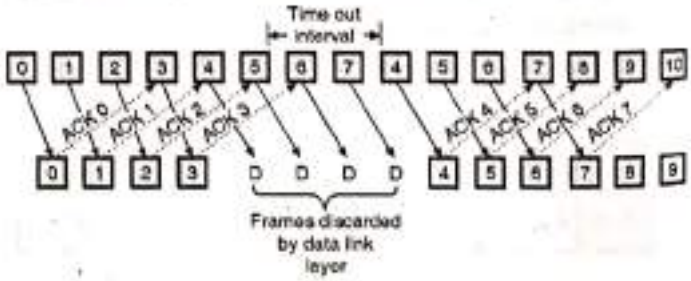
3.16 University Questions and Answers :

Q. 1 Explain sliding window protocol. Draw the sender and receiver windows for a system using Go-Back-N sliding window system given that

1. Frame 0 is sent ; Frame 0 is ACK
2. Frames 1 and 2 are sent ; Frames 1 and 2 are ACK.
3. Frames 3, 4, 5 are sent. Frame 4 is ACK. Timer for frame 5 expires.
4. Frames 5, 6, 7 are sent, Frames 4 through 7 are ACK. **(Dec. 2004, Dec. 2013, 10 Marks)**

Ans. :

Refer section 3.9 for sliding window protocol.



(G-303) Fig. 1 : Go-Back-N sliding window

Q. 2 What are the advantages of a variable length frame over fixed length frames ? Explain the different framing methods. **(May 2012, May 2013, 10 Marks)**

Scanned by CamScanner

Ans. :

For different framing methods refer sections 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5 and 3.4.6

- The data link layer packs bits into frames so that each frame is distinguishable from the other frames.
- Framing can be of two different types :
  1. Fixed size framing
  2. Variable size framing.
- In the fixed size framing, the frame size is fixed. It is same for all frames. Hence there is no need for defining the boundaries of the frames. This type of framing is used in ATM wide area networks.
- The variable size framing is used in LANs. In this type of framing it is necessary to define the end of a frame and beginning of next frame.

Advantages of variable size framing :

1. Although the whole message could be packed in one big frame, it is not done practically because for large frames the flow and error control becomes inefficient. Also even for a single error the whole message needs to be retransmitted. When the same message is divided into smaller frames, the flow and error control become efficient.
2. In LANs there are more than one senders. The messages sent by them could be of different size. Hence it makes system efficient by keeping frame size variable as it is possible to select an optimum frame size as per requirements.

3.17 University Questions and Answers (New Syllabus) :

Dec. 2018 [Total Marks : 14]

Q. 1 Explain in short different framing methods.

(Sections 3.4.1, 3.4.2, 3.4.3, 3.4.4 and 3.4.5) **(4 Marks)**

Q. 2 Explain the use of TCP timers in detail.

(Section 3.5.1) **(10 Marks)**

❑❑❑

Scanned by CamScanner

CHAPTER 4

Module 3

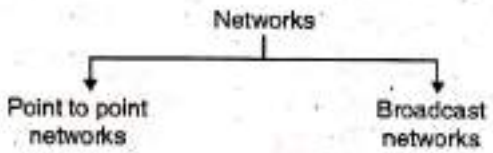
Medium Access Control Layer & LAN

Syllabus :

Channel allocation problem, Multiple access, Protocol (ALOHA, Carrier sense multiple access (CSMA/CD), Local Area Networks - Ethernet (802.3).

4.1 Introduction :

- We can classify the networks into two categories as shown in Fig. 4.1.1.

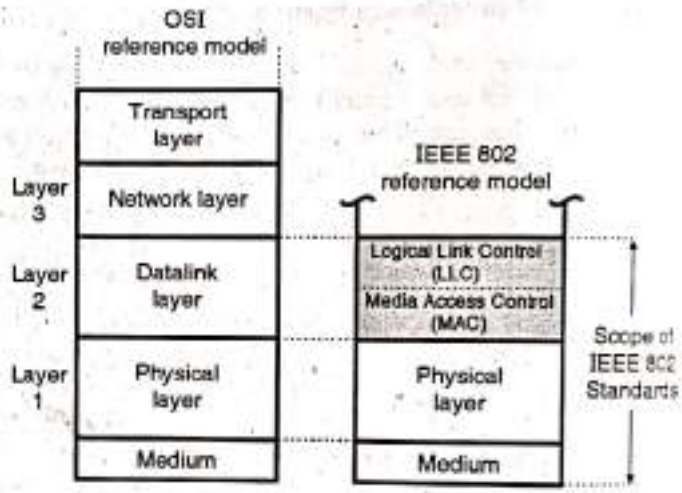


(G-264)**Fig. 4.1.1**

- 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.

4.1.1 MAC and LLC Sublayers :

- Fig. 4.1.2 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. 4.1.2.
- Fig. 4.1.2 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.



(G-265)**Fig. 4.1.2 : IEEE 802 protocol layers compared to OSI model**

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.

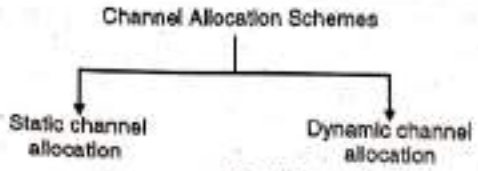
Functions of Logical Link Control (LLC) sublayer :

- Error recovery.
- It performs the flow control operation.
- User addressing.

4.2 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. 4.2.1.

Scanned by CamScanner



(G-266)Fig. 4.2.1

4.2.1 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 or 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.

4.2.2 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 :

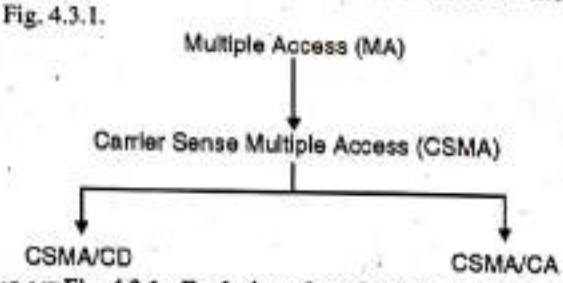
1. Station model – This model consists of N independent stations such as a PC, computer etc. which can generate frames for transmission.
2. Single channel – A single channel is available for all communication.
3. Collision – If frames are transmitted at the same time by two or more stations, there is 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.

4.3 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 :
  1. Random Access
  2. Controlled Access 3. Channelization.
- Let us discuss them one by one.

4.3.1 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. 4.3.1.



(G-267)**Fig. 4.3.1 : Evolution of random access methods**

4.3.2 Evolution of Random Access Methods :

- The first method in the evolution ladder of Fig. 4.3.1, known as ALOHA used a simple procedure called multiple access (MA).

Scanned by CamScanner

- 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.

4.4 Multiple Access (ALOHA System) :

MU : Dec. 06, May 10, Dec. 10, May 11, May 13

University Questions

Q. 1 Write short notes on : ALOHA. **(Dec. 06, 3 Marks)**

Q. 2 Explain ALOHA and Slotted ALOHA in detail. **(May 10, 10 Marks)**

Q. 3 Explain ALOHA in detail. **(Dec. 10, May 11, 5 Marks)**

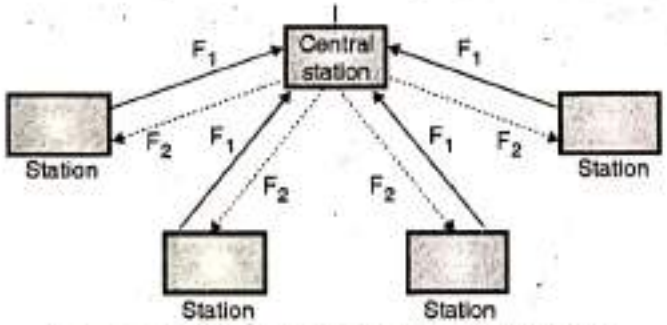
Q. 4 Explain the ALOHA protocol. Compare the performance of pure ALOHA versus slotted ALOHA at low load and high load. **(May 13, 10 Marks)**

ALOHA System :

- Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as Contention systems.
- The ALOHA system is a contention protocol which was developed at the University of Hawaii in the early 1970's by Norman Abramson and his colleagues.
- The ALOHA system has two versions :
  1. Pure ALOHA – Does not require global time synchronisation.
  2. Slotted ALOHA – Requires time synchronisation.

4.4.1 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. 4.4.1, when the central station receives a frame it sends an acknowledgement on a different frequency.



F_1 = Broadcast frequency from the individual stations.

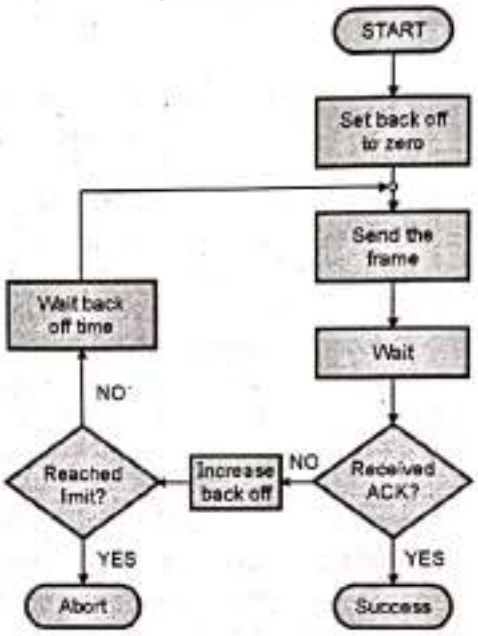
F_2 = Broadcast frequency from the central station.

(G-268)**Fig. 4.4.1 : Pure ALOHA system**

- If a user station receives an acknowledgement it assumes that the transmitted frame was successfully received and if it does get an acknowledgement it assumes that collision had occurred and is ready to retransmit.
- The advantage of pure ALOHA is its simplicity in implementation but it's performance becomes worse as the data traffic on the channel increases.

4.4.2 Protocol Flow Chart for ALOHA :

- Fig. 4.4.2 shows the protocol flow chart for ALOHA.



(G-269)**Fig. 4.4.2 : 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.

Scanned by CamScanner

4.4.3 Efficiency of an ALOHA Channel :

MU : Dec. 04, May 12, Dec. 16

University Questions

Q. 1 Derive the formula for measuring the efficiency of the ALOHA system and explain how the efficiency is increased for slotted ALOHA.

(Dec. 04, 10 Marks)

Q. 2 Derive the efficiency of Pure ALOHA protocol.

(May 12, 10 Marks)

Q. 3 What is the throughput of the system both in pure ALOHA and slotted ALOHA, if the network transmits 200 bit-frames on a shared channel of 200 kbps and the system produces :

(a) 1000 frames per second

(b) 500 frames per second. **(Dec. 16, 10 Marks)**

- Efficiency of an ALOHA system is that fraction of all transmitted frames which escape collisions i.e. which do not get caught in collisions.
- Consider ∞ number of interactive users at their computers (stations). Each user is either typing or waiting. Initially all of them are in the typing state.
- When a user types a line, the user stops and waits. The station then transmits a frame containing this line and checks the channel to confirm the success. If it is successful then the user will start typing again, otherwise the user waits and its frame is retransmitted many time till it is sent successfully.

Frame time :

- Let the frame time be defined as the amount of time required to transmit the standard fixed length frame. Note that

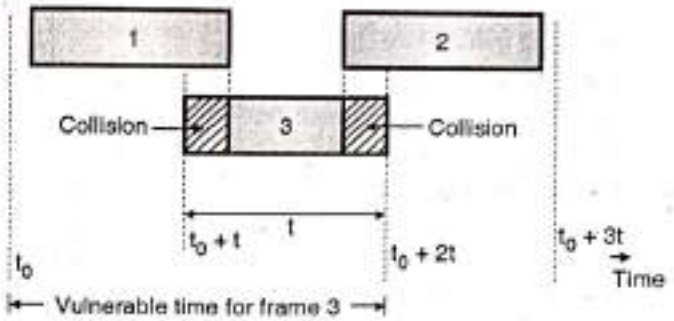
$$\text{Frame time} = \frac{\text{Frame length}}{\text{Bit rate}}$$

- 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 $N = 0$ there will be less number of collisions so less number of retransmissions and $G = N$.
- 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. 4.4.3.



(G-270) **Fig. 4.4.3**

- What is the condition for frame 3 in Fig. 4.4.3 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 $S = G P_0$

$$\therefore \quad S = Ge^{-2G}$$

- Fig. 4.4.5 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.

4.4.4 Slotted ALOHA :

MU : Dec. 07, May 10, Dec. 16

University Questions

Q. 1 Describe in brief : Slotted ALOHA.

(Dec. 07, 5 Marks)

Q. 2 Explain ALOHA and Slotted ALOHA in detail.

(May 10, 10 Marks)

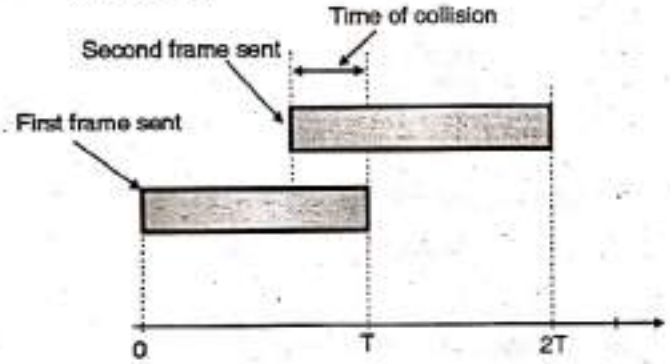
Q. 3 What is the throughput of the system both in pure ALOHA and slotted ALOHA, if the network transmits 200 bit-frames on a shared channel of 200 kbps and the system produces :

(a) 1000 frames per second

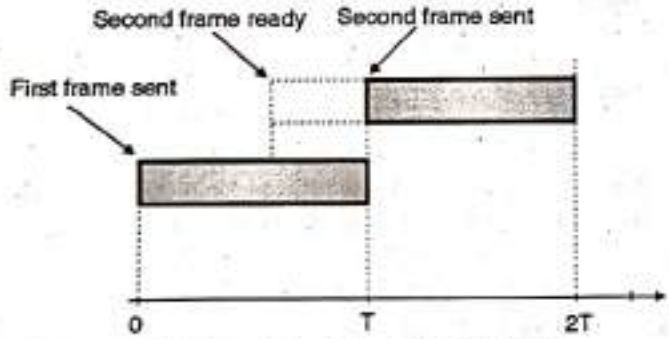
(b) 500 frames per second. **(Dec. 16, 10 Marks)**

Scanned by CamScanner

- 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. 4.4.4. In case of pure ALOHA allowing a station to transmit at arbitrary times can waste time upto 2T.



(a) Transmission using pure ALOHA



(b) Transmission using slotted ALOHA

(G-271)Fig. 4.4.4

- 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. 4.4.4(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. 4.4.5. 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.

4.4.5 Comparison of Pure and Slotted ALOHA : MU : May 13, May 15

University Questions

Q. 1 Explain the ALOHA protocol. Compare the performance of pure ALOHA versus slotted ALOHA at low load and high load. **(May 13, 10 Marks)**

Q. 2 Differentiate between ALOHA and slotted ALOHA. **(May 15, 4 Marks)**

- A mathematical model can be created for the relationship between the number of frames transmitted and the number of frames transmitted successfully.
- Let G represent the traffic measured as the average number of frames generated per slot.
- Let S be the success rate measured as the average number of frames sent successfully per slot.
- The relationship between G and S for both pure and slotted ALOHA is given as follows :

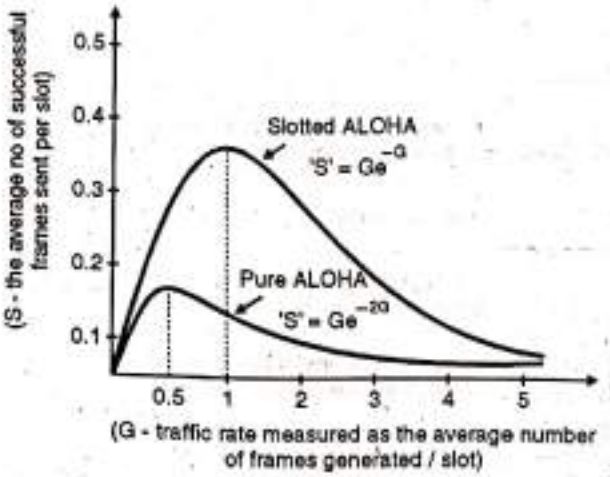
Pure ALOHA → $S = Ge^{-2G}$

Slotted ALOHA → $S = Ge^{-G}$

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. 4.4.5.
- As seen in the Fig. 4.4.5 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.

Scanned by CamScanner



(G-272)**Fig. 4.4.5 : Comparison of pure and slotted ALOHA**

- 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%.
- 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.

4.5 Carrier Sense Multiple Access (CSMA) :

MU : Dec. 04, Dec. 13, Dec. 14, May 15, Dec. 16, Dec. 17, New Syll. : Dec. 18

University Questions

Q. 1 How are collisions handled by a 1-persistant CSMA protocol ? Give an example of a collision-free multiple access protocol and explain it in detail. **(Dec. 04, 10 Marks)**

Q. 2 Explain the different protocols in the MAC sublayer which uses carrier sensing. **(Dec. 13, 10 Marks)**

Q. 3 Explain CSMA protocols. Explain how collisions are handled in CSMA/CD. **(Dec. 14, May 15, Dec. 16, Dec. 17, 10 Marks)**

- The CSMA protocol operates on the principle of carrier sensing. In this protocol, a station listens to see the presence of transmission (carrier) on the cable and decides to act accordingly.

Non-Persistent CSMA :

- In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.
- After this time, it again checks the status of the channel and if the channel is free it will transmit.

1-Persistent CSMA :

- In this scheme the station which wants to transmit, continuously monitors the channel until it is idle and then transmits immediately.
- The disadvantage of this strategy is that if two stations are waiting then they will transmit simultaneously and collision will take place. This will then require retransmission.

P-Persistent CSMA :

- The possibility of such collisions and retransmissions is reduced in the p-persistent CSMA. In this scheme all the waiting stations are not allowed to transmit simultaneously as soon as the channel becomes idle.
- A station is assumed to be transmitting with a probability "p". For example if p = 1/6 and if 6 stations are waiting then on an average only one station will transmit and others will wait.

4.5.1 Carrier Sense Multiple Access/Collision Detection (CSMA/CD) :

MU : Dec. 13, Dec. 14, May 15, Dec. 15, Dec. 16, Dec. 17, New Syll. : Dec. 18

University Questions

Q. 1 Explain the different protocols in the MAC sublayer which uses carrier sensing. **(Dec. 13, 10 Marks)**

Q. 2 Explain CSMA protocols. Explain how collisions are handled in CSMA/CD. **(Dec. 14, May 15, Dec. 16, Dec. 17, 10 Marks)**

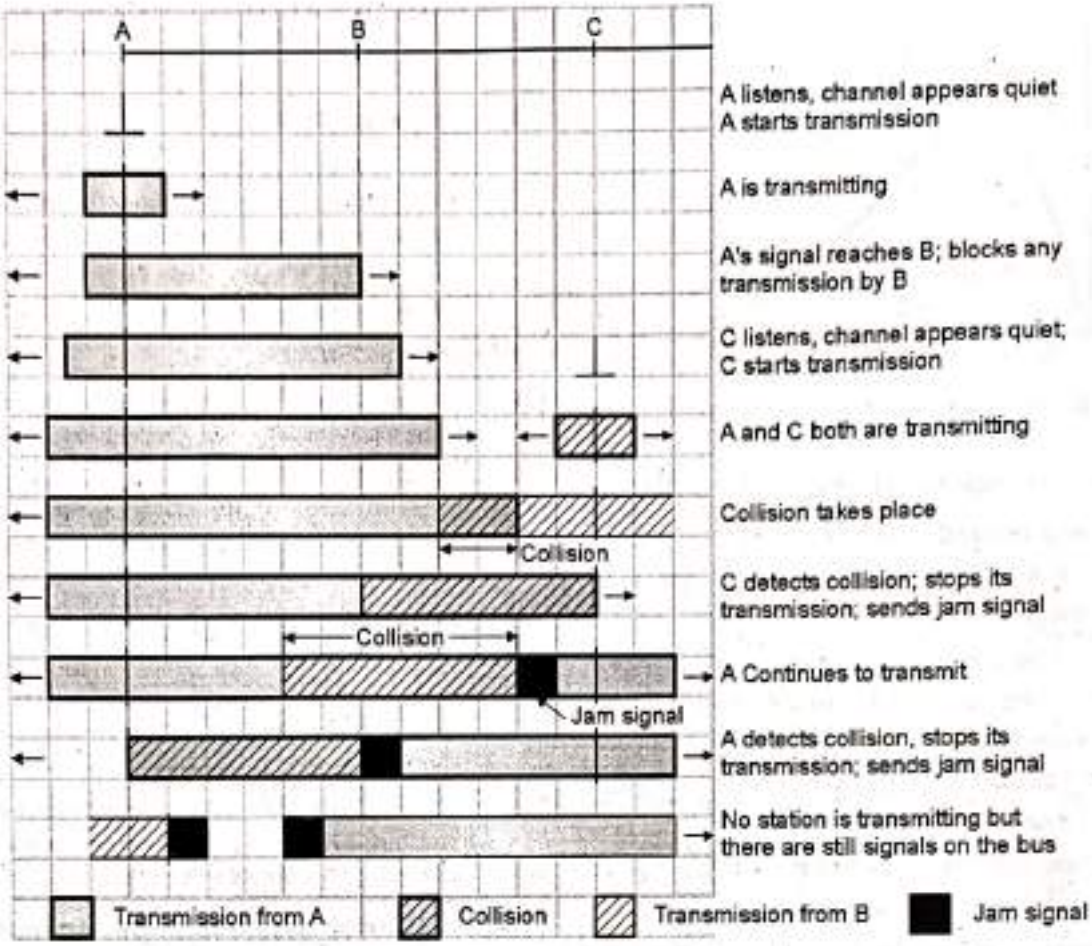
Q. 3 Write in brief about : CSMA/CD **(Dec. 15, 5 Marks)**

The CSMA/CD specifications have been standardized by IEEE 802.3 standard. It is a very widely used MAC protocol.

Media access control :

- The problem in CSMA explained earlier is that a transmitting station continues to transmit its frame even though a collision occurs.
- The channel time is unnecessarily wasted due to this. In CSMA/CD, if a station receives other transmissions when it is transmitting, then a collision can be detected as soon as it occurs and the transmission time can be saved.
- As soon as a collision is detected, the transmitting stations release a jam signal.
- The jam signal will alert the other stations. The stations then are not supposed to transmit immediately after the collision has occurred.

Scanned by CamScanner



(G-273)**Fig. 4.5.1 : CSMA/CD scheme**

- 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. 4.5.1.

4.5.2 CSMA/CD Procedure :

MU : Dec. 14, May 15, Dec. 15, Dec. 16, Dec. 17,

New Syll. : Dec.'18

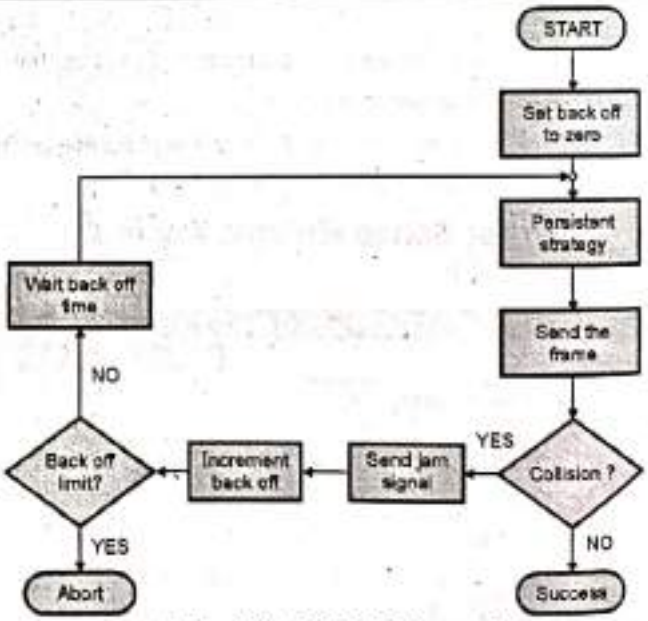
University Questions

Q. 1 Explain CSMA protocols. Explain how collisions are handled in CSMA/CD.

(Dec. 14, May 15, Dec. 16, Dec. 17, 10 Marks)

Q. 2 Write in brief about : CSMA/CD **(Dec. 15, 5 Marks)**

- Fig. 4.5.2 shows a flow chart for the CSMA/CD protocol.



(G-276)**Fig. 4.5.2 : 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.

Scanned by CamScanner

- 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.

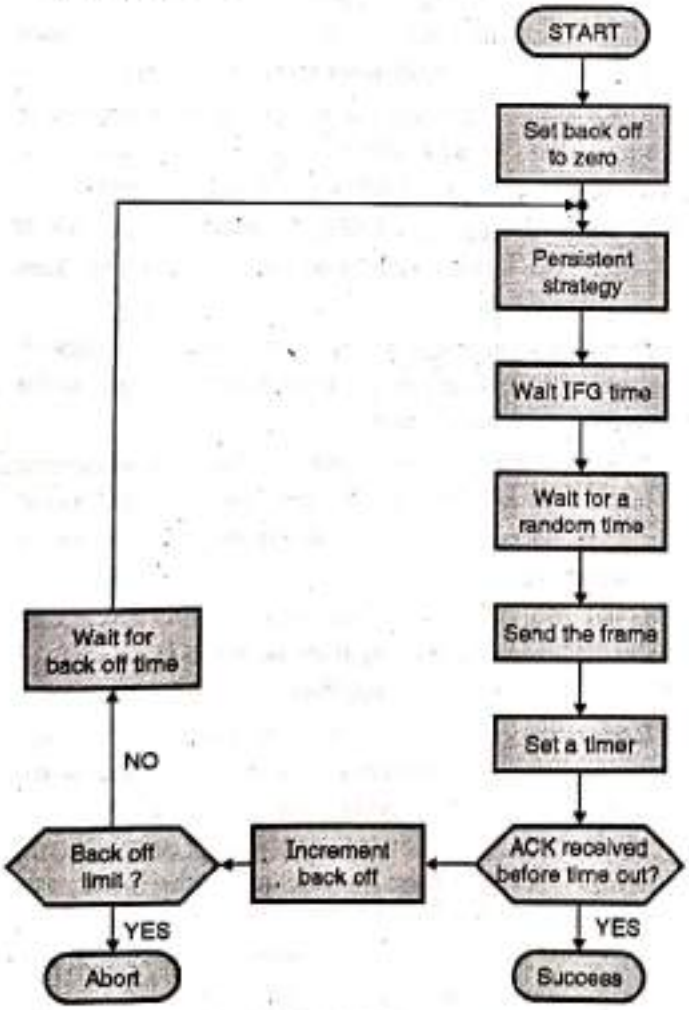
4.5.3 CSMA/CA : MU : Dec. 09, Dec. 13

University Questions

Q. 1 What is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol ? Explain with timing diagram. **(Dec. 09, 10 Marks)**

Q. 2 Explain the different protocols in the MAC sublayer which uses carrier sensing. **(Dec. 13, 10 Marks)**

- The long form of CSMA/CA is CSMA protocol with collision avoidance.
- Fig. 4.5.3 shows the flow chart explaining the principle of CSMA/CA.



(G-277)**Fig. 4.5.3 : CSMA/CA procedure**

- The station ready to transmit, senses the line by using one of the persistent strategies.
- As soon as it find 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.

4.6 Collision Free Protocols : MU : Dec. 04

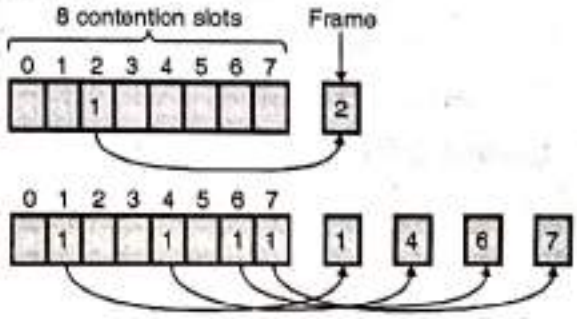
University Questions

Q. 1 How are collisions handled by a 1-persistant CSMA protocol ? Give an example of a collision-free multiple access protocol and explain it in detail. **(Dec. 04, 10 Marks)**

- 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 systems performance adversely. This happens when the cable is long and length of frames are short. This problem becomes serious as fiber optic networks come into use.
- Here we will discuss some protocols that resolve the collisions during the contention period.

4.6.1 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.



(G-278)**Fig. 4.6.1 : A bit-map protocol**

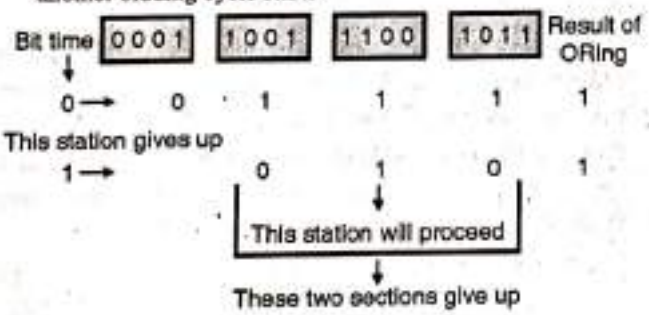
Scanned by CamScanner

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 vary few frames to transmit.
- At high-load, when all the stations have something to send all the time, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame. This indicates that the protocol efficiency is high.
- Generally high numbered stations have to wait half a scan (N/2 bit slots) time before starting to transmit, low-numbered stations have to wait on an average 1.5 N slots.

4.6.2 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 see 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.



(G-279)Fig. 4.6.2 : Binary countdown

4.6.3 Limited Contention Protocols :

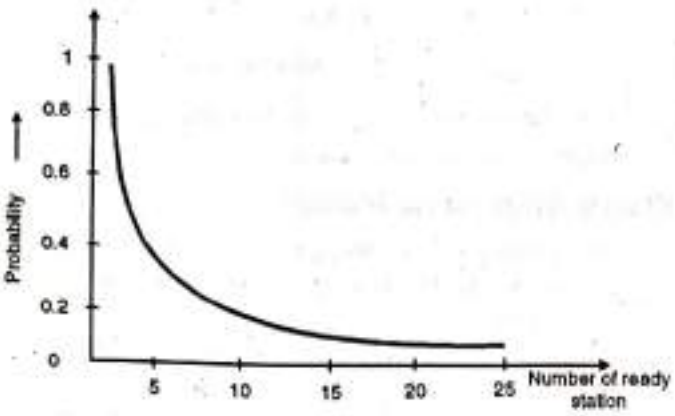
Meaning of contention system :

- 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. 4.6.3 shows the graph of probability plotted against number of stations ready to transmit their frames.

Scanned by CamScanner

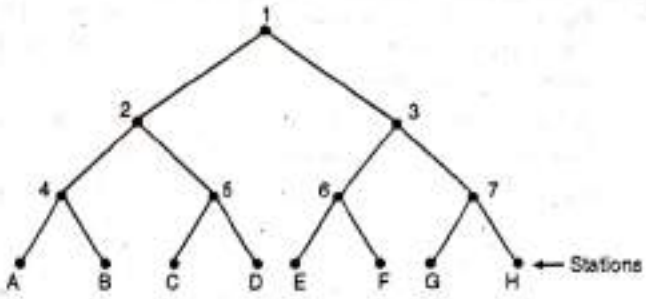


(G-280) Fig. 4.6.3

- 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.

4.6.4 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. 4.6.4.
- The tree for eight stations is shown in Fig. 4.6.4. As shown in the Fig. 4.6.4 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. 4.6.4 : Adaptive tree walk protocol

4.7 Controlled Access : MU : Dec. 15

University Questions

Q. 1 What is controlled access for collision control ? Explain all the methods of controlled access. **(Dec. 15, 10 Marks)**

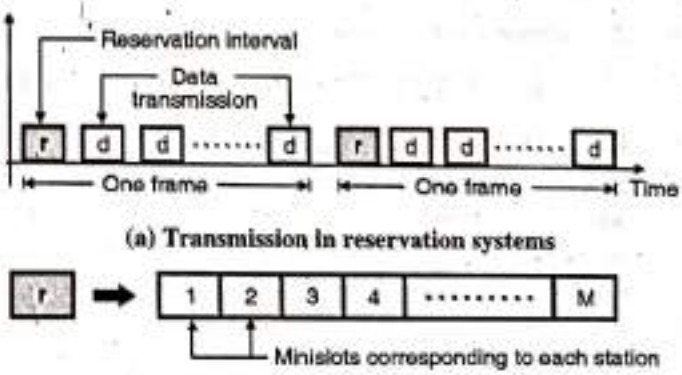
- In the previous section we have discussed the random access approach for sharing a transmission medium.
- The random access approach is simpler to implement and are useful in handling the light traffic.
- In this section we will discuss the scheduling approaches to the medium access control.
- There are three important approaches in the scheduling approach as follows :
  1. Reservation system 2. Polling system
  3. Token passing ring networks.

4.7.1 Reservation Systems : MU : Dec. 15

University Questions

Q. 1 What is controlled access for collision control ? Explain all the methods of controlled access. **(Dec. 15, 10 Marks)**

- The principle of reservation system can be understood from Fig. 4.7.1.
- 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. 4.7.1(a).



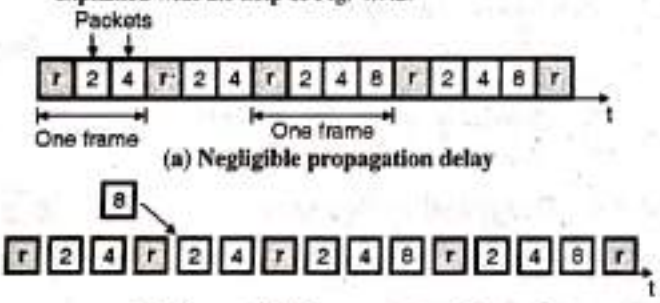
(a) Transmission in reservation systems

(b) Details of reservation interval

(L-733) Fig. 4.7.1 : Basic reservation system

Scanned by CamScanner

- Fig. 4.7.1(b) shows the details of the reservation interval "r". The reservation interval consists of M minislots with one slot allotted to each station.
- These minislots are used by the stations to indicate that they have a packet to transmit in the corresponding frame.
- The station that wants to transmit packet by broadcasting their reservation bit during the appropriate 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. 4.7.2.



(b) Non negligible propagation delay

(L-734)**Fig. 4.7.2 : Operation of reservation system with negligible and non-negligible delays**

- Refer Fig. 4.7.2(a) which shows a system with negligible propagation delay. In the first frame, only the stations 2 and 4 transmit their packets. But in the middle portion, station 8 also wants to transmit its packet. So the frame gets expanded from two slots to three slots.
- The maximum throughput from this system can be attained when all the stations transmit their packet in each frame.
- The corresponding maximum throughput is given by,

$$\rho_{max} = \frac{1}{1+v} \quad \text{...for one packet reservation/minislot}$$

- If $v << 1$ then the value of ρ_{max} can be very high.
- Now refer Fig. 4.7.2(b) which shows a reservation system with some finite non zero propagation delay which can not be neglected. In this system the stations will transmit their reservations in the same way as they used to do before.
- It is possible to modify the basic reservation system so that stations can reserve more than one slot per packet transmission per minislot.
- Let us assume that a minislot can reserve say upto k packets.

Then the maximum achievable throughput is given by,

$$\rho_{max} = \frac{1}{1+(v/k)} \quad \text{...for k packet reservation/minislot}$$

- Note that this value of ρ_{max} will be higher than that for the single packet reservation/minislot.

Effect of number of stations (M) :

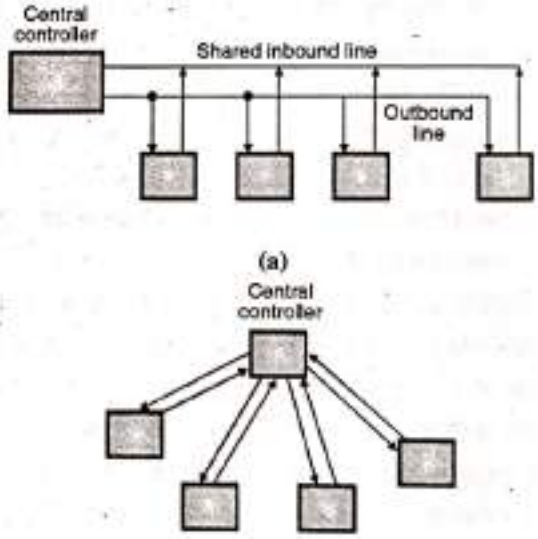
- The reservation intervals introduce overhead which is proportional to M. That means the reservation interval becomes $M \times v$.
- As the number of stations (M) become very large, this overhead will become significant. This then becomes a serious problem.
- This problem can be sorted out by not allocating 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.

4.7.2 Polling : MU : Dec. 15

University Questions

Q. 1 What is controlled access for collision control ? Explain all the methods of controlled access. **(Dec. 15, 10 Marks)**

- Now consider polling system shown in Fig. 4.7.3. In this system the stations access the common medium one by one (by taking turns).
- At any given time only one of the stations will transmit into the medium.



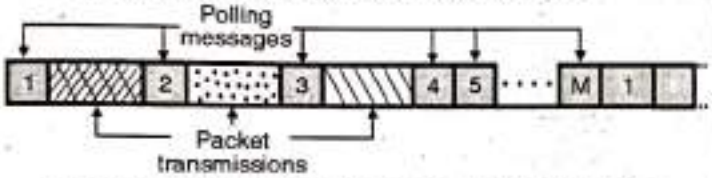
(L-735)**Fig. 4.7.3 : Examples of polling systems**

- When a station finishes its transmitting, then some mechanism is used to pass the right of transmission to another station which wants to transmit next.
- There are different ways of passing the right of transmission from one station to the other station.
- Fig. 4.7.3(a) shows a scheme in which M stations communicate with a central controller. The outbound line is

Scanned by CamScanner

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. 4.7.3(b) shows another system where it is possible to use polling. The central controller of this system can make use of radio transmission.
- Fig. 4.7.4 shows the sequence of polling messages.



(L-736)**Fig. 4.7.4 : Polling messages and transmissions in a polling system**

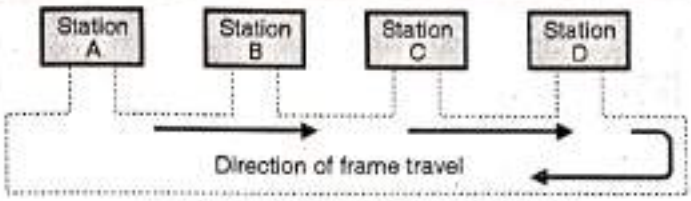
- Station 1 gets the polling message first. The polling message will propagate. It is received by all stations but only station 1 begins transmission. All this process needs a time called **walk time.**
- The next period is occupied by the transmission from station 1.
- This period will then be followed by the walk time corresponding to station-2. This process will continue until all the M stations are polled. Thus in this system the stations are polled in the round robin manner.
- The walk time can be considered to be an overhead in the polling system because it is an unproductive time. The total walk time τ' is the sum of walk time corresponding to each station.

4.7.3 Token Passing : MU : Dec. 15

University Questions

Q. 1 What is controlled access for collision control ? Explain all the methods of controlled access. **(Dec. 15, 10 Marks)**

- Token is a special frame which is used to authorize a particular station for transmission.
- In the token passing method, the token is given to that station, which is authorized to send its data. Thus the station that has the token with it can transmit others listen.



(L-737)**Fig. 4.7.5 : Token passing network**

- In a token passing network, each station has a predecessor and successor as shown in Fig. 4.7.5.
- The frames travel in one direction. They come from the predecessor and go to the successor as shown in Fig. 4.7.5.
- A token frame is circulated around the ring when no data is being transmitted and the line is idle.
- The stations which are ready to send data, will wait for the token. As the token circulates the first ready station in the ring will grab the circulating token and transmit one or more frames.
- This station will keep sending the frames as long as it has frames to send or the allotted time is not complete.
- It then passes this token on the ring from which the next ready to transmit station will grab it.
- This is the simplest possible token passing technique in which all the stations have equal priority or right to send.
- In the practical system, some other features such as priority and reservation are added.

4.8 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.

4.8.1 FDMA : MU : May 12, Dec. 12, May 13

University Questions

Q. 1 Explain FDMA, TDMA and CDMA. **(May 12, Dec. 12, May 13, 10 Marks)**

- 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 is Fig. 4.8.1.
- FDMA is a data link layer protocol which uses FDM at the physical layer.

Scanned by CamScanner

(L-739)Fig. 4.8.1 : Concept of FDMA

- Guard bands are provided in between the adjacent frequency slots. e.g. $(f_1 - f_2)$ is a guard band between the bands allotted to stations 1 and 2. Guard bands avoid the adjacent channel interference.
- FDMA is used in cellular phones and satellite networks.

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 :

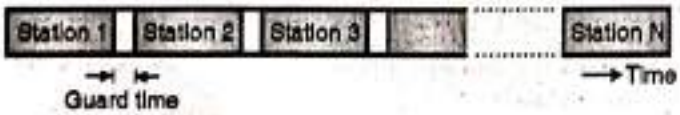
1. Each channel or earth station can use only a part of the total satellite bandwidth.
2. Inspite of guard bands being provided, there is some adjacent channel interference present.
3. As FM is used, it requires larger bandwidth, hence less number of channels will be accommodated in the bandwidth of a satellite.
4. Due to the nonlinearity of companders, the intermodulation products are generated.

4.8.2 TDMA : MU : May 12, Dec. 12, May 13

University Questions

Q. 1 Explain FDMA, TDMA and CDMA.
(May 12, Dec. 12, May 13, 10 Marks)

- 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. 4.8.2 illustrates the concept of TDMA. Guard times are inserted between the adjacent time slots in order to prevent any cross talk. No data transmission takes place during the guard times.



(L-740)Fig. 4.8.2 : Concept of TDMA

- TDMA is a data link layer protocol which uses TDM at the physical layer.
- TDMA finds its application in cellular phones and satellite networks.

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.

4.8.3 Code Division Multiple Access (CDMA) : MU : May 12, Dec. 12, May 13

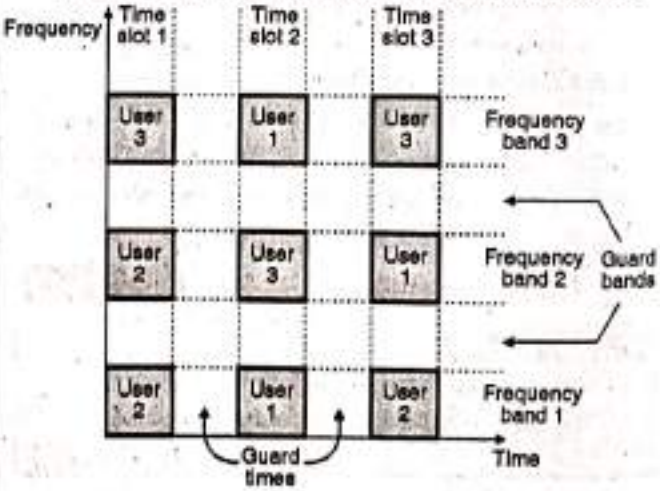
University Questions

Q. 1 Explain FDMA, TDMA and CDMA.
(May 12, Dec. 12, May 13, 10 Marks)

- An alternative to FDMA and TDMA is an 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-741)Fig. 4.8.3 : Structure of CDMA showing the guard bands and the guard times

- In CDMA the users access the channel in a random manner. Hence the signals transmitted by multiple users will completely overlap both in time and in frequency.

Scanned by CamScanner

- 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. 4.8.3.
- CDMA does not need any synchronization, but the code sequences or signature waveforms are required to be used.

4.8.4 Comparison of FDMA, TDMA and CDMA :

Sr. 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 required.	Code word is not required	Code words are required.
5.	Guard bands between adjacent channels are necessary.	Guard times between adjacent time slots are necessary.	Guard bands and Guard times both are necessary.

4.9 Ethernet : MU : Dec. 14

University Questions

Q. 1 Give short notes on : Ethernet (Dec. 14, 5 Marks)

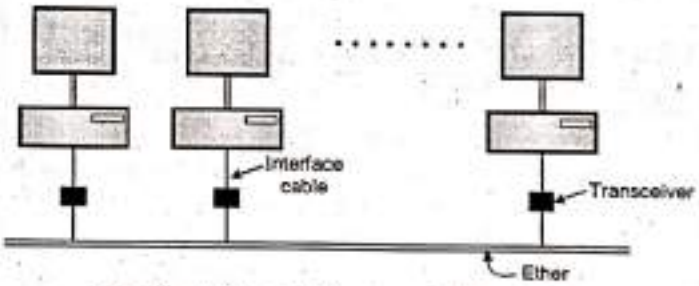
- Both Internet and ATM were designed for wide area networking. But in many applications, a large number of computers are to be connected to each other.
- For this the local area network (LAN) was introduced. The most popular LAN is called Ethernet.
- The IEEE 802.3 standard is popularly called as Ethernet. It is a bus based broadcast network with decentralized control.
- It can operate at 10 Mbps or 100 Mbps or even above 1 Gbps.
- Computers on an Ethernet can transmit whenever they want to do so. If two or more machines transmit simultaneously, then their packets collide.
- Then the transmitting computers just wait for an arbitrary time and retransmit their signal.
- There are various technologies available in the LAN market but the most popular one of them is **Ethernet.**
- In this section we are going to discuss three generations of Ethernet :
  1. Traditional Ethernet (10 Mbps)
  2. Fast Ethernet (100 Mbps)
  3. Gigabit Ethernet (1000 Mbps)
- 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. 4.9.1.



(G-293) **Fig. 4.9.1 : 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).

Scanned by CamScanner

- 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.

4.9.1 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 fall, 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.

4.9.2 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.

4.9.3 Switched Ethernet : MU : Dec. 10, Dec. 13

University Questions

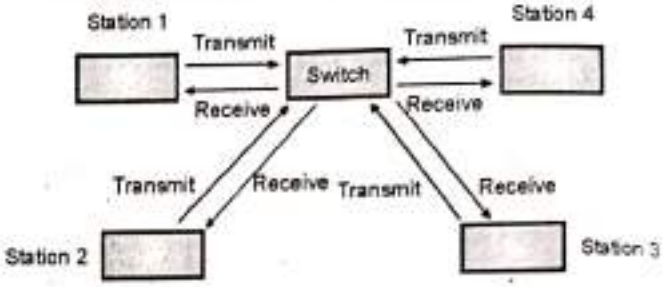
Q. 1 Discuss the working of switched Ethernet with suitable example. **(Dec. 10, 10 Marks)**

Q. 2 Make a comparative study of switched ethernet, fast ethernet and gigabit ethernet. **(Dec. 13, 10 Marks)**

- 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 to layer-2 switches.

4.9.4 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. 4.9.2 : 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. 4.9.2 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.

4.9.5 Fast Ethernet : MU : Dec. 13

University Questions

Q. 1 Make a comparative study of switched ethernet, fast ethernet and gigabit ethernet. **(Dec. 13, 10 Marks)**

- 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.

4.9.6 Gigabit Ethernet : MU : Dec. 13

University Questions

Q. 1 Make a comparative study of switched ethernet, fast ethernet and gigabit ethernet. **(Dec. 13, 10 Marks)**

- 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.

Scanned by CamScanner

4.10 IEEE Standards :

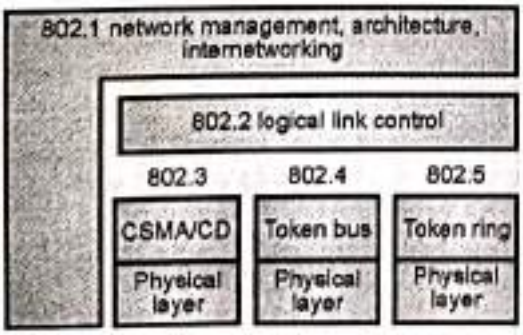
- The Institution of Electrical and Electronics Engineers (IEEE) has developed the layered architecture and other standards of LAN, under their project 802 set up in 1980. The IEEE 802 standards are as follows :

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 :

1. Carrier sense multiple access/collision detection (CSMA/CD)
2. Token bus and
3. Token ring

- Thus there are three protocols for the MAC sublayer. The IEEE standard 802.3 (CSMA/CD), 802.4 (Token bus), 802.5 (Token ring) are associated with these protocols as shown in Fig. 4.10.1.
- The physical layer protocols do the job of signal encoding, data rate control and interfacing to the transmission medium. The Logical Link Control layer (LLC) specifications are given in IEEE 802.2.



(G-295) **Fig. 4.10.1 : IEEE LAN and related standards**

4.11 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.

4.11.1 Traditional Ethernet Frame : MU : May 12

University Questions

Q. 1 Write short notes on : Ethernet frame formats. **(May 12, 6 Marks)**

Fig. 4.11.1 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. 4.11.1 : Traditional Ethernet frame**

Frame format :

The 64-bit (8 bytes) preamble allows the receiver to synchronize with the signal, it is a sequence of alternating 0's and 1's.

DA and SA :

- Both the source and destination hosts are identified with a 48-bit (6 bytes) address. These are indicated by the 6 byte number entered in the destination address (DA) and source address (SA) fields of the frame.
- The packet type field serves as the de-multiplexing key.

Data :

- Each frame contains upto 1500 bytes of data. The minimum size of a frame is 46 bytes of data, the reason for this is that the frame must be long enough to detect a collision. Each frame includes 32 bit (4 bytes) checksum. CRC is the last field in the Ethernet frame.
- The Ethernet is a bit-oriented framing protocol. An Ethernet frame has 14-byte header, two 6-bytes addresses and 2-byte type field.
- The sending adapter attaches the preamble, CRC and postamble before transmitting and the receiving adapter removes them.

Scanned by CamScanner

Start Frame Delimiter (SFD) :

- This is the second field in the Ethernet frame and it is of 1 byte length. The byte stored at this field is 10101011.
- This field signals the beginning of the frame.
- The SDF is used to communicate to the station that this is the last chance for synchronization.
- The last two bits 11 alert the receiver that the next field in the frame contains the destination address.

4.11.2 Frame Length : MU : Dec. 13

University Questions

Q. 1 State the reasons for having a minimum length requirement for a frame in Ethernet. How is it achieved ? **(Dec. 13, 5 Marks)**

- 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. 4.11.2(a) and that of the maximum length frame is shown in Fig. 4.11.2(b).

Destination address	Source address	Length PDU	Data and padding	CRC
6 bytes	6 bytes	2 bytes	46 bytes	4 bytes

64 bytes

(a) Minimum length frame

Destination address	Source address	Length PDU	Data and padding	CRC
6 bytes	6 bytes	2 bytes	1500 bytes	4 bytes

1518 bytes

(b) Maximum length frame

(G-306) Fig. 4.11.2 : Minimum and Maximum length frame formats of traditional Ethernet

- The restriction on the minimum length is to ensure correct operation of CSMA/CD, whereas the restriction on the maximum length is just out of some hystorical reasons.

4.11.3 Addressing :

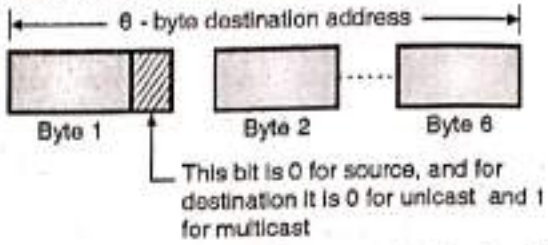
- There can be various types of stations connected on an Ethernet network such as PC on workstation or printer.
- Each station has its own network interface card (NIC) which fits inside the station to contain the 6 byte physical address of the station.
- Fig. 4.11.3 shows a 6-byte Ethernet address in the hexadecimal notation.

04 – 02 – 01 – 06 – 1C – 5B

(G-307) Fig. 4.11.3 : Ethernet address

4.11.4 Types of Addresses :

- A source address is only unicast address. This is because the frame comes from only one source.



(G-308) Fig. 4.11.4 : Difference between unicast and multicast addresses

- The destination address can be one of the following three types :
  1. Unicast
  2. Multicast 3. Broadcast
- Fig. 4.11.4 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.

4.11.5 Physical Properties of Ethernet :

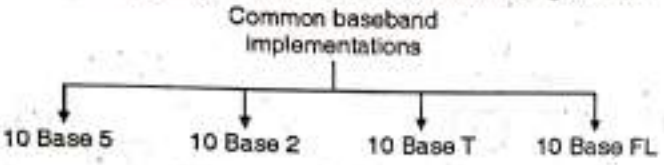
- Let us see some physical properties of Ethernet. An Ethernet segment is implemented on a coaxial cable of upto 500 m.
- A **transceiver**, which is a small device directly attached to the tap, detects when the line is idle and drives the signal when the host is transmitting. Tap must be at least 2.5 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.

Scanned by CamScanner

- 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.

4.11.6 Physical Layer Implementation of Traditional Ethernet :

The standard has defined four different implementations for the baseband (digital) 10 Mbps Ethernet as shown is Fig. 4.11.5.



(G-312)**Fig. 4.11.5 : Categories of traditional Ethernet**

IEEE 802.3 10 Mbps Specifications (Ethernet) :

- IEEE 802.3 committee defines alternative physical configurations. Various defined options are as follows :
  1. 10 BASE 5
  2. 10 BASE 2
  3. 10 BASE – T (T stands for twisted pair)
  4. 10 BASE – FL (F stands for optical fiber)
- All the four options stated above are for the 10 Mbps Ethernet.

1. 10 Base 5 : Thick Ethernet :

- The first implementation of the traditional Ethernet is called 10 Base 5 or thick Ethernet or thicknet.
- This was the first Ethernet technology.
- The name thicknet is due to the use of thick coaxial cable.
- The thicknet uses the bus topology.
- It is the original 802.3 medium specification and is based directly on Ethernet.
- A 50 Ω 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 50 Ω coaxial cable and the data is converted into Manchester digital signalling before putting it on the cable.
- Thin Ethernet uses a thin cable, supports less number of users and specified for an effective length of 185 metres only.
- The data rate is same as that of 10 BASE 5 specification i.e. 10 Mbps hence it is possible to combine them in a network.
- Note that the 10 BASE 2 should not be used to connect two segments of 10 BASE 5 cable.

3. 10 Base-T : Twisted pair Ethernet :

- This is the third physical layer implementation of traditional Ethernet. It makes use of a physical star topology.
- The twisted pair cable of unshield type is used instead of coaxial cable as the common medium.
- The data is converted into Manchester digital signaling before putting it on the cable.
- The maximum segment length is reduced to only 100 m. It is much less than the 10 BASE 5 specification.
- The advantage of this type is that the twisted pair wire is easily available in any building (due to the existing telephone connection).
- As an alternative an optical fiber link can be used. Then the maximum length becomes 500 m.

4. 10 Base FL : Fiber Link Ethernet :

- This is the fourth physical layer implementation of traditional Ethernet.
- It makes use of the star topology for connecting stations to a hub.
- The transceiver is connected to the hub by using two pairs of fiber optic cables.
- This standard contains three specifications as follows :
  1. 10 BASE FP (P for passive)
  2. 10 BASE FL (L for link)
  3. 10 BASE FB (B for backbone)
- All these specifications use a pair of optical fibers for each transmission link.
- The data is converted into the Manchester code and then the Manchester signal is converted into light signal (off for 0 and on for 1). Hence the frequency of the Manchester bit stream actually needs to be 20 Mbps on the fiber.

4.12 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.

Scanned by CamScanner

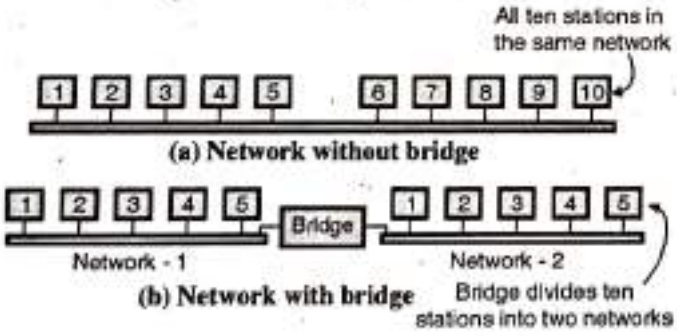
4.13 Bridged Ethernet :

- 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 :

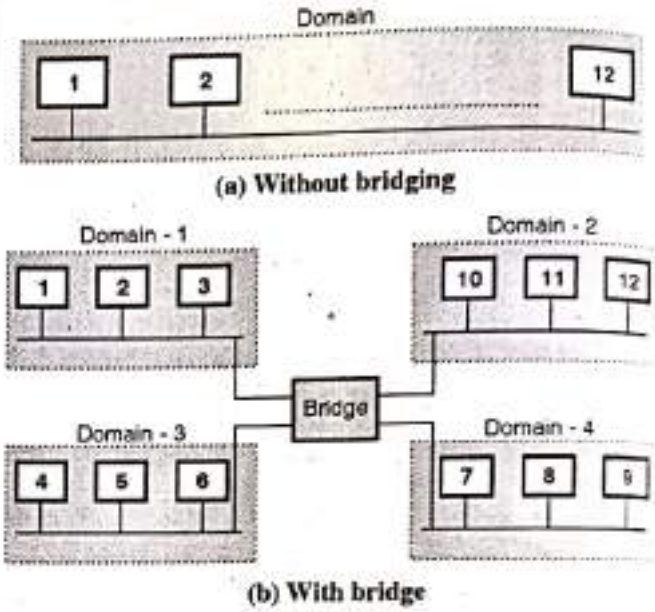
- In the traditional Ethernet the total capacity the network is 10 Mbps and it is shared among all the stations when a frame is to be sent. The stations share the bandwidth of the network.
- If only one station has frames to send, then it can use the entire bandwidth 10 Mbps for itself. But if there 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. 4.13.1 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. 4.13.1 : Increase in Bandwidth due to bridge**

2. Separation of collision domain :

- Fig. 4.13.2 explains the concept of separation of collision domains. Fig. 4.13.2(a) shows the collision domains for the original network without bridge whereas Fig. 4.13.2(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.

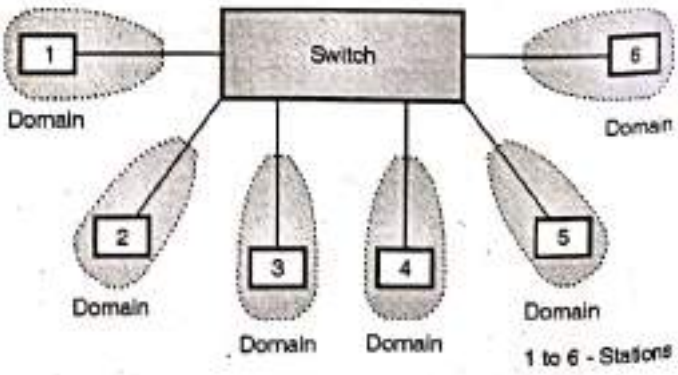


(G-314)**Fig. 4.13.2 : Collision domains in the nonbridged and bridged network**

4.14 Switched and Full Duplex Ethernet :

4.14.1 Switched Ethernet :

- The concept of bridged LAN can be extended to form the switched LAN.
- An N port switch is used to connect N number of stations on the LAN. Each member of the LAN is connected to a port of the switch.
- The entire bandwidth is shared only between the stations and the switch. The collision domain is divided into N domains. This reduces the possibility of collisions in the network.
- Due to the use of a layer 2 switch faster handling of packets is also possible.
- The concept of switched Ethernet is illustrated in Fig. 4.14.1.

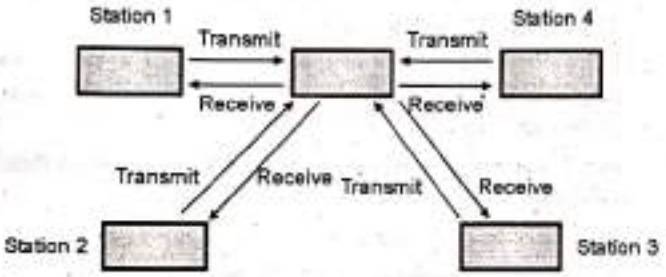


(G-315)**Fig. 4.14.1 : Switched Ethernet**

Scanned by CamScanner

4.14.2 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. 4.14.2 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. 4.14.2 : 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.

4.15 Fast Ethernet : MU : May 16

University Questions

Q.1 Write short notes on : FDDI **(May 16, 5 Marks)**

- Fast Ethernet is the protocol designed to work upto 100 Mbps and it is compatible with the standard Ethernet.
- The traditional Ethernet can operate only upto 10 Mbps. Hence for higher data rates fast Ethernet has been developed.

MAC sublayer :

- In the evolution of Ethernet, care has been taken to keep the MAC sublayer untouched. So MAC sublayer of the fast Ethernet is same as that of the traditional Ethernet.
- For the standard Ethernet the bus and star topologies were used. But the fast Ethernet uses only the star topology.

Access method :

- The access method also remains the same. It is CSMA/CD.
- However the fast Ethernet is a full duplex protocol and does not need the CSMA/CD.
- But the CSMA/CD is used for backward compatibility, with the traditional Ethernet.

Frame format :

Frame format of fast Ethernet is same as that of the traditional Ethernet.

Minimum and maximum frame lengths :

Minimum and maximum frame lengths of the fast Ethernet frame are same as those of traditional Ethernet.

Addressing :

Addressing is also same a that for the traditional Ethernet.

4.15.1 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 rare of operation.

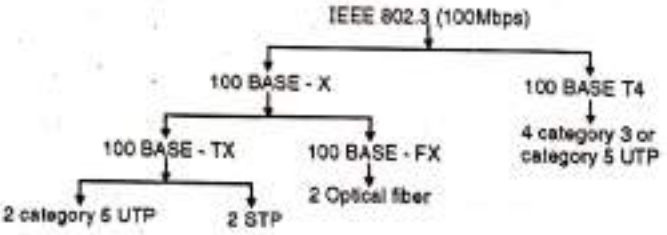
Features of the autonegotiation :

The important features of autonegotiation are :

1. The non-compatible devices can be connected to each other.
2. One device can be allowed to have multiple capabilities.
3. A station can check hub's capabilities.

4.15.2 Physical Layer Implementation :

- Fig. 4.15.1 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. 4.15.1 : IEEE 802.3 100 BASE – T options**

- All of the 100 BASE – T options shown in Fig. 4.15.1 use the IEEE 802.3 MAC protocol and frame format.
- 100 BASE – X indicates the options which use the medium specifications defined by FDDI.

Scanned by CamScanner

- 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. 4.15.1. 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.

4.16 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.

Topology :

- This Ethernet uses a point-to-point topology if only two stations are to be connected. But it uses the star topology if more number of stations are to be connected to each other.
- The Gigabit Ethernet was designed with some specific goals in mind :
  1. To increase the data rate to 1 Gbps.
  2. To make it downward compatible with the older version i.e. standard or fast Ethernet.
  3. To make use of the same 48-bit address.
  4. To utilize the same frame format.
  5. Not to change the minimum and maximum frame lengths.
  6. To use the autonegotiation as defined in fast Ethernet.

4.16.1 MAC Sublayer :

- The MAC sublayer can not remain unchanged or same as standard or fast Ethernet if the data rate of 1 Gbps is to be achieved. The Gigabit Ethernet has to use two approaches for the medium access :
  1. Full duplex and 2. Half duplex.
- The full duplex approach is being followed by almost all the implementations of Gigabit Ethernet.
- But if the half duplex approach is followed then the Gigabit Ethernet can be made compatible with standard or fast Ethernet.

Full duplex mode :

- In this approach, a central switch is connected to all computers or other switches. Each switch has buffers for each input port. The incoming data are stored on these buffers until it is transmitted.
- There is no collision in this mode. Hence CDMA/CD is not used. As there is no collision, the length of cable is dependent on the signal attenuation in the cable and not on the collision detection process.

Half duplex mode :

- The Gigabit Ethernet is used very rarely in the half duplex mode. For this mode a hub can be used instead of the switch.
- The CDMA/CD which is not used for the full duplex mode has to be used for the half duplex mode. The maximum length of the cable is entirely decided by the minimum value of the frame size.
- In relation with the minimum frame size the following three methods have been defined :
  1. Traditional method
  2. Carrier extension and 3. Frame bursting

1. Traditional method :

- In the traditional method, the minimum length of the frame is kept same as that in the traditional Ethernet (512 bits or 64 bytes).
- But in Gigabit Ethernet the length of each bit is $1/1 \times 10^9 = 1$ nsec. The bit length for a 10 Mbps Ethernet is $1/10 \times 10^6 = 100$ ns. Thus the length of each bit is 1/100 times shorter in the Gigabit Ethernet as compared to that in the 10 Mbps Ethernet.
- Hence the slot time for Gigabit Ethernet is given by

  $$\text{Slot time} = 512 \text{ bits} \times 1 \times 10^{-9} \text{ sec.} = 0.512 \ \mu\text{sec.}$$
- Due to reduced slot time, the collision is detected 100 times earlier and therefore the maximum length of the network is restricted to only 25 m i.e. 100 times less than the maximum length of the traditional Ethernet (2.5 km).
- This length is very short and not suitable for connecting computers even in one single office.
- Due to these demerits the traditional approach is not suitable.

2. Carrier extension method :

- In order to increase the length of the network the minimum frame length is increased to 512 byte i.e. 4096 bits in the carrier extension approach.
- This is 8 times longer than the minimum frame size of 64 bytes in the traditional approach. Therefore the maximum length of the network also is increased 8 times and becomes $25 \times 8 = 200$ m.

Scanned by CamScanner

3. Frame bursting :

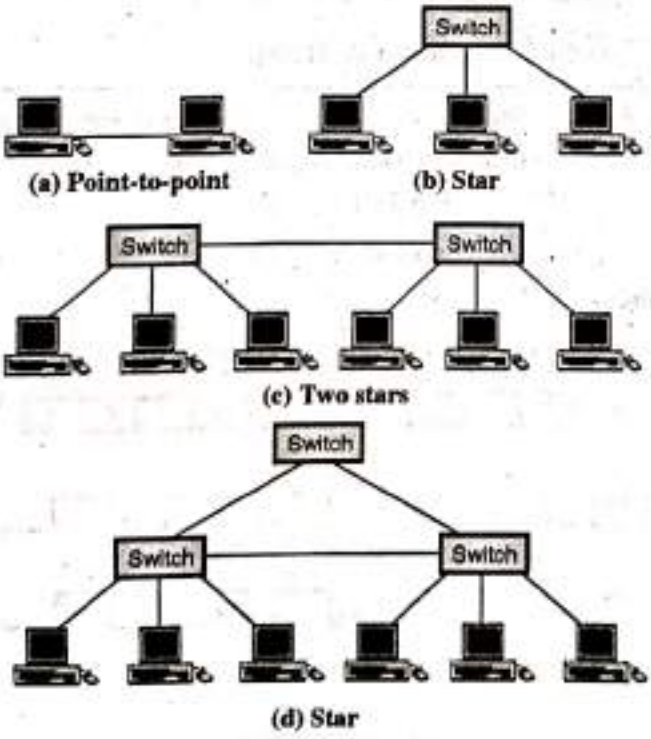
- The carrier extension technique increases the maximum length of the network. But it is very inefficient technique because for sending short frames we need to send a lot of redundant data so a make the frame length equal to 4096 bits.
- The efficiency can be increased with the help of the **frame bursting** technique. Here instead of adding an extension to each frame, multiple frames are sent to make the minimum frame length of 4096 bits.
- However in order to make these multiple frames appear like one frame, padding is added between the frames. This is same as that used for the carrier extension approach. Thus we send a large frame without adding any redundant bits.

4.16.2 Physical Layer :

The physical layer in the Gigabit Ethernet is not as simple as that in the standard or fast Ethernet. Some of its features are as follows :

Topology :

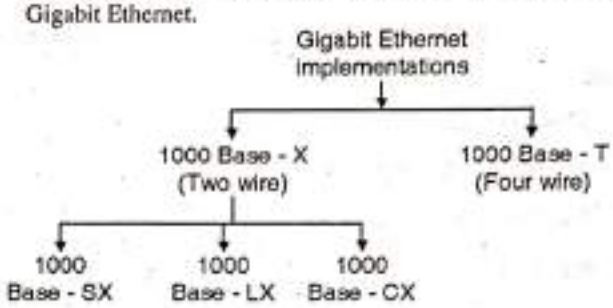
- The topology used for connecting the stations in Gigabit Ethernet depends on the number of stations to be connected.
- For example : if two stations are to be connected, a point to point topology may be used. For three or more stations a star topology is used with a hub or switch at the center.
- Another option is to connect several startopologies with a star topology being a part of another one as shown in Figs. 4.16.1(c) and (d).



(L-799)**Fig. 4.16.1 : Topologies of Gigabit Ethernet**

4.16.3 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. 4.16.2 shows the physical layer implementations for the Gigabit Ethernet.



(G-323) **Fig. 4.16.2 : Physical layer implementations of Gigabit Ethernet**

Encoding :

- The Gigabit Ethernet cannot use the Manchester encoding due to its high bit rate.
- Hence the 8B/10B block encoding followed by NRZ encoding is used for all the two wire implementations.

4.16.4 Ten Gigabit Ethernet :

- The next step of Gigabit Ethernet is ten gigabit Ethernet. The IEEE committee calls this Ethernet as standard 802.3ae.
- The goals of 10GB Ethernet are as follows :
  1. Data rate is to be upgraded to 10 Gbps.
  2. This Ethernet should be downward compatible to the standard, fast and gigabit Ethernet.
  3. Frame format and 48-bit address should be same as the older versions.
  4. Minimum and maximum frame lengths should remain same.
  5. This Ethernet should be connectable to the existing LAN, WAN and MAN.
  6. This Ethernet should be mode compatible with the technologies like Frame Relay and ATM.

MAC sublayer :

- This Ethernet operates only in the full duplex mode. Hence there is no possibility of contention. So CDMA/CD is not used in this Ethernet.

Physical layer :

- The physical layer of this Ethernet is designed to work with the optical fiber cable.
- The three commonly used implementations are :
  1. 10 G Base-S
  2. 10 G Base-I
  3. 10 G Base-E

Scanned by CamScanner

4.17 Solved Examples :

Ex. 4.17.1 : 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 :**

For a slotted ALOHA, $P_0 = e^{-G}$

But $P_0 = 10\%$ i.e. 0.1

$\therefore \quad 0.1 = e^{-G}$

$\therefore -2.3 = -G \qquad \therefore \quad G = 2.3$

2. **Throughput :**

$$S = G e^{-G} = 2.3 e^{-2.3} = 0.23$$

3. Since G is beyond 1 the channel is overloaded.

Ex. 4.17.2 : 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.

Length $L = 1$ km $= 1 \times 10^3$ m

Speed $v = 2,00,000$ km/s $= 2 \times 10^8$ 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 $\tau = 5$ µsec. $\therefore 2\tau = 10$ µsec.
3. To make CSMA/CD work, it must be ensured that the minimum frame size should be equal to $2\tau = 10$ µsec.

But $\quad R = 1 \times 10^9$ bits/sec

$\therefore \quad 1$ sec $= 1 \times 10^9$ bits

$\therefore 10 \times 10^{-6}$ sec $=$? bits

$$\therefore \quad \frac{1}{10 \times 10^{-6}} = \frac{1 \times 10^9}{x}$$

$$\therefore \quad x = 1 \times 10^9 \times 10 \times 10^{-6} = 10 \times 10^3 = 10{,}000 \text{ bits.}$$

$\therefore$ Minimum frame size

$= 10{,}000$ bits or 1250 bytes.

Ex. 4.17.3 : 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 sec $=$ 50 requests (transmissions)

$\therefore$ 40 msec $=$ x transmissions. $\quad \therefore \dfrac{1}{40 \times 10^{-3}} = \dfrac{50}{x}$

$\therefore \quad x = 50 \times 40 \times 10^{-3} \qquad \therefore \quad x = 2$

2. But number of transmissions $(x) = e^G$

$\therefore \quad 2 = e^G \qquad \therefore \quad G = 0.693$

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 $G e^{-G}$

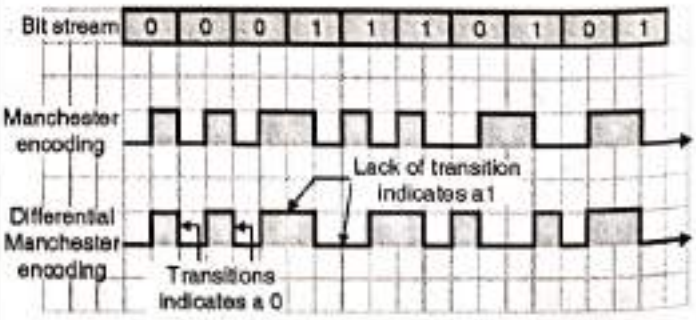
i.e. $\quad 0.693\, e^{-0.693} = 0.3465$ or 34.65%.

Ex. 4.17.4 : Sketch Manchester encoding and differential Manchester encoding for bit stream.

1. 0 0 0 1 1 1 0 1 0 1
2. 1 1 0 0 1 0 1 1 1 0

Soln. :

The required waveforms are as shown in Fig. P. 4.17.4.



(G-337) **Fig. P. 4.17.4**

Scanned by CamScanner

Ex. 4.17.5 : 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) :

For the slotted ALOHA, $P_0 = e^{-G}$

$\therefore 0.2 = e^{-G}$

$\therefore G = 1.6094$ **...Ans.**

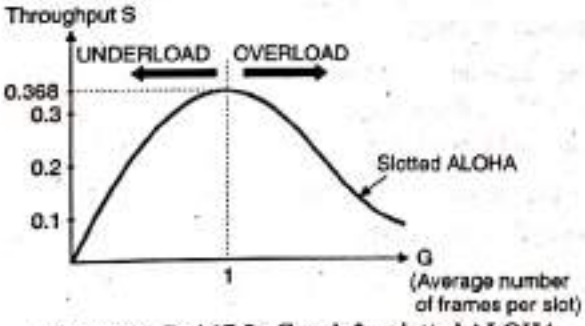
2. Throughput (S) :

$S = Ge^{-G} = P_0 G = 0.2 \times 1.6094$

$\therefore S = 0.3218$ **...Ans.**

3. Status of the channel :

- From Fig. P. 4.17.5 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. 4.17.5 : Graph for slotted ALOHA**

Ex. 4.17.6 : Using the binary count down 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. 4.17.7 : An ALOHA network user 19.2 kbps channel for sending message packets of 100 bit long size. Calculate the maximum throughput for pure ALOHA network.

Soln. :

Given : Rate of transmission = 19200 bits.

Frame length = 100 bits

$\therefore$ Number of frames per second $= \dfrac{\text{Rate of transmission}}{\text{Frame length}}$

$= \dfrac{19200}{100}$

= 192 frames / sec

The maximum throughput for a pure ALOHA system is 0.184.

$\therefore$ Throughput = 0.184 × Number of frames/sec.

= 0.184 × 192 = 35.328 frames/sec....**Ans.**

Ex. 4.17.8 : 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 bit.

Soln. :

Given : Number of stations N = 20

Length of the ring d = 100 m

Scanned by CamScanner

Propagation speed V = 2×10^8 m/sec.

Rate of transmission R = 4 Mbps.

Delay introduced by each station = b = 2.5 bits.

Step 1 : Calculate the total delay :

$$\text{Delay introduced by N stations} = \frac{N \times b}{R} = \frac{20 \times 2.5}{4 \times 10^6}$$

$$= 12.5\ \mu\text{sec} \quad \ldots(1)$$

$$\text{Additional delay introduced by the ring} = \frac{d}{V}$$

$$= \frac{100\text{ m}}{2 \times 10^8\text{ m/s}}$$

$$= 0.5\ \mu\text{S} \quad \ldots(2)$$

So total delay = $12.5 + 0.5 = 13\ \mu$ sec.

Step 2 : Calculate the ring latency :

Ring latency is defined as the number of bits that can be simultaneously in transit around the ring.

$$\therefore \text{ Ring latency} = \text{Total delay} \times \text{Rate of transmission.}$$

$$= 13 \times 10^{-6} \times 4 \times 10^6$$

$$= 52 \text{ bits} \quad \ldots\textbf{Ans.}$$

Ex. 4.17.9 : ALOHA protocol is used to share 56 kbps satellite channel. If each packet is 1000 bits long find maximum throughput in pockets/sec.

Soln. :

Given : Rate of transmission = 56 kbps = 56000 bps

Frame length = 1000 bits

1. For pure ALOHA :

$$\therefore \text{ Number of frames/sec} = \frac{56000 \text{ bits}}{1000 \text{ bits/frame}}$$

$$= 56 \text{ frames/sec}$$

The maximum throughput for pure ALOHA

$$= 0.184$$

$$\therefore \text{ Throughput} = 56 \times 0.184$$

$$= 10.304 \text{ frames/sec.} \quad \ldots\textbf{Ans.}$$

2. For slotted ALOHA :

Maximum throughput = 0.368

$$\therefore \text{ Throughput} = 0.368 \times 56 = 20.608 \text{ frames/sec.}$$

$$\ldots\textbf{Ans.}$$

Ex. 4.17.10 : 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.

$$\therefore \quad N = \frac{R}{10 \text{ bits/sec}} = \frac{10.3 \text{ kbps}}{10}$$

$$= 1030 \quad \ldots\textbf{Ans.}$$

Ex. 4.17.11 : 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.

1. Stop and wait ARQ :

There are no outstanding frames at the sending end.

∴ The size of sending window is zero. The size of receive window is always 1.

2. Go-back-N ARQ :

The maximum size of send window with an "m" bit sequence number is 2^{m-1}. Hence for a 5 bit sequence number (m = 5) the maximum send window size is $2^5 - 1 = 31$.

∴ The maximum receive window size is always 1.

3. Selective repeat ARQ :

The maximum send and receive window size is $2^m/2$.

∴ For m = 5 the window size is $2^5/2 = 16$.

Ex. 4.17.12 : 1 Gbps CSMA/CD LAM is to be designed over 1 km cable without repeater. The cable supports signal speed of 200,000 km/sec. What is the minimum frame size that data link layer should consider.

Dec. 03, Dec. 16, 10 Marks

Soln. :

Propagation speed = 200000 km/sec.

Length of cable = 1 km

$$\text{Propagation Time} = \frac{1}{200000} = 5 \times 10^{-6}\text{ s} = 5\ \mu\text{sec}$$

Scanned by CamScanner

Transmission speed = 1 Gbps.

Number of bits in cable :

Number of bits sender can transmit from time it sends 1st bit to the time that bit reaches end of cable.

$$1 \times 10^9 \times \frac{1}{20000} = 0.5 \times 10^5 = 5 \times 10^4 \text{ bits.}$$

$$\text{Frame size} = 5 \times 10^4 \times 2$$

$$= 10{,}000 \text{ bits}$$

$$\text{Total round time} = 5 \times 2 = 10\ \mu\text{ sec.}$$

For collision detection frame should take at least 10 µS to send.

$$\text{Data rate} = 1000 \text{ bit per } \mu\text{S.}$$

Thus 10,000 bits could be sent in 10 µS. Thus frame size should be at least 10,000 bits.

Ex. 4.17.13 : A pure ALOHA network transmits 200 bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces ?

1. 1000 frames per second
2. 500 frames per second
3. 250 frames per second.

MU : Dec. 16, 10 Marks

Soln. :

Given : Rate of transmission = 200 kbps

= 200000 bps

Frame length = 200 bits

To find : Throughput

1. Number of frames / sec = 1000 frames / sec.

The maximum throughput for a pure ALOHA system is 0.184

$$\therefore \text{Throughput} = 1000 \times 0.184$$

$$= 184 \text{ frames /sec}$$

2. Number of frames / sec = 500

$$\therefore \text{Throughput} = 500 \times 0.184$$

$$= 92 \text{ frames / sec}$$

3. Number of frames / sec = 250

$$\therefore \text{Throughput} = 200 \times 0.184$$

$$= 36.8 \text{ frames / sec}$$

$$\text{Throughput of all stations} = 184 + 92 + 36.8$$

$$= 312.8 \text{ frames / sec}$$

4.18 Data Link Layer Switching :

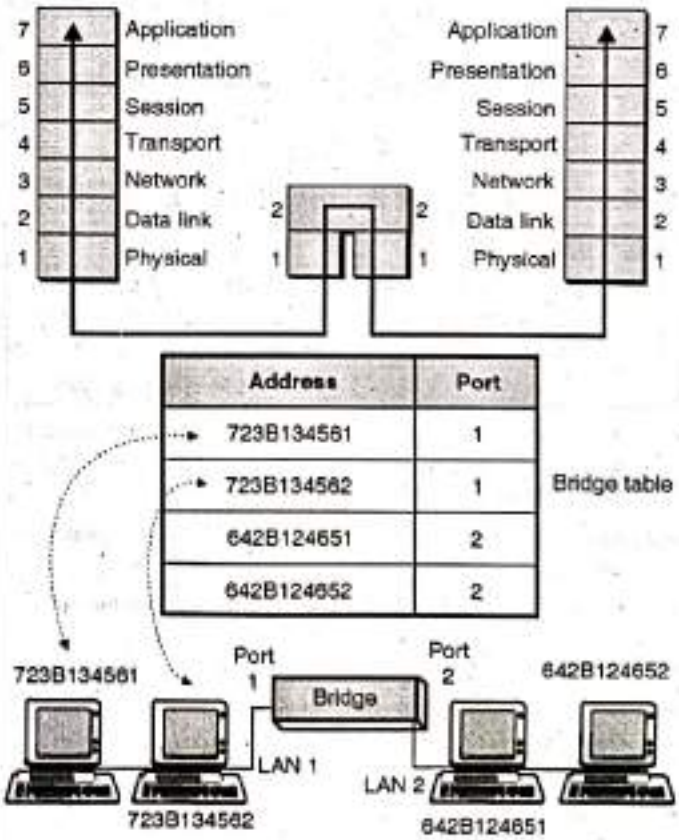
- Many organizations have more than one LANs and these LANs need to be interconnected.
- LANs can be connected with the help of devices called as bridges.
- In the following sections we are going to discuss the bridges, switches and some other devices that are used for interconnected of LANs.

4.19 LAN Bridges :

- 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. 4.19.1.
- 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. 4.19.1 a two port bridge is shown but in reality a bridge has more than two ports.



(G-354) **Fig. 4.19.1 : Bridge and bridge table**

Scanned by CamScanner

- 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 :
  1. 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 :
  1. Filtering frames 2. Forwarding and 3. 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.

4.19.1 802 Bridges :

Various difficulties are faced when trying to build a bridge between the various 802 LANs :

1. Each of the LANs use a different frame format, as a result any copying between different LANs requires reformatting which takes CPU time, requires a new checksum calculation and introduces the possibility of undetected errors due to bad bits in the bridge's memory.
2. Interconnected LANs do not necessarily run at the same data rate.
3. All three 802 LANs have a different maximum frame length.

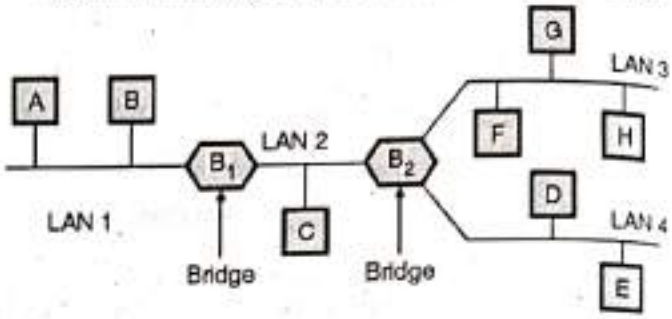
4.19.2 Transparent Bridges : MU : Dec. 09

University Questions

Q. 1 What is the difference in functionalities between a bridge and a repeater ? Explain the process of learning in case of transparent bridge.

(Dec. 09, 10 Marks)

- 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. 4.19.2. As shown in the Fig. 4.19.2 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.



(L-448) **Fig. 4.19.2 : Configuration of bridge and LAN**

- 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 4.19.1.

Table 4.19.1 : 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 :

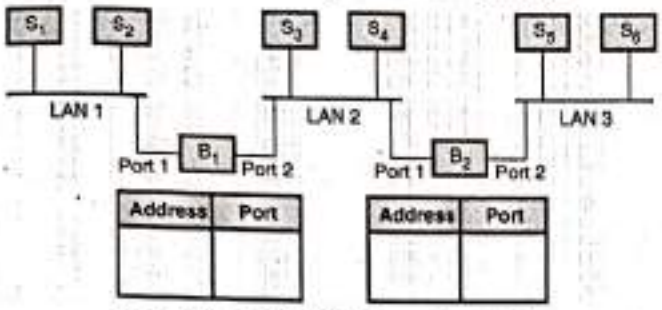
Bridge learning procedure :

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.

Scanned by CamScanner

Example on bridge learning :

Consider the network shown in Fig. 4.19.3(a). Assume that forwarding tables of both the bridges are initially empty.



(L-649) **Fig. 4.19.3(a) : Example network**

1. **S_2 sends a frame to S_1 :**
   - If S_2 sends a frame to S_1, then B_1 compares the source address of the received frame with the existing entries. So here S_2 is the sender and S_1 is destination.
   - But there are no entries in B_1 table. So it adds the address of S_2 in its forwarding table as shown in Fig. 4.19.3(b).
   - Then B_1 compares the destination address of the received frame with the existing entries. But the table is empty. So the bridge B_1 thinks of flooding the frames. But then it understands that the **destination S_1 is connected on the same port (Port 1) on which the frame has been received.**
   - So B_1 will note down the address of S_1 in its table and **discard the frame.** This is because bridge B_1 is not required to be used when a communication between S_1 and S_2 is to be made.
   - The traffic is now completely isolated in LAN 1, and the updated bridge tables are shown in Fig. 4.19.3(b).

B_1

Address	Port
S_2	1
S_1	1

B_2

Address	Port

Fig. 4.19.3(b) : Forwarding tables after $S_2 \rightarrow S_1$

2. **S_5 transmits to S_4 :**
   - The two stations correspond to two different LANs. S_5 is the sender and S_4 is the destination.
   - First B_2 records the address of S_5 and port number (Port 2) because the address of S_5 is not found in its forwarding table.
   - Then B_2 checks the destination address. Since there are no entries, it will add S_4 and port 1 in its table as shown in Fig. 4.19.3(c).
   - Bridge B_2 will forward the frame to port 2 of B_1 as well as to LAN 2 where S_4 will receive it.
   - When this frame arrives at port 2 of B_1 it also adds the source address i.e. S_5 and port 2 in its table as shown in Fig. 4.19.3(c).
   - However the destination address (S_4) is on the same port (2) of B_1 on which it has received the frame. So it will note down S_4 and port 2 in its table but **discard** the frame.

B_1

	Address	Port
$S_2 \rightarrow S_1$	S_2	1
	S_1	1
$S_5 \rightarrow S_4$	S_5	2
	S_4	2

B_2

	Address	Port
$S_5 \rightarrow S_4$	S_5	2
	S_4	1

(G-1970) **Fig. 4.19.3(c) : Forwarding tables after $S_5 \rightarrow S_4$**

The table entries for the remaining transmissions are given in Figs. 4.19.3(d) and (e).

3. **S_3 transmits to S_5 :**

B_1

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

B_2

	Address	Port
$S_5 \rightarrow S_4$	S_5	2
	S_4	1
$S_3 \rightarrow S_5$	S_3	2

(G-1971) **Fig. 4.19.3(d) : Tables after $S_3 \rightarrow S_5$**

4. **S_1 transmits to S_2 :**

   No change in the tables.

5. **S_6 transmits to S_5 :**

B_1

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

B_2

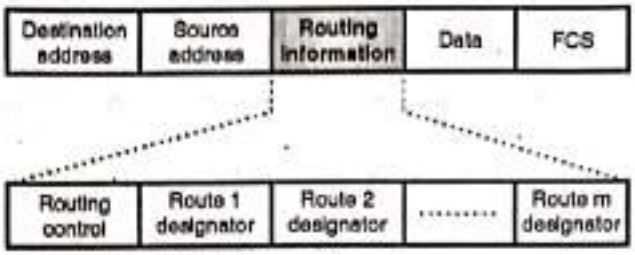
	Address	Port
$S_5 \rightarrow S_4$	S_5	2
	S_4	1
$S_3 \rightarrow S_5$	S_3	2
$S_6 \rightarrow S_5$	S_6	2

(G-1972) **Fig. 4.19.3(e) : Table after $S_6 \rightarrow S_5$**

4.19.3 Source Routing Bridges :

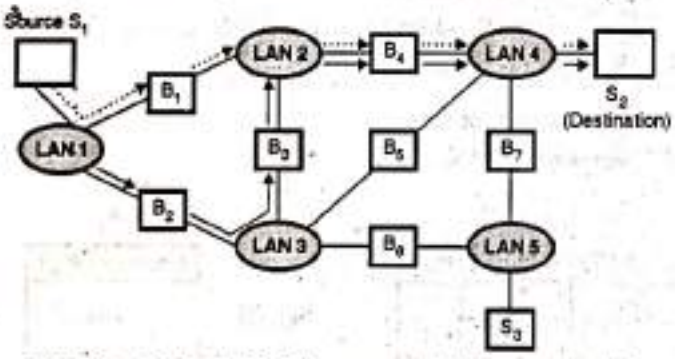
- The source routing bridges were developed by the IEEE 802.5 committee and they are used basically to interconnect token ring networks.
- The main idea of source routing is that each station should determine the route to the destination when it wants to send a frame and therefore include the route information in the header of the frame.

Scanned by CamScanner



(L-654) **Fig. 4.19.4 : Frame format for source routing**

- The frame format for source routing is shown in Fig. 4.19.4.
- Note that the routing information field is inserted only if the two communicating stations are on different LANs.
- Fig. 4.19.5 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 → B_1 → LAN 2 → B_4 → 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.



(L-655) **Fig. 4.19.5 : LANs interconnected with source routing bridges**

How to discover a route ?

To discover a route the basic idea is as follows :

1. The station who wants to discover a route first broadcasts a special frame called single route broadcast frame.
2. This frame will visit every LAN exactly once and eventually reaches the destination.
3. 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.
4. After collecting all routes the source chooses the best possible route and saves it.

4.19.4 Comparison of Transparent and Source Routing Bridge :

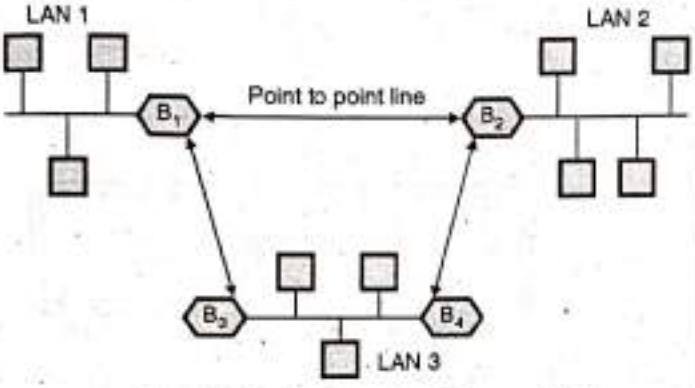
Sr. No.	Parameters	Transparent Bridge	Source Routing Bridge
1.	Ability to reconfigure	High. Bridges keep information on location of stations.	High. Each station must learn the route to its destination before sending
2.	Stations responsibilities	None. They just send the frames and let the bridges do the 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.

4.19.5 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. 4.19.6.

Scanned by CamScanner

- 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.



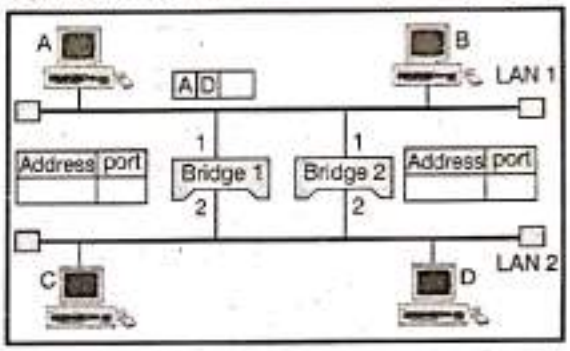
(L-656) **Fig. 4.19.6 : Configuration of remote bridges**

4.19.6 Loop Problem in Bridge LAN :

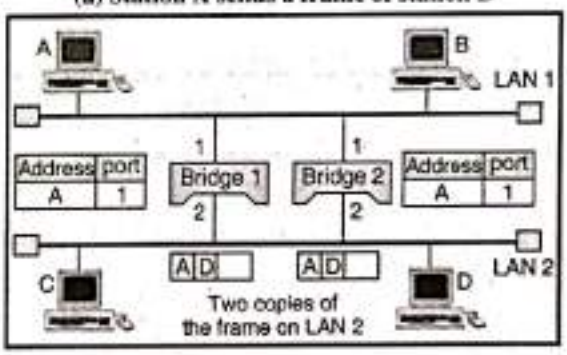
- In the practical LANs loops gets created accidentally or sometimes they are created intentionally to increase redundancy.
- Transparent bridges work without any problem as long as there are no redundant bridges in the given network. But network administrators include redundant bridges (more than one bridges between two LANs) in order to improve the reliability of the network.
- If one bridge fails then, the other one can take over the job until the faulty bridge gets repaired.
- But if we include redundant bridges then it gives rise to a problem called **looping.**

Example :

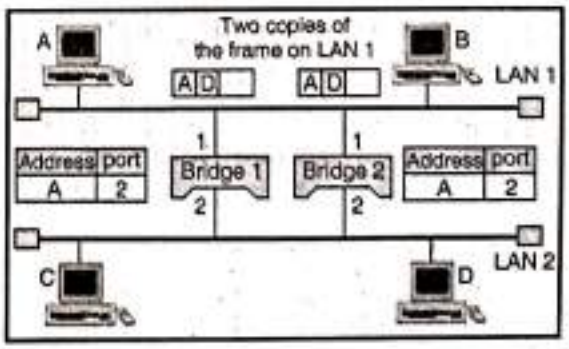
- Fig. 4.19.7 demonstrates the looping problem. It shows that two LANs are connected to each other via two bridges.
- The looping takes place as follows :
  1. Initially the tables of both the bridges are empty. Station A sends a frame to station D. Both the bridges forward the frame and update their tables on the basis of source address A. (See Fig. 4.19.7(a)).
  2. Thus there are two copies of the same frame on LAN 2 as shown in Fig. 4.19.7(b), one each produced by the two bridges.
  3. The copy forwarded by bridge - 1 is received by bridge - 2 which does not have any information about the destination address D. It floods the bridge.
  4. Similarly the copy forwarded by bridge - 2 is received by bridge - 1 and is sent out for lack of information about destination D. Thus each frame is being handled separately by the two bridges as both of them work as two nodes on a network sharing the medium with the help of access method such as CSMA/CD. Therefore the tables of both the bridges get updated but there is no information about the destination D.
  5. Now there will be two copies of the frame on LAN - 1 as shown in Fig. 4.19.7(c). As explained earlier both these copies will flood the network.
  6. This process continuous and becomes cumulative because the bridges are also repeaters and regenerate frames.
- The looping problem can be solved if bridges use the spanning tree algorithm to create a loopless topology.



(a) Station A sends a frame of station D



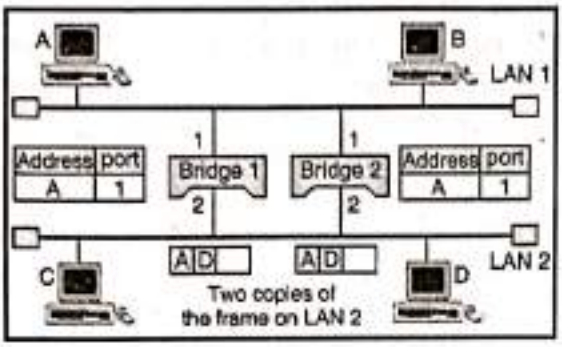
(b) Both bridges forward the frame



(c) Both bridges forward the frame

(G-1498) **Fig. 4.19.7(Contd...)**

Scanned by CamScanner



(d) Both bridges forward the frame

(G-1498) **Fig. 4.19.7 : Looping problem in bridges**

4.20 Mixed Media Bridges :

- The mixed media bridges are the bridges that interconnect LANs of different types.
- For example the interconnection of Ethernet and token ring LANs has to be done using the mixed media bridges.
- This types of interconnection is not simple because these two LANs differ in their frame structure, their operation and their speed and the bridge need to take these differences into account.
- Another problem in interconnecting LANs is that they use different transmission rates.
- The bridge which is interposed between two LANs must have sufficient buffering.

4.21 NIC (Network Interfacing Card) :

- Each PC or workstation or printer, in short each station that is to be connected in a network has its own Network Interface Card (NIC).
- The NIC is fitted inside the station and provides the station its physical address which is generally 6 byte long.
- The station address when connected in an Ethernet is 6 bytes (48 bits) and it is normally written in hexadecimal notation using a hyphen to separate bytes from each other as shown in Fig. 4.21.1.

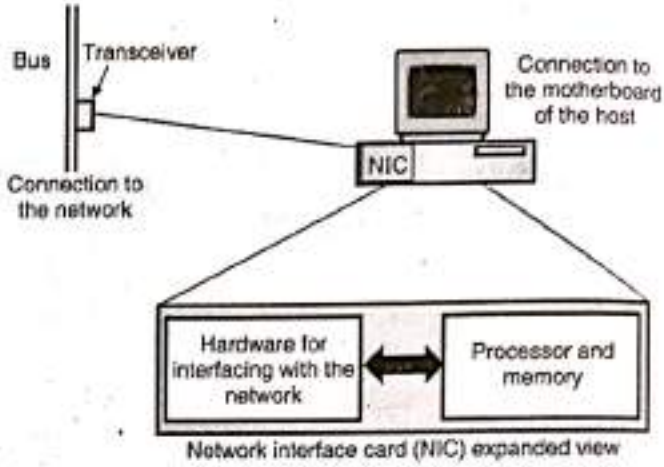
06 – 02 – 03 – 04 – 4C – 2B

Fig. 4.21.1 : Ethernet address in hexadecimal notation

- NIC is housed inside the computer on the motherboard. It provides the physical connection between the network and the computer station.
- The speed of NIC is important in determining the speed and efficiency of a network.
- There are three common types of NICs :
  1. Ethernet cards
  2. Local talk connectors
  3. Token ring cards.

4.21.1 NIC Operation :

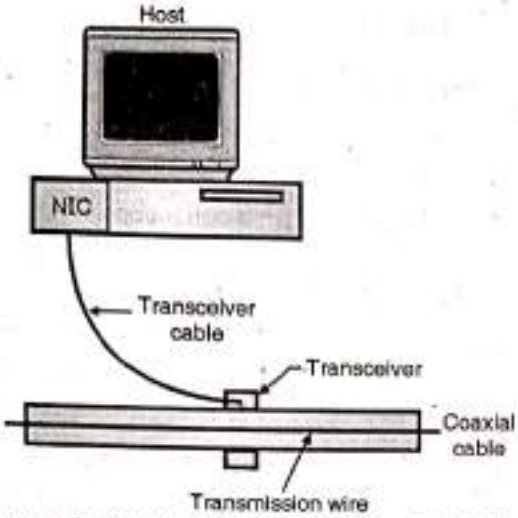
- A transceiver is responsible for establishing connection between a computer and Ethernet (LAN), as shown in Fig. 4.21.2.



(G-1417) **Fig. 4.21.2 : Use of transceiver to connect a Host to the Cable**

- The transceiver senses voltages on the cable to interprete the signals. It consists of analog circuits to interface with the cable and digital circuits for interfacing with the host.
- Depending on the signals on the cable, the transceiver can understand if another host is using the cable.
- **NIC** of each host would control the operations of its transceiver using the **network software** inside the host.
- At any given instant the Ethernet bus can be in any one of the following states :
  1. The bus is idle. No host is using it.
  2. The bus is busy that means it is carrying a legitimate signal.
  3. An erratic signal generated out of collision is present on the bus.
- The transceiver constantly monitors the bus status and decides the course of action.
- But the transceiver does not get connected to the host directly. Instead it is connected to the NIC. The NIC functions like a small computer as it has a small CPU, memory and a small instruction set of its own.
- The NIC performs all the functions related to network on behalf of the host.
- Each NIC has a unique **physical address** which identifies its host uniquely. (This address unique all over the world).
- Hence if NIC of a computer is replaced by another NIC then its physical address will change to that of the new NIC.
- The host gives instructions to NIC for data transfer from the host to cable and vice versa.
- When such instructions are received, the NIC would control the transceiver and carry out the desired operation as per the instruction.

Scanned by CamScanner

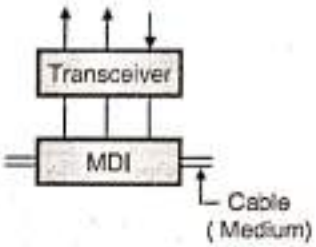


(G-1418)**Fig. 4.21.3 : Local organization of the NIC**

- The NIC carries out all the function without using the host's CPU. Fig. 4.21.3 shows the logical architecture of a NIC.
- A NIC contains a processor, a memory block and hardware for interfacing with the network.
- The steps followed for transmitting a file or message, by one host to the other host are as follows :
  1. The message is divided into different frames with each frame having a header and data. The header contains the source address and destination address and some other fields like CRC.
  2. The host sends each frame to its NIC. This frame is stored in NIC's memory.
  3. NIC checks the status of bus using transceiver and waits till the **idle** status of bus is obtained.
  4. After finding the idle status, the NIC sends the frame in a bit by bit manner. It also computes and inserts the CRC in the header of the frame being transmitted.
  5. If there is no collision taking place on the bus, then the frame will travel over the bus to all the nodes connected to it.
  6. The transceivers of every host receives the signal from the bus and converts them into bits and sends it in a bit by bit manner to the NIC of each host.
  7. These bits are stored in the memory of NIC of each host.
  8. NICs of each host will compare the destination address in the frame header with its own physical address. If the two match, the frame is retained otherwise it is discarded. Thus only the intended destination host will receive the frame.
  9. If the received frame is meant for itself (i.e. if the addresses match) then the NIC of the destination host carries out the CRC check on the received bits. If error is found then such frame will be discarded. No acknowledgements are provided for receiving or discarding a frame.
  10. The frames without any error are passed to the destination host for further processing.

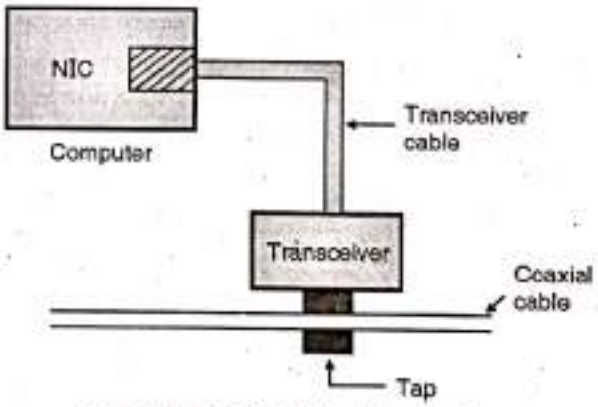
4.22 Transceivers :

- Transceiver is a combination of transmitter and receiver. It has the following functions to perform :
  1. To transmit signals over the transmission medium.
  2. To receive signals over the transmission medium.
  3. To detect collisions (in Ethernet LANs).
- Fig. 4.22.1 shows the simplified block diagram of a transceiver.



(G-1553)**Fig. 4.22.1 : Transceiver**

- A transceiver can be external or internal block of a computer. An internal transceiver is installed inside the computer on the network interface card (NIC) whereas an external transceiver is outside the station and mounted close to media.
- MDI in Fig. 4.22.1 is the medium dependent interface. It is used for connecting the transceiver (internal or external) to the medium (cable).
- The MDI is a piece of hardware. It can be in the form of a tap or T connector for an external MDI or a jack for an internal transceiver.
- Fig. 4.22.2 illustrates the connection of external MDI.
- Transceiver is directly attached to the tap. It detects when the line is idle and transmits the signal when the host wants to send a signal.
- Transceiver also receives the signal and through adapter applies it to the host.
- If the station uses an internal transceiver, then there is no need to use an external one and cable for its connection.



(L-640)**Fig. 4.22.2 : External transceiver**

4.23 Network Connecting Devices :

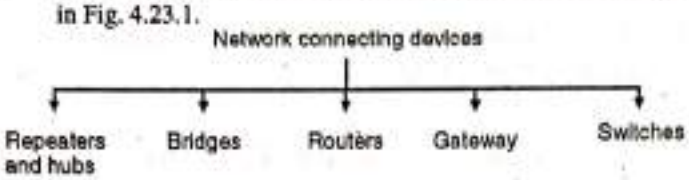
MU : Dec. 15, New Syll. : Dec. 18

University Questions

Q. 1 Write short notes on : Internetworking devices. **(Dec. 15, 10 Marks)**

Scanned by CamScanner

- Different types of network connecting devices are as shown in Fig. 4.23.1.

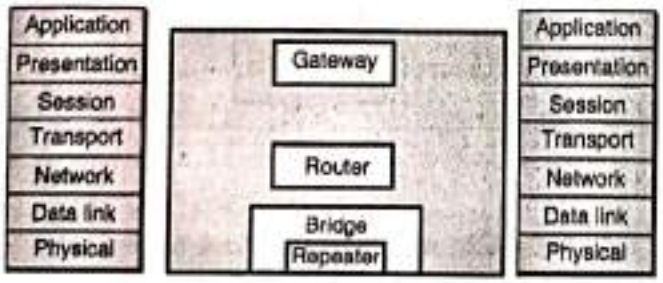


(G-348) **Fig. 4.23.1**

- The relation between OSI reference model and various connecting devices is shown in Fig. 4.23.2.

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. 4.23.2.



(G-806(a)) **Fig. 4.23.2 : Connecting devices and OSI model**

Categories of connecting devices :

Fig. 4.23.2 shows the relationship between the connecting devices and various layers of the internet model.

Table 4.23.1 : Role of networking devices

Sr. 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 seperate but compatible networks. It works in the network layer.
5.	Gateways	Gateways provide translation services between incompatible networks and works in all the layers.

4.24 Hubs :

MU : May 10, May 11, Dec. 11, May 12, Dec. 12, Dec. 13, Dec. 15

University Questions

Q. 1 Explain working of following network components and state in which layer they work. Repeaters, Hubs, Bridges, Routers, Switches, Gateways. **(May 10, May 11, Dec. 11, 10 Marks)**

Q. 2 What a neat diagram compare the uses and functions of different hardware components/devices used in an internetwork. **(May 12, 10 Marks)**

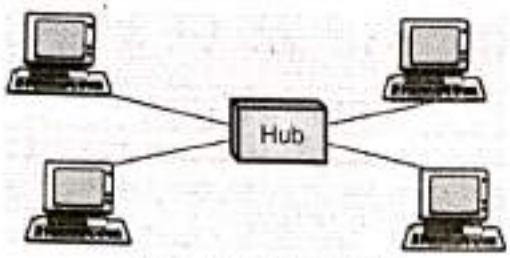
Q. 3 Explain with example : Hubs. **(Dec. 12, 2 Marks)**

Q. 4 Explain the functions of the different network hardware components. **(Dec. 13, 10 Marks)**

Q. 5 Write short notes on : Internetworking devices. **(Dec. 15, 10 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. 4.24.1.
- There are three main types of hubs :
  1. Passive hubs 2. Active hubs 3. Intelligent hubs

Scanned by CamScanner



(G-350) **Fig. 4.24.1 : Hub**

4.24.1 Passive Hubs :

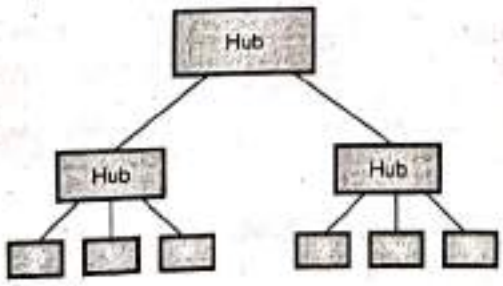
- A passive hub simply combines the signals of a network segments. There is no signal processing or regeneration. It merely acts as a connector.
- A passive hub reduces the cabling distance by half because it does not boost the signals and in fact absorbs some of the signal.
- With a passive hub, each 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.

4.24.2 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.

4.24.3 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. 4.24.2.



(L-646)**Fig. 4.24.2 : Hubs to create multiple levels of hierarchy**

4.25 Repeaters :

MU : Dec. 09, May 10, May 11, Dec. 11, May 12, Dec. 12, Dec. 13, Dec. 15

University Questions

Q. 1 What is the difference in functionalities between a bridge and a repeater ? Explain the process of learning in case of transparent bridge. **(Dec. 09, 10 Marks)**

Q. 2 Explain working of following network components and state in which layer they work. Repeaters, Hubs, Bridgers, Routers, Switches, Gateways. **(May 10, May 11, Dec. 11, 10 Marks)**

Q. 3 What a neat diagram compare the uses and functions of different hardware components/devices used in an internetwork. **(May 12, 10 Marks)**

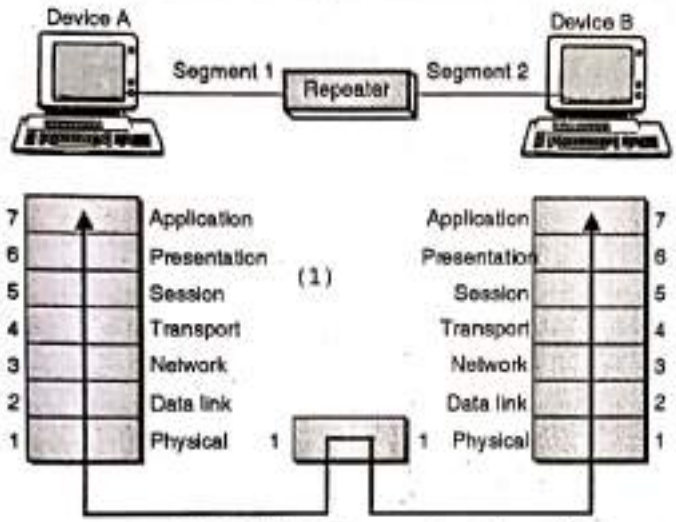
Q. 4 Explain with example : Repeater. **(Dec. 12, 2 Marks)**

Q. 5 Explain the functions of the different network hardware components. **(Dec. 13, 10 Marks)**

Q. 6 Write short notes on : Internetworking devices. **(Dec. 15, 10 Marks)**

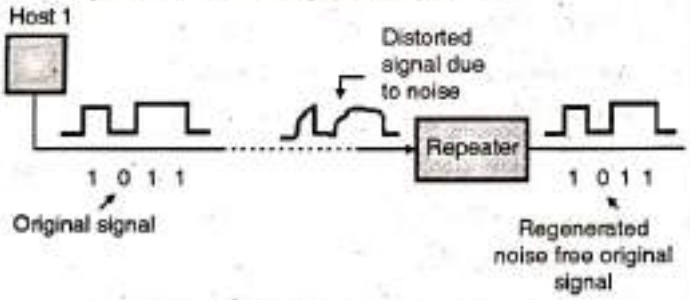
- A repeater is a connecting device which can operate only in the physical layer.
- All transmission media weaken the electromagnetic waves that travel through them.
- Attenuation of signals limits the distance any medium can carry data. Devices that amplifies signals to ensure data transmission are 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. 4.25.1(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. 4.25.1(a) and (b).
- A repeater does not connect two LANs. It connects only two devices connected in the same LAN.

Scanned by CamScanner



(G-351) **Fig. 4.25.1(a) : Repeater in OSI model**

- 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. 4.25.1(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.



(G-352) **Fig. 4.25.1(b) : Function of a repeater**

4.26 Bridges :

MU : Dec. 09, May 10, May 11, Dec. 11, May 12, Dec. 12, Dec. 13, Dec. 15

University Questions

Q. 1 What is the difference in functionalities between a bridge and a repeater ? Explain the process of learning in case of transparent bridge. **(Dec. 09, 10 Marks)**

Q. 2 Explain working of following network components and state in which layer they work. Repeaters, Hubs, Bridges, Routers, Switches, Gateways. **(May 10, May 11, Dec. 11, 10 Marks)**

Q. 3 What a neat diagram compare the uses and functions of different hardware components/devices used in an internetwork. **(May 12, 10 Marks)**

Q. 4 Explain with example : Bridges. **(Dec. 12, 2 Marks)**

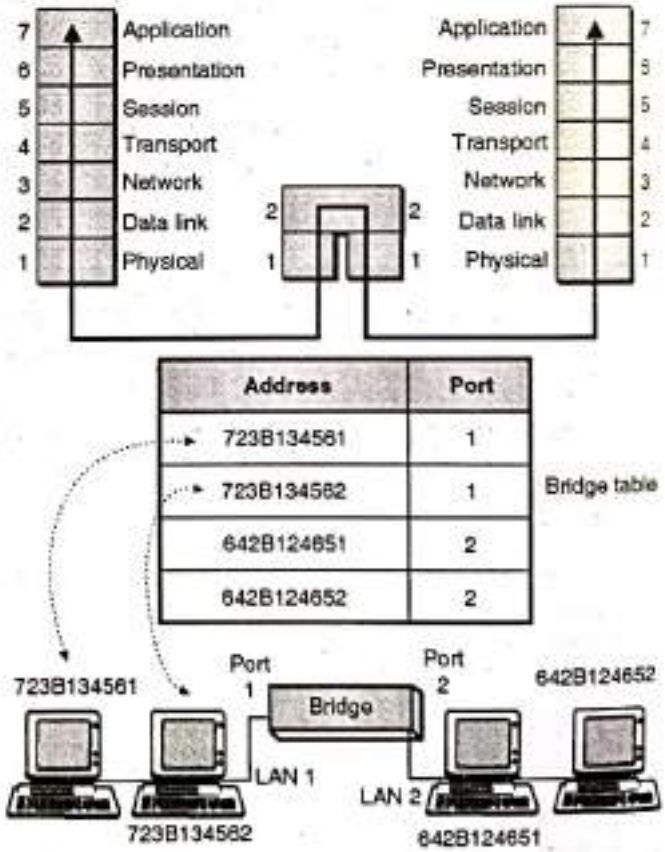
Q. 5 Explain the functions of the different network hardware components. **(Dec. 13, 10 Marks)**

Q. 6 Write short notes on : Internetworking devices. **(Dec. 15, 10 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. 4.26.1.
- 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. 4.26.1 a two port bridge is shown but in reality a bridge has more than two ports.



(G-354) **Fig. 4.26.1 : Bridge and bridge table**

- It is important to note that the bridges do not change the physical address contained in the frame.

Scanned by CamScanner

Types of bridges :

- The bridges are of two types :
  1. 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 :
  1. Filtering frames 2. Forwarding and 3. 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.

4.27 Routers :

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

University Questions

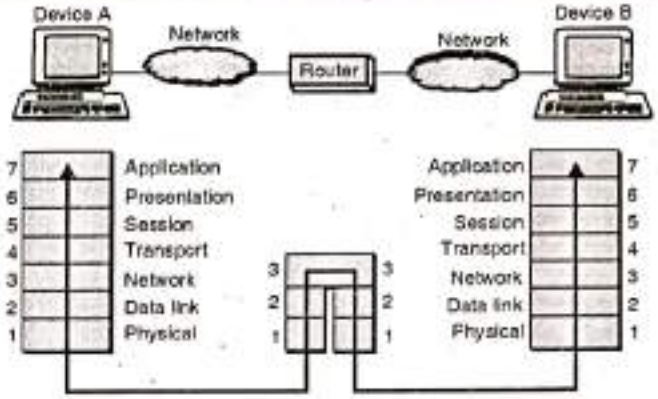
Q. 1 Explain working of following network components and state in which layer they work. Repeaters, Hubs, Bridges, Routers, Switches, Gateways. **(May 10, May 11, Dec. 11, 10 Marks)**

Q. 2 What a neat diagram compare the uses and functions of different hardware components/devices used in an internetwork. **(May 12, 10 Marks)**

Q. 3 Explain with example : Router. **(Dec. 12, 2 Marks)**

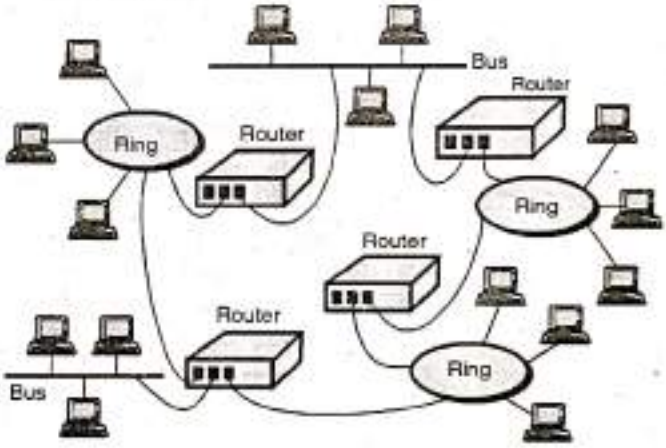
Q. 4 Explain the functions of the different network hardware components. **(Dec. 13, 10 Marks)**

- Routers are devices that connect two or more networks as shown in Figs. 4.27.1(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. 4.27.1(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.



(G-364) **Fig. 4.27.1(a) : A router in the OSI model**

- Each of the subnet is given a logical address. This allows the networks to be separate but still access each other and exchange data.



(G-365) **Fig. 4.27.1(b) : Routers in an internet**

- Data is grouped into packets, or blocks of data. Each packet has a * information. The two methods of route discovery are :
  1. Distance vector routing 2. 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.

4.28 Gateways :

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

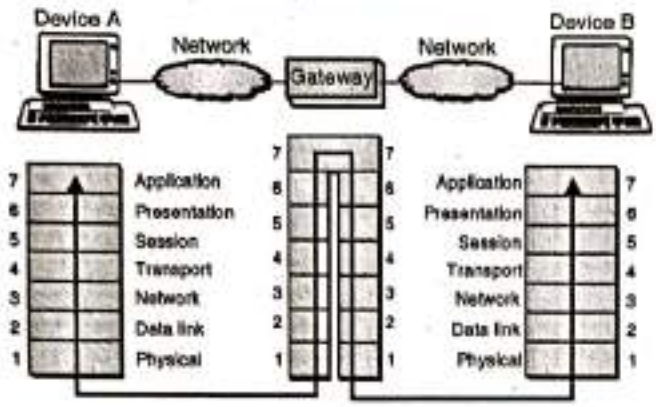
University Questions

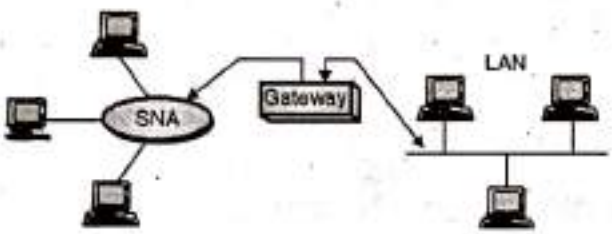
Q. 1 Explain working of following network components and state in which layer they work. Repeaters, Hubs, Bridgers, Routers, Switches, Gateways. **(May 10, May 11, Dec. 11, 10 Marks)**

Q. 2 What a neat diagram compare the uses and functions of different hardware components/devices used in an internetwork. **(May 12, 10 Marks)**

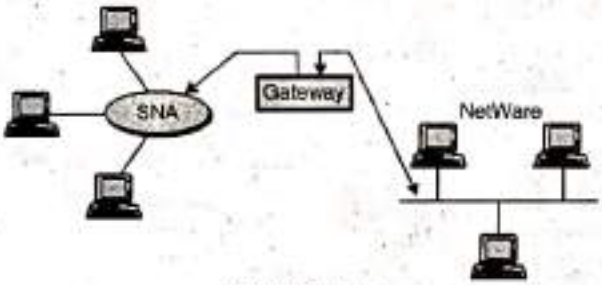
Q. 3 Explain the functions of the different network hardware components. **(Dec. 13, 10 Marks)**

Scanned by CamScanner





(a) A gateway in the OSI model



(b) A gateway

(G-366) Fig. 4.28.1

- 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. 4.28.1(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.

4.29 Switches :

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

University Questions

Q. 1 Explain working of following network components and state in which layer they work. Repeaters, Hubs, Bridgers, Routers, Switches, Gateways. **(May 10, May 11, Dec. 11, 10 Marks)**

Q. 2 What a neat diagram compare the uses and functions of different hardware components/devices used in an internetwork. **(May 12, 10 Marks)**

Q. 3 Explain with example : Switches. **(Dec. 12, 2 Marks)**

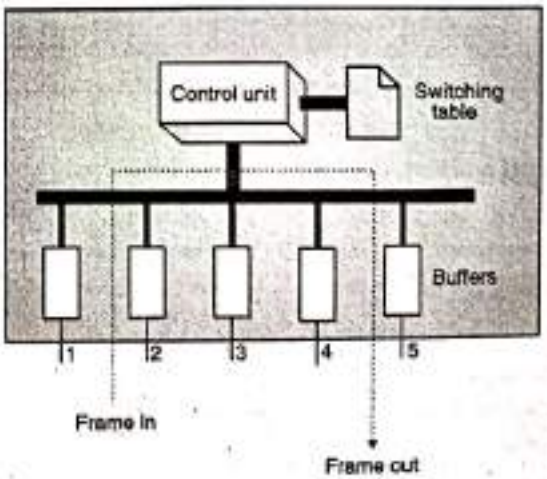
Q. 4 Explain the functions of the different network hardware components. **(Dec. 13, 10 Marks)**

- 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. 4.29.1. As shown in the Fig. 4.29.1 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-367) Fig. 4.29.1 : Switch

Scanned by CamScanner

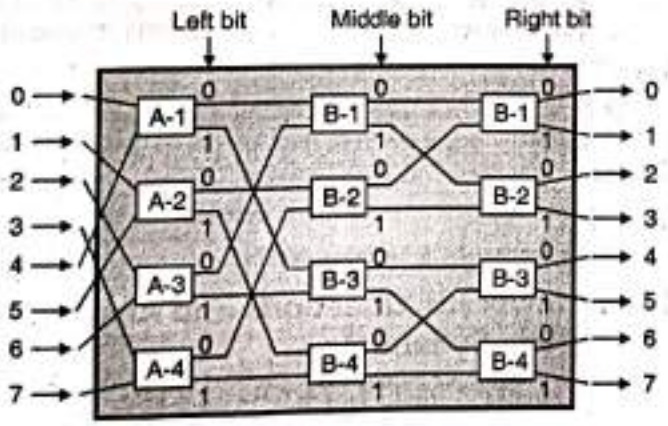
Note : Routing switches use the network layer destination address to find the output link to which the packet should be forwarded.

4.29.1 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.

4.29.2 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. 4.29.2.
- 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.



(G-368) **Fig. 4.29.2 : A three layer switch**

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

4.29.3 Comparison of Hub and Switch :

MU : Dec. 09, Dec. 10

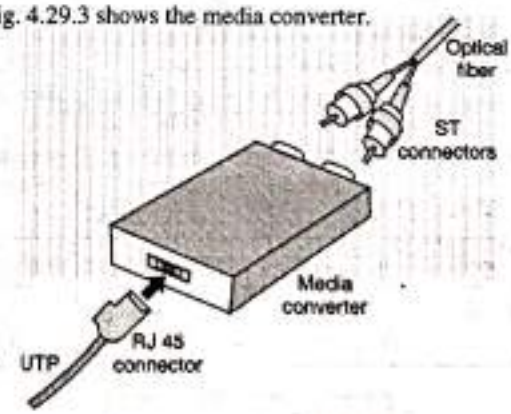
University Questions

Q. 1 Differentiate between Hub and Switch. **(Dec. 09, Dec. 10, 6 Marks)**

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.

4.29.4 Media Converters :

- 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. 4.29.3 shows the media converter.



(G-369) **Fig. 4.29.3 : Media converter**

- Various functions performed by a media converter are as follows :
  1. Connect two different types of wiring systems without an additional repeater.
  2. Connect two 10 Base T or 100 Base TX networks in different buildings using fiber-optic cable.

Scanned by CamScanner

3. 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.

4.29.5 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.

4.29.6 Comparison of Bridge, Switch and Hub :

Sr. No.	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

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. 19 How does the Token Ring LAN operate ?

Q. 20 Explain the frame format of 802.3, 802.4 and 802.5.

Q. 21 What is Fast Ethernet ?

Q. 22 Explain the LLC and MAC in IEEE 802 standard and explain the operation of CSMA/CD as used in LAN.

Q. 23 Write a short note on FDDI.

4.30 University Questions and Answers :

Q. 1 Consider the delay of pure ALOHA versus slotted ALOHA at low load. Which one is less ? Explain your answer. **(Dec. 2011, 5 Marks)**

Ans. :

With pure ALOHA transmissions can start instantly. At low load, no collisions are expected so the transmission is likely to be successful. With slotted ALOHA, it has to wait for the next slot. This introduces half a slot time delay on average.

(Refer section 4.4.5 for more details).

4.31 University Questions and Answers (New Syllabus) :

Dec. 2018 [Total Marks : 20]

Q. 1 Explain CSMA protocols. Explain how collision are handled in CSMA / CD.

(Sections 4.5, 4.5.1 and 4.5.2) **(10 Marks)**

Q. 2 Write a short note on Internetworking Devices.

(Section 4.23) **(10 Marks)**

□□□

Scanned by CamScanner

CHAPTER 5

Module 4

Network Layer

Syllabus

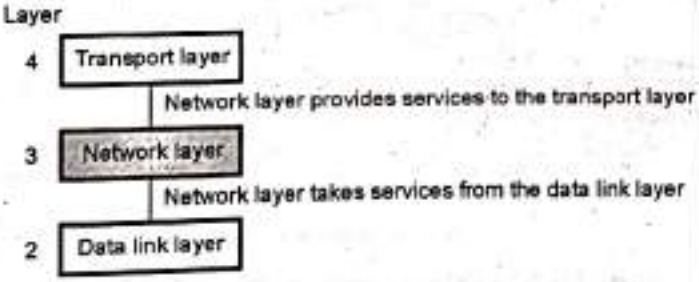
Network layer design issues, Communication primitives : Unicast, Multicast, Broadcast, IPv4 addressing (Classful and classless), Subnetting, Supernetting design problems, IPv4 protocol, Network Address Translation (NAT). **Routing algorithms :** Shortest path (Dijkastra's), Link state routing, Distance vector routing, **Protocols :** ARP, RARP, ICMP, IGMP, **Congestion control algorithms :** Open loop congestion control, Closed loop congestion control, QoS parameters, Token and leaky bucket algorithms.

5.1 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.

5.1.1 Position of Network Layer :

- Fig. 5.1.1 shows the position of network layer in the 5 layer internet model. It is the third layer.



(G-433) **Fig. 5.1.1 : Position of network layer**

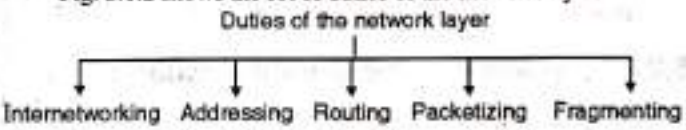
- It receives services from the data link layer and provides services to the transport layer.
- The network layer was designed to solve the problem of delivery through several links. The network layer is also called as the **Internetwork** layer.
- In addition to the host-to-host delivery the network layer is also responsible for **routing** the packets through the router.
- As a pure concept we can imagine that the Internet is a black box which connects a very large number of computers in the entire world together.
- But the Internet also is not a single network. It is infact the network of many networks or links.
- That means the Internet is an **internetwork** which is actually a combination of LANs and WANs.
- All these LANs and WANs are connected to each other via a connecting device such as a **router** which acts as a switch.

Routers :

Routers have many ports or interfaces. When it receives a packet at one of its ports, it forwards the packet through another port to the next switch or the final destination.

5.1.2 Network Layer Duties :

Fig. 5.1.2 shows the set of duties of the network layer.



(G-434) **Fig. 5.1.2 : 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 be able to uniquely define the connection of a computer to the Internet universally.

3. **Routing :**

   In a network, there are multiple roots available from a source to a destination and one of them is to be chosen.

Scanned by CamScanner

The network layer decides which root is to be taken. This is called as routing and it depends on various criterions.

4. Packetizing :

As discussed earlier, the network layer receives the packets from upper layer protocol and encapsulates them to form new packets.

This is called as packetizing. A network layer protocal called IP (Internetworking Protocol), does the job of packetizing.

5. Fragmenting :

The sent 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.

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 or ARP etc. in the network layer.

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.

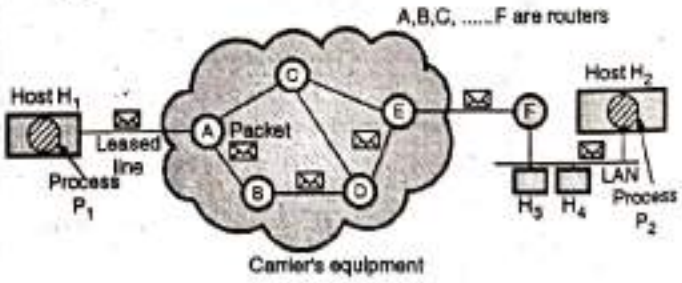
5.2 Network Layer Design Issues :

- 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.

5.2.1 Store and Forward Packet Switching :

- Refer Fig. 5.2.1 which demonstrates the environment of the network layer protocols.
- This system of Fig. 5.2.1 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. 5.2.1 : 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.

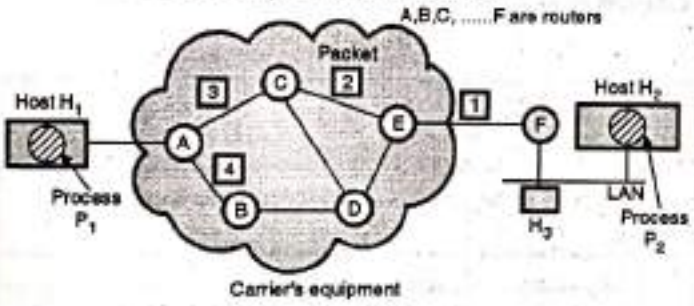
Scanned by CamScanner

5.2.2 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.

5.2.3 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. 5.2.2.

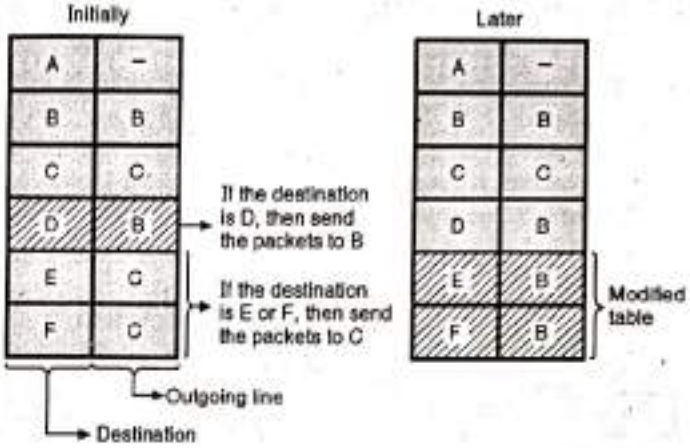


(G-436) **Fig. 5.2.2 : Routing within a datagram subnet**

- No advanced connection establishment is required. The packets are called as **datagrams** and the subnet is called as **datagram subnet**.

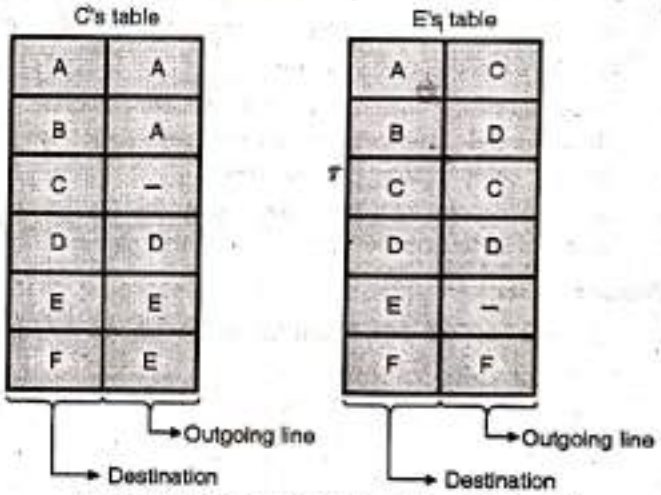
Working :

- 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. 5.2.2, 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. 5.2.2(a) shows the routing table of A. It has two tables named as **initially** and **later**.



(G-437) **Fig. 5.2.2(a) : Routing tables of A**

- 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. 5.2.2(a) as **later** and routed the 4th packet via path ABDEF.
- Fig. 5.2.2(b) shows the routing tables for C and E.



(G-438) **Fig. 5.2.2(b) : Routing tables of C and E**

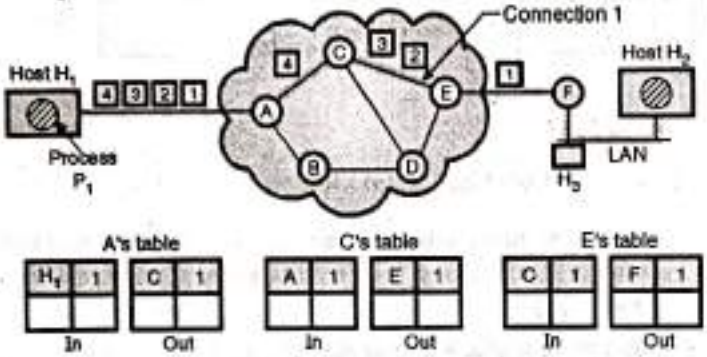
5.2.4 Implementation of Connection-Oriented Service :

- 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 opened, the virtual circuit is also terminated. In the connection oriented service, each packet

Scanned by CamScanner

carries an identifier. This identifier can tell us about the virtual circuit (VC) that this packet belongs to.

- Refer Fig. 5.2.3. 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. 5.2.3, 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.



(G-439) **Fig. 5.2.3 : Routing within a VC subnet**

5.2.5 Internal Organization of the Network Layer :

- Basically there are two philosophies for organizing the subnet :
  1. To use connection oriented service.
  2. 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 analogus 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.

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 set up 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.

5.2.6 Comparison of Virtual Circuit and Datagram Subnets :

MU : Dec. 09, May 10, May 11, May 12

University Questions

Q. 1 Differentiate between virtual-circuit and datagram subnets. **(Dec. 09, May 10, May 11, 10 Marks)**

Q. 2 Compare virtual circuits and datagram subnets and show their diagrammatic representation during congestion control. **(May 12, 10 Marks)**

Table 5.2.1 shows the comparison of VC subnet and datagram subnets.

Table 5.2.1

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.
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.

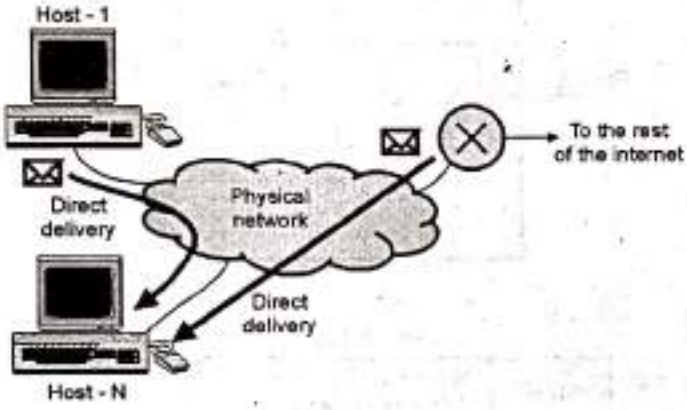
Scanned by CamScanner

5.3 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.

5.3.1 Direct Delivery :

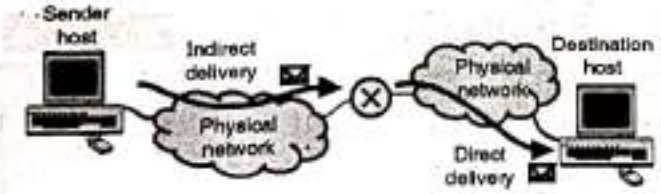
- In the direct delivery the destination host and the one who delivers the packet are in the same physical network as shown in Fig. 5.3.1(a).
- The sender can extract the network address of the destination using the mask. It then compares this address with the addresses of the networks to which it is connected. If these two addresses are identical then the delivery is direct.



(G-440) **Fig. 5.3.1(a) : Direct delivery**

5.3.2 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. 5.3.1(b).



(G-441) **Fig. 5.3.1(b) : Indirect delivery**

- In such a situation, the packets travel from one router to the other and are finally delivered to the destination host.
- The indirect delivery involves one direct and zero or more indirect deliveries. The last delivery is always a direct one.

5.4 Forwarding :

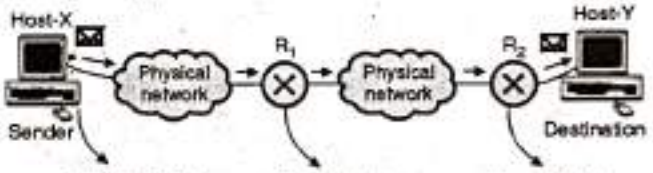
- Forwarding is defined as the process of placing the packet in its route towards its destination. Forwarding is possible only if the host or a router have a routing table of their own.
- A sender host or a router will refer to this routing table when it receives a packet and from the table they will 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.

5.4.1 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.

5.4.2 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. 5.4.1(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. 5.4.1(a).



Based on route

Destination	Route
Host Y	R_1, R_2, Host Y

Based on route

Destination	Route
Host Y	R_2, Host Y

Based on route

Destination	Route
Host Y	Host Y

Based on next hop

Destination	Next hop
Host Y	R_1

Based on next hop

Destination	Next hop
Host Y	R_2

Based on next hop

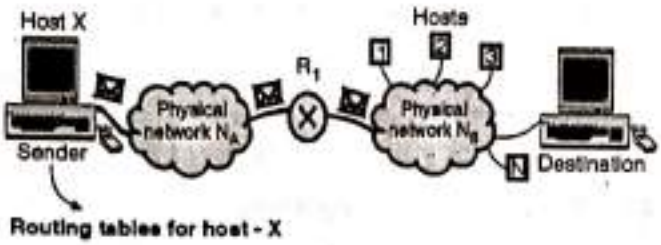
Destination	Route
Host Y	–

(G-442) **Fig. 5.4.1(a) : Route method versus Next Hop method**

5.4.3 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. 5.4.1(b).

Scanned by CamScanner



Host specific method

Destination	Next hop
Host - 1	R_1
Host - 2	R_2
⋮	⋮
Host - N	R_1

Network specific method

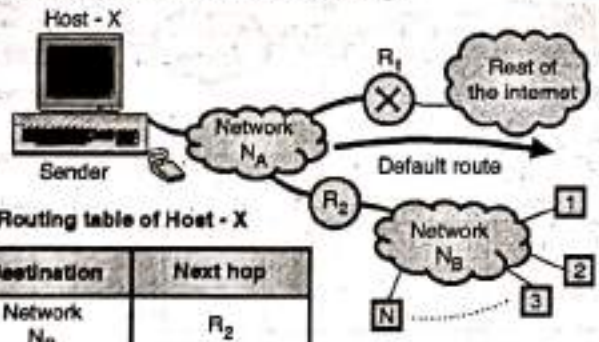
Destination	Next hop
Network N_B	R_1

(G-443) **Fig. 5.4.1(b) : Host specific method versus network specific method**

- That means we consider all hosts connected to the same network N_B as one single entry. This will reduce the routing table and simplify the searching process considerably.

5.4.4 Default Method :

- This is one more method of simplifying the routing tables. Refer Fig. 5.4.1(c) in which the sending host X is connected to a network with two routers R_1 and R_2.



Routing table of Host - X

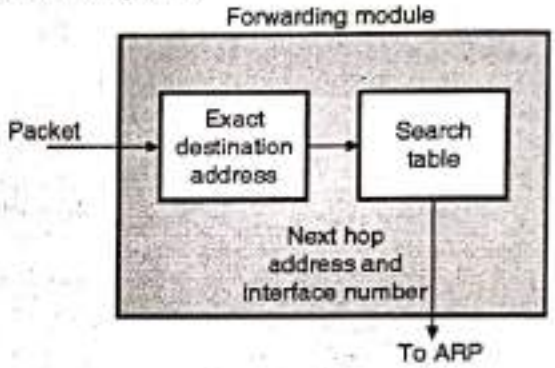
Destination	Next hop
Network N_B	R_2
Any other network	R_1

(G-444) **Fig. 5.4.1(c) : Default method**

- Router R_2 routes the packets to the hosts connected to network N_B. However router R_1 is used for the rest of the Internet.
- Hence in the routing table instead of listing all networks in the entire Internet, host X will have only one entry called as the default entry (normally defined as network address 0.0.0.0).

5.4.5 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 as shown in Fig. 5.4.2.



Search table

Mask	Network address	Next hop address	Interface
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....

(G-445) **Fig. 5.4.2 : Forwarding module in classless address**

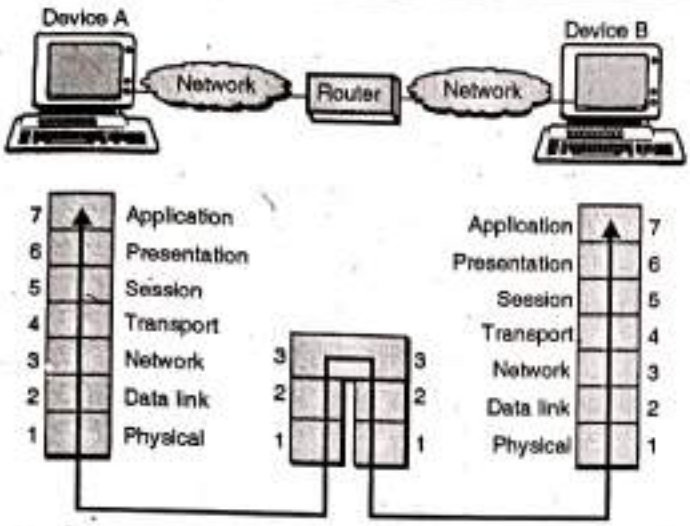
5.5 Routers : MU : May 04

University Questions

Q. 1 What does routing mean and how does it works ? Describe routing table structure. **(May 04, 10 Marks)**

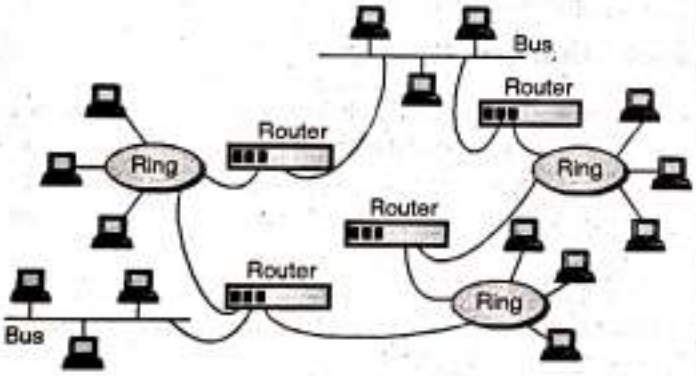
- Routers are devices that connect two or more networks as shown in Figs. 5.5.1(a) and (b). They consist of a combination of hardware and software.

Scanned by CamScanner



(G-446) **Fig. 5.5.1(a) : A router in the OSI model**

- 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 network can be interconnected through routers as shown in Fig. 5.5.1(b).



(G-447) **Fig. 5.5.1(b) : Routers in an internet**

- 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 :
  1. Distance vector routing
  2. 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.

5.5.1 Routing Tables : MU : May 04

University Questions

Q. 1 What does routing mean and how does it works ? Describe routing table structure.

(May 04, 10 Marks)

- The routing table for a host or a router consists of an entry for each destination, or a combination of destinations to route the IP packets.
- Routing tables can be of two types :
  1. Static routing tables 2. Dynamic routing tables

1. Static routing table :

- The information in the static routing tables is entered manual. The route of a packet to each destination is entered into the table by the administrator.
- This routing table can not 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 BGB.
- The structure of a dynamic routing table is shown in Table 5.5.1.

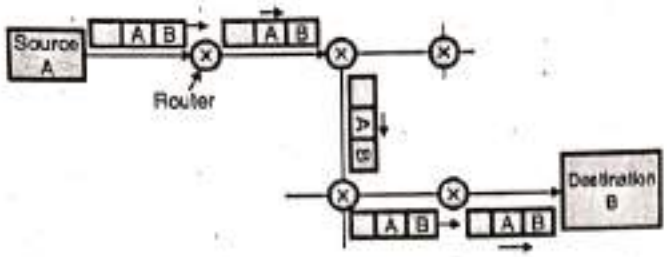
Table 5.5.1 : Format of dynamic routing table

Mask	Network Address	Next hop address	Interface	Flags	Reference count	Use

5.5.2 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. 5.5.2.

Scanned by CamScanner



(G-448) **Fig. 5.5.2 : 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 can not find the destination address.

Metric :

- A metric is defined as the cost assigned for passing through a network.
- The metric assigned to each network depends on the type of protocol.

Interior and exterior routing :

- An Internet is so large that for one routing protocol it is impossible to handle the task of updating the routing tables of all the routers.
- So an Internet is divided into a number of autonomous systems (AS). An AS is group of networks and routers.

Interior routing :

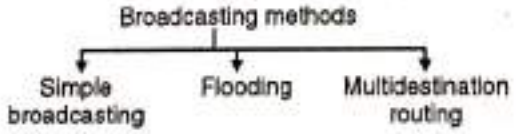
The routing that takes place inside an AS is called as interior routing.

Exterior routing :

The routing that takes place among various autonomous systems is called as exterior routing.

5.5.3 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**.
- Various methods of broadcasting are as follows :



(G-449) **Fig. 5.5.3 : Various methods of broadcasting**

1. Simple broadcasting :

In this method the source will simply send a distinct (a separate) packet to each destination.

This method has two drawbacks :

1. A lot of bandwidth is wasted.
2. The source has to have a complete list of all destinations.

2. Flooding :

Flooding is another method used for broadcasting. The problem with flooding is that it has a point to point routing algorithm. So it consumes a lot of bandwidth and generates too many packets.

3. Multidestination routing :

- This is the third algorithm used for broadcasting.
- In this algorithm each packet will contain a list of destinations or a bit map which indicates the desired destination.
- When such a packet arrives at a router, the router first checks all the destinations. Then it decides the set of output lines that will be required based on the destination addresses.
- The router then generates a new copy of the received packet for each output line to be used. It includes a list of only those destinations that are to use the line in each packet going out on that line. This will save bandwidth to a great extent. Also generation of too many packets right from the sending end will also be avoided.

5.5.4 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.

5.6 Network Layer Services :

- The duty of the network layer in TCP/IP is to provide the host-to-host delivery of datagrams.
- In this section we are going to discuss the services that are expected from the network layer.
- At the sending end, the network layer will accept a packet from its transport layer, encapsulate the packet into datagram and will deliver the packet to the data link layer.
- At the destination, exactly opposite process takes place. That means, at the destination the received datagram is decapsulated to extract the packet from it and the packet is delivered to the transport layer.

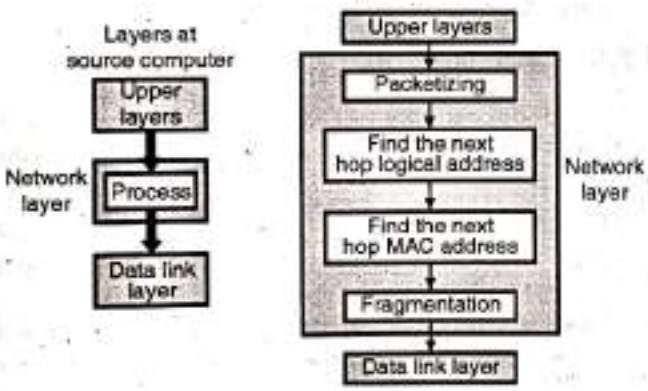
Scanned by CamScanner

5.6.1 Logical Addressing :

- The two computers in communication with each other should have some universal identification system which is called as the **network layer address or logical address.** Thus the sending and receiving computers must have two network-layer addresses for them to communicate.

5.6.2 Services Provided at the Source Computer :

- The following four services are provided by the network layer at the source computer :
  1. Packetizing.
  2. To find the logical address of the next hop.
  3. To find the physical or MAC address for the next hop.
  4. Fragmentation of the datagram if necessary.
- These services are as shown in Fig. 5.6.1(b).
- The upper layers (transport and application) take services of the network layer. For this the upper layers send several pieces of information.
- The network layer processes these pieces of information and creates fragmented datagrams alongwith the next hop MAC address to finally deliver it to the data link layer as shown in Fig. 5.6.1(a).



(a) Network layer process **(b) Network layer services**

(G-1999) **Fig. 5.6.1**

1. Packetizing :

- **Packetizing** is the first duty of the network layer in which it encapsulates the payload (data received from the transport layer) in a packet at network layer at the source. Then at the destination the decapsulation process takes place.
- In this way the network layer is doing the job of a postal service in delivering the packages from source to destination.

At the source :

At the sending end the events take place in the following sequence :

1. The payload (data) from the upper layer is received.
2. A header containing the source and destination address and some other information is added to the payload.
3. This packet is then delivered to the data layer.
4. If the payload is too large, then the host carries out **fragmentation** on it. Otherwise the host is not allowed to modify the contents of the payload.

2. Finding the logical address of the next hop :

- The datagram prepared with packetizing contains the source and destination addresses of the packet.
- The datagram is to be delivered to the next router. But the source and destination addresses in the datagram do not give any information about the logical address of the next hop.
- The network layer at the source computer finds the logical address of the next hop by consulting a routing table.

3. Finding MAC address of next hop :

- Note that it is the duty of data link layer (and not of network layer) to actually deliver the datagram to the next hop.
- And to do this the data link layer needs the physical or MAC address of the next hop.
- The network layer uses another table to map the logical address of next hop into the corresponding MAC address of next hop.
- However generally an auxiliary protocol called as ARP (Address Resolution Protocol) is used for this purpose.

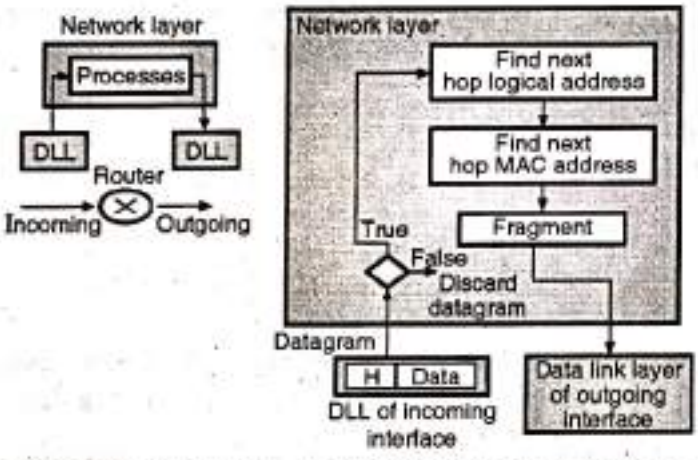
4. Fragmentation :

- The datagram at this stage may not always be ready to be given to the data link layer. The LANs and WANs can carry the data of a limited size in a frame.
- If the data is longer than the maximum specified size for LANs and WANs then it is not possible to fit it in one frame.
- In such circumstances, the datagram should be **fragmented** in to smaller data units before passing it to the data link layer.
- The datagram header is copied into all these fragments so that all the necessary information in the datagram is present in every fragment.
- In addition to this some more information regarding the position of that fragment in the whole datagram should be added to the header of the fragment.

Scanned by CamScanner

5.6.3 Services Provided at Each Router :

- The routers present in between the source and destination are supposed to check the source and destination addresses in the packet in order to forward it to the next network on the path.
- The router is not allowed to decapsulate the received packet unless it is too big and fragmentation needs to be carried out on it.
- The routers are not supposed to change the source and destination addresses.
- In the event of fragmentation, a router has to copy the header in all the fragments.
- At the router the services provided by the network layer are as follows :
  1. To find the next hop logical address.
  2. To find the next hop MAC address.
  3. To carry out fragmentation if required.
- Fig. 5.6.2 shows all these services.



(a) Process at the router **(b) Services provided at the router**

(G-2000) **Fig. 5.6.2**

- Before providing the services mentioned above the router checks the validity of the incoming datagram with the help of checksum.
- In checking the validation, the following two things are checked :
  1. Whether the datagram header is corrupted.
  2. Whether the datagram is delivered to the correct router.
- If the incoming datagram fails the validation test then it is simply discarded as shown in Fig. 5.6.2(b).

5.6.4 Services Provided at the Destination Computer :

- The sequence of events taking place at the destination is as follows :
  1. The network layer packet is received from the data link layer.
  2. The received packet is decapsulated and the payload is delivered to the upper layer protocol.
  3. If a large packet is fragmented by either the source host or a router, then the responsibility of the network layer at the destination is to wait until all fragments are received, reassemble them and deliver them to the upper layer protocol.
- The network layer at the destination computer is much simpler than that at the source computer or router.
- Before providing any service, the received datagram should be subjected to validation. If it passes the validation test then all the services mentioned above should be provided. Otherwise the datagram is discarded.
- The network layer also sets a reassembly timer when it receives fragments of a datagram that are to be reassembled.
- If the reassembly timer expires before arrival of all the fragments, then all data fragments are destroyed and an error message is sent that the entire fragmented datagram be sent again.

5.7 Other Services :

- The other services expected from the network layer are as follows :
  1. Error control.
  2. Flow control.
  3. Congestion control.
  4. Quality of service (QoS).
  5. Security.
- Let us discuss them one by one.

5.7.1 Error Control :

- Eventhough it is possible to implement the error control at the network layer level, the design engineers have neglected this issue.
- One possible reason for this is that the packets may get fragmented at every router due to which the error checking becomes inefficient.
- However a **checksum** field has been added to the datagram in order to control any corruption in the header only. The error control is not applicable to the whole datagram.
- Thus there is no direct error control provided by the network layer in the Internet. But an auxiliary protocol ICMP is used by the Internet for providing some error control to the datagram.

5.7.2 Flow Control :

- The purpose of providing the flow control is to regulate the data rate of the source so as to avoid the receiver getting overwhelmed.
- The receiver will be overwhelmed if the upper layers at the sending end are producing data at a rate which is higher than the rate at which the upper layers at the destination can consume it (data).

Scanned by CamScanner

- So as to control the sender's data rate, some kind of a feedback mechanism should be setup so that the receiver can tell the source that it (receiver) has overwhelmed with excess data.
- It is important to remember that the network layer does not directly provide any flow control.
- The flow control is not provided at the network layer level because it is provided for most of the upper layer protocols and there is no need to provide flow control again which makes the design of network layer complex.

5.7.3 Congestion Control :

- This is another important issue to be handled at the network layer. **Congestion** will take place if the source computer sends more datagrams than the capacity of the network or routers.
- In this situation, the routers will drop some of the received packets.
- But this will make the congestion worse because the error control mechanism present at the upper layers will retransmit the packets dropped by the routers.
- Sometimes the congestion becomes so bad that the system collapses and no datagrams are delivered at the destination.
- The congestion control at the network layer is never implemented in the Internet.

5.7.4 Quality of Service (QoS) :

- The quality of service in the Internet has become more important since new applications like multimedia communication have been introduced.
- The Internet has grown as it successfully provides the quality of service to support all the modern day applications.
- However the QoS provisions are not implemented in the network layer. They are mostly implemented in the upper layers.

5.7.5 Security :

- During the early days of the Internet, security was not a major design concern due to limited (small) number of users. Hence the network layer was designed without any security provisions.
- But security has become a big concern now. But network layer is connectionless. Hence to provide security at the network layer we need to have another virtual level in order to change the connectionless service to connection oriented one.
- The virtual layer is known as IPsec.

5.8 IPv4 Addresses :

- Each computer connected to the Internet should be identified uniquely. The identifier used for this purpose is called as the **Internet address** or IP address.
- The hosts and routers on the Internet have unique IP addresses.
- The current version of IP (Internet Protocol) is IPv4 whereas the advanced version is IPv6.
- The IPv4 address is a 32-bit address and it is used for defining the connection of a host or router to the Internet. **Thus an IP address is an address of the interface.**

5.8.1 Uniqueness of IP Addresses :

- The IP address is **unique** and **universal.** That means each IP address defines only **one connection** to the Internet.
- At any given time, no two devices connected to the Internet can have the same IP address.
- But if a device is connected to the Internet via two connections through two different networks, then it can have two different IP addresses.
- All the IPv4 addresses are 32 bit long and they are used in the source address and destination address fields of the IP header.
- The IP addresses for hosts are assigned by the network administrator. For Internet it has to be obtained from the network information center.

5.8.2 Address Space :

- The IPv4 protocol has an address space. It is defined as the total number of addresses used by the protocol.
- If N 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.
- Thus **the address space** of IPv4 is 2^{32}.

5.8.3 Notation :

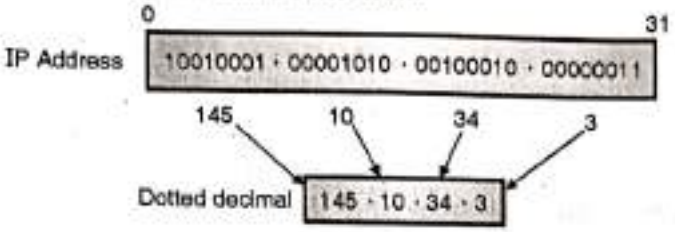
- The IPv4 addresses can be shown use three different notations as follows :
  1. Binary notations (base 2).
  2. Dotted decimal notation (base 256).
  3. Hexadecimal notation (base 16).
- Out of these the **dotted decimal** notation is most commonly used.

Dotted decimal notation :

- This notation has become popular because of the two advantages it offers. This notation makes the IPv4 address more compact and easy to read.
- The 32 bit IPv4 address is grouped into groups of 8-bits each separated by decimal points (dots).
- Each 8-bit group is then converted into an equivalent decimal number as shown in Fig. 5.8.1.
- Each octet (byte) can take a value between 0 and 255. Therefore the IPv4 address in the dotted decimal notation has a range from 0.0.0.0 to 255.255.255.255.
- For example the IPv4 address of

Scanned by CamScanner

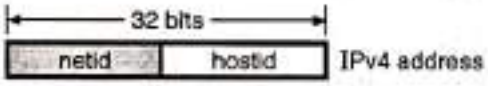
1001 0001.00001010 00100010 00000011 is denoted in the dotted decimal form as 145.10.34.3.



(G-2001) **Fig. 5.8.1 : Dotted decimal notation**

5.8.4 IPv4 Address Format :

- A 32 bit IPv4 address consists of two parts. The first part is called as **net id** i.e. network identification which identifies a network on the Internet and the second part is called as the **host id** which identifies a host on that network.
- Fig. 5.8.2 shows the IPv4 address format. Note that the **net id** and **host id** are of variable lengths depending on the class of address.
- Note that class D and E addresses are not divided into net id and host id for the reasons discussed later on.



(G-2002) **Fig. 5.8.2 : IPv4 address format**

5.9 Classful Addressing : MU : May 10

University Questions

Q. 1 Explain classful addressing in IPv4. **(May 10, 10 Marks)**

- The concept of IP addresses is few decades old. It uses the concept of **classes.** This architecture is called as the **classful addressing.**
- Later on in mid 1990s a new architecture of addressing was introduced which was known as **classless addressing.** This new architecture has superseded the original architecture.
- In this section we are going to discuss the classful addressing.

5.9.1 IPv4 Address Classes :

MU : Dec. 05, Dec. 06, Dec. 07, May 08, May 09, May 10, May 17, New Syll. : Dec. 18

University Questions

Q. 1 Describe the classification of IP-addresses in IPv4. **(Dec. 05, 5 Marks)**

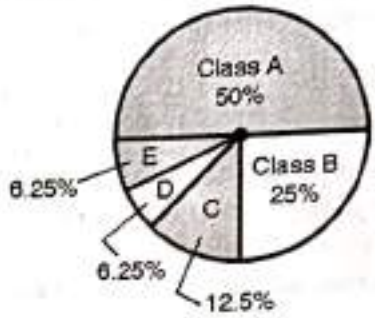
Q. 2 Explain the following term : IP address. **(Dec. 06, Dec. 07, May 08, May 09, 10 Marks)**

Q. 3 Discuss various special IP addresses. **(May 09, 10 Marks)**

Q. 4 Explain classful addressing in IPv4. **(May 10, 10 Marks)**

Q. 5 Explain with examples the classification of IPv4 addresses. **(May 17, 5 Marks)**

- In the classful addressing architecture, the IP address space has been divided into five classes : A, B, C, D and E.
- Fig. 5.9.1 shows the percentage of occupation of the address space by each class.
- The number of class A addresses is the highest i.e. 50% and those of classes D and E is the lowest i.e. 6.25%.



Class	No. of addresses	
A	2^{31}	50%
B	2^{30}	25%
C	2^{29}	12.5%
D	2^{28}	6.25%
E	2^{28}	6.25%

(G-2003) **Fig. 5.9.1 : Classful addressing occupation of address space**

5.9.2 Formats of Various Classes :

MU : Dec. 05, Dec. 06, Dec. 07, May 08, May 09, May 17

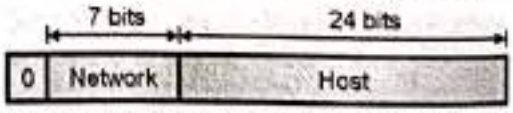
University Questions

Q. 1 Describe the classification of IP-addresses in IPv4. **(Dec. 05, 5 Marks)**

Q. 2 Explain the following term : IP address. **(Dec. 06, Dec. 07, May 08, May 09, 10 Marks)**

Q. 3 Discuss various special IP addresses. **(May 09, 10 Marks)**

Q. 4 Explain with examples the classification of IPv4 addresses. **(May 17, 5 Marks)**



(G-531) **Fig. 5.9.2(a) : Class A IPv4 address formats**

Class A format :

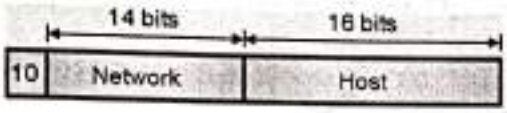
- The formats used for IPv4 address are as shown in Fig. 5.9.2. The IPv4 address for class A networks is shown in Fig. 5.9.2(a).

Scanned by CamScanner

- The network field is 7 bit long as shown in Fig. 5.9.2(a) and the host field is of 24 bit length. So the network field can have numbers between 1 to 126.
- But the host numbers will range from 0.0.0.0 to 127.255.255.255.
- Thus in class A, there can be 126 types of networks and 17 million hosts.
- The "0" in the first field identifies that it is a class A network address.

Class B format :

- The class B address format is shown in Fig. 5.9.2(b).
- The first two fields identify the network, and the number in the first field must be in the range 128 - 191.

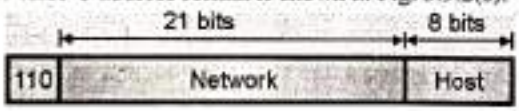


(G-532) **Fig. 5.9.2(b) : Class B format**

- 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. 5.9.2(c).



(G-533) **Fig. 5.9.2(c) : Class C format**

- The first block in class C covers addresses from 192.0.0.0 to 192.0.0.255 and the last block covers addresses from 223.255.255.0 to 223.255.255.255.

Class D format :

- The class D address format is shown in Fig. 5.9.2(d).

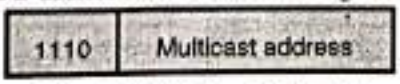


Fig. 5.9.2(d) : Class D format

- The class format allows for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

Class E address format :

- Fig. 5.9.2(e) shows the address format for a class E address. This address begins with 11110 which shows that it is reserved for the future use.

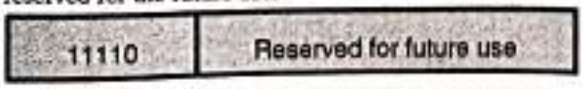
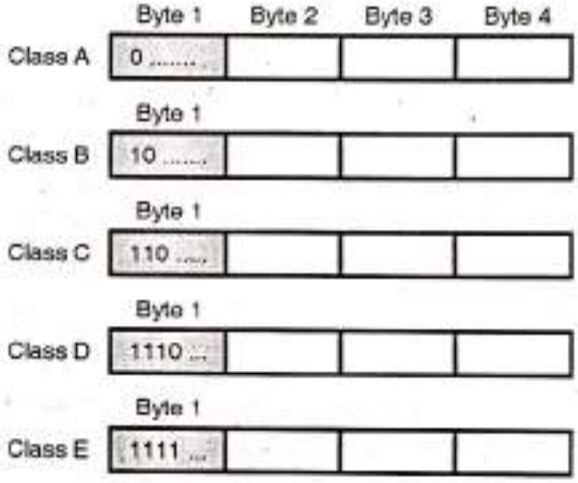


Fig. 5.9.2(e) : IPv4 address for class E network

- The 32 bit (4 byte) network addresses are usually written in dotted decimal notation. In this notation each of the 4-bytes is written in decimal from 0 to 255.
- So the lowest IP address is 0.0.0.0 i.e. all the 32 bits are zero and the highest IPv4 address is 255.255.255.255.

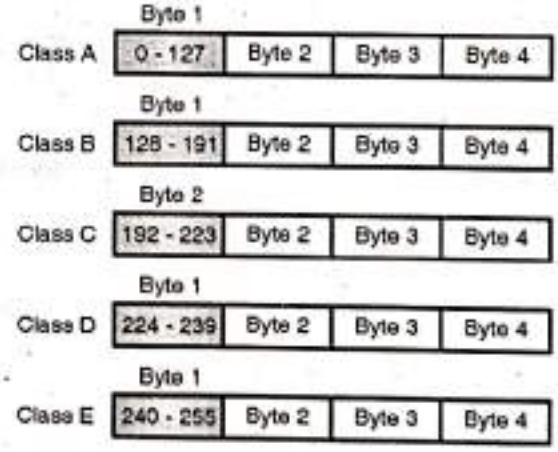
5.9.3 How to Recognize Classes ?

- When an IPv4 address is given to us either in the binary or dotted decimal notation, we can find the class of the address.
- If the given address is in the binary notation then we can identify its class by inspecting the first few bits of the address. This is as shown in Fig. 5.9.3(a).



(G-2004) **Fig. 5.9.3(a) : Finding the address class**

- If the given address is in the dotted decimal notation then we can identify the address class by inspecting the first byte of the address. This is as shown in Fig. 5.9.3(b).



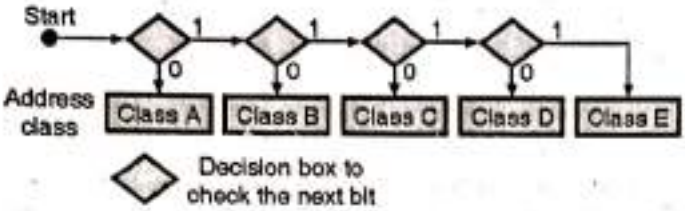
(G-2005) **Fig. 5.9.3(b) : Finding the address class**

- It is important to note here that there are some special addresses which fall in class A or E. These special addresses are to be treated as the exceptions to the classful addressing. We have discussed them later in the chapter.
- In computers, the IPv4 addresses are generally stored in the binary notation format. Therefore it is possible to write an

Scanned by CamScanner

algorithm which can identify the address class by using the continuous checking process.

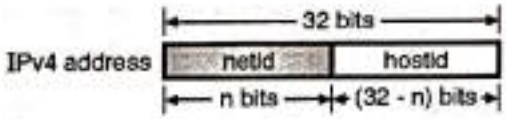
- The principle of such an algorithm has been shown in Fig. 5.9.4.



(G-2006) **Fig. 5.9.4 : Algorithm to identify address class**

5.9.4 Two Level Addressing :

- The IPv4 addressing is used for defining a destination for an Internet packet at the network layer.
- At the time when classful addresses were designed, the Internet was considered as the network of networks. In other words the whole Internet was divided into a number of smaller networks with many hosts connected to each network.
- Normally an organization which wants to connect to the Internet creates a network and the Internet authorities allocate a block of address to the organization. These addresses can be in class A, B or C.
- All the addresses allotted to an organization belong to a single block. Therefore each IPv4 address in classful addressing system is made up of two parts namely **net id** and **host id** as shown in Fig. 5.9.5.



(G-2007) **Fig. 5.9.5 : Two level addressing in classful addressing**

- The job of the **net id** is to define a network and that of the **host id** is to define a particular host in that network.
- As shown in Fig. 5.9.5 if n bits define **net id** then the remaining (32-n) bits define **host id.**
- The value of "n" is not same for all the classes. Infact it is depend on the class as shown in Table 5.9.1.

Table 5.9.1

Class	Value of n
A	n = 8
B	n = 16
C	n = 24

5.9.5 Extracting Information in a Block :

- A block is nothing but a range of addresses. For any given block we would be interested to extract the following three pieces of information :
  1. The total number of addresses in the block.
  2. The first address of the block.
  3. The last address in the block.
- Before extracting all this information, we have to identify the class of the address as discussed earlier.
- Once we find the class of the block, we will have the values of "n" (the length of **net id** in bits) and (32 – n) i.e. the length of the **host id** in bits.
- It is now possible to obtain the three pieces of information mentioned above as shown in Fig. 5.9.6.

1. Total number of addresses in the block :

The total number of IPv4 addresses in the given block will be equal to,

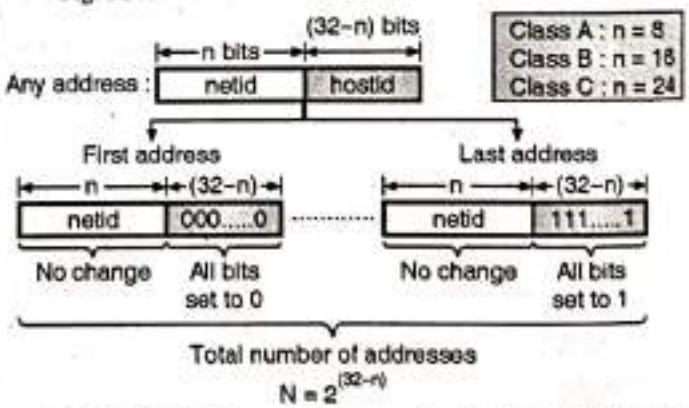
$$N = 2^{(32-n)} \quad \text{...(5.9.1)}$$

2. First address in the block :

The first address in the given block can be obtained by keeping the leftmost "n" bits in the address as it is and setting all the (32 – n) rightmost bits to 0 as shown in Fig. 5.9.6.

3. Last address in the block :

The last address in the given block can be obtained by keeping the leftmost "n" bits in the address as it is and then setting all the (32 – n) rightmost bits to 1 as shown in Fig. 5.9.6.

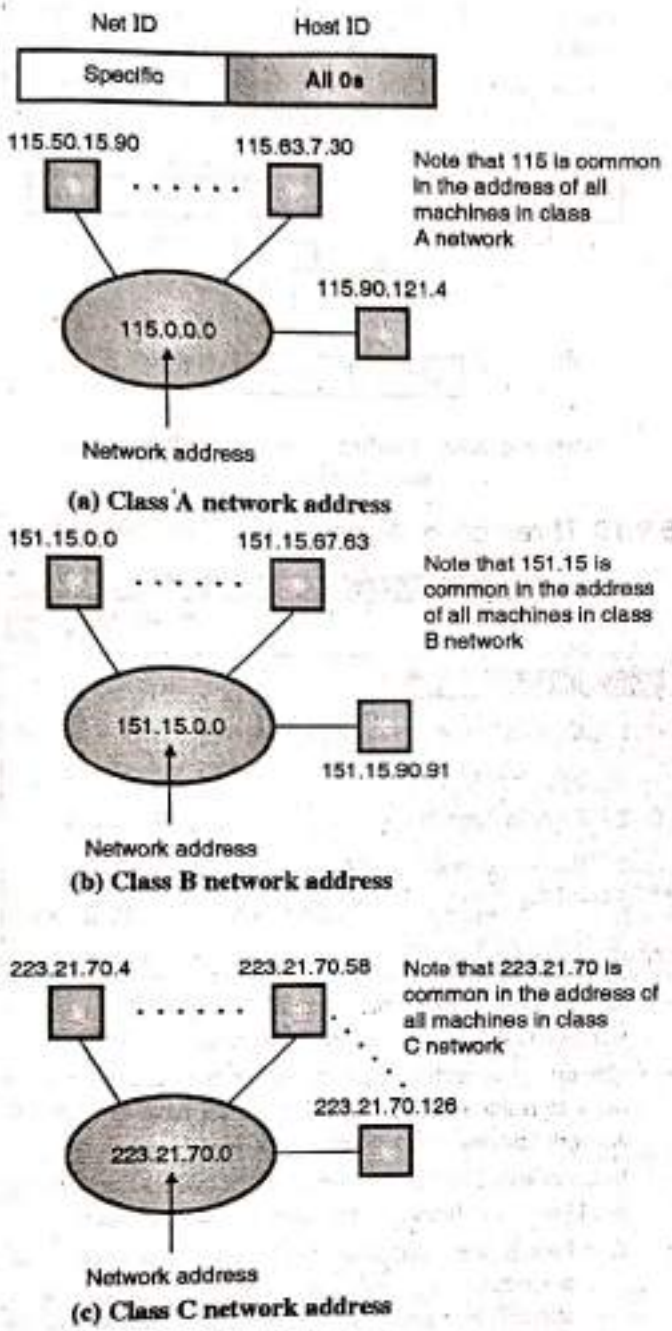


(G-2008) **Fig. 5.9.6 : Information extraction in classful addressing**

5.9.6 Network Address :

- The network address is an address that defines the network itself. It cannot be assigned to a host. Fig. 5.9.7 shows the examples of network addresses for different classes.

Scanned by CamScanner



(a) Class A network address

(b) Class B network address

(c) Class C network address

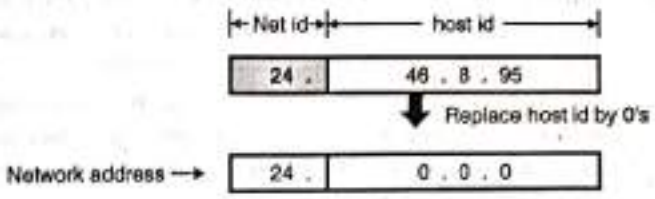
(G-536) Fig. 5.9.7

- The following examples will enable you to find the network address.

Ex. 5.9.1 : 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. 5.9.1.



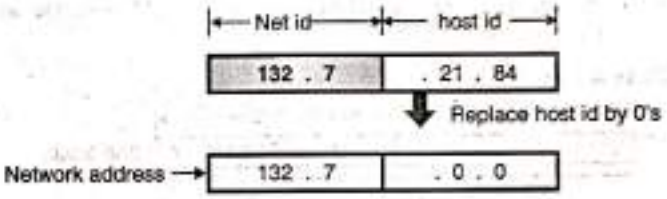
(G-537) Fig. P. 5.9.1

So the network address is 24.0.0.0.

Ex. 5.9.2 : For the address 132.7.21.84 find the type of network and the network address.

Soln. :

- Examine the first byte. It is 132 i.e. between 128 and 192. So it is a class B network.
- So the first two bytes define the net id. Replace the host id with 0's to get the network address as shown in Fig. P. 5.9.2.



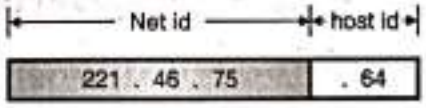
(G-538) Fig. P. 5.9.2

So the network address is 132.7.0.0.

Ex. 5.9.3 : 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. 5.9.3.



(G-539) Fig. P. 5.9.3

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.

5.9.7 Network Mask or Default Mask :

MU : Dec. 06

University Questions

Q. 1 Explain subnetting and masking with suitable examples. **(Dec. 06, 10 Marks)**

Scanned by CamScanner

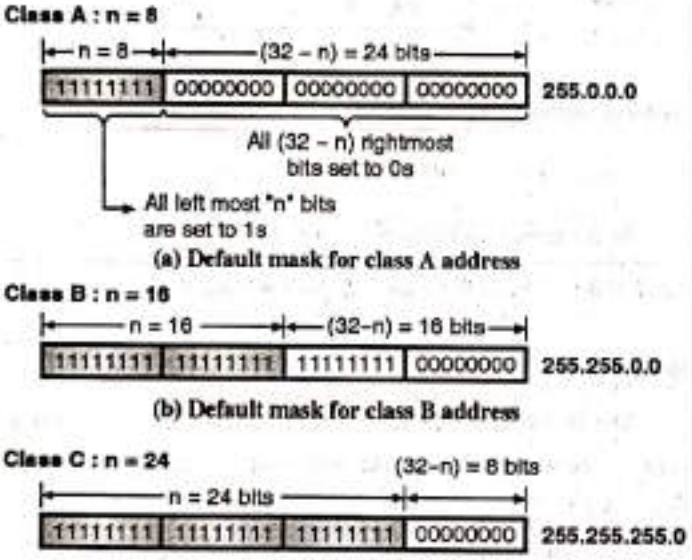
- Earlier we have discussed the methods for extracting different pieces of information. But all these methods are theoretical methods which are useful in explaining the concept.
- But practically these methods are not used. When a packet arrives at the input of the router in the Internet, it uses an algorithm to extract the **network address** from the destination address in the received packet.
- This can be achieved by using a **network mask.**

Definition of default mask :

A **network mask** or **default mask** in classful addressing is defined as a 32-bit number obtained by setting all the "n" leftmost bits to 1s and all the (32 – n) rightmost bits to 0.

5.9.8 Default Masks for Different Classes :

- We know that the value of n is different for different classes. Therefore their default masks also will be different.
- The default masks for class A, B and C addresses are as shown in Fig. 5.9.8.



(a) Default mask for class A address

(b) Default mask for class B address

(c) Default mask for class C address

(G-2009) Fig. 5.9.8

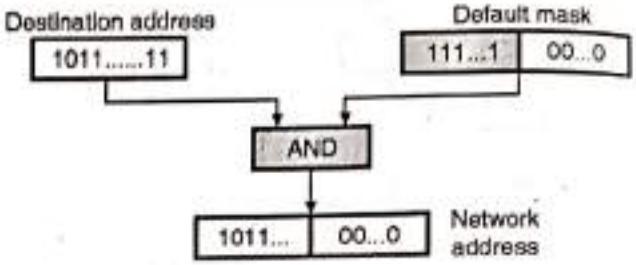
- Table 5.9.2 enlists the default masks of the three classes of IPv4 addresses.

Table 5.9.2 : Default masks

Address class	Default mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

5.9.9 Finding Network Address using Default Mask :

- The router uses the AND operation for extracting the network address from the destination address of the received packet.
- The router ANDs the destination address with the default mask to extract the network address as shown in Fig. 5.9.9.
- It is possible to use the default mask to find the number of addresses and the last address in the block.



(G-2010) **Fig. 5.9.9 : Finding a network address using the default mask**

5.9.10 Three Level Addressing : Subnetting :

MU : Dec. 06, May 07, May 08, Dec. 08, May 16

New Syll. : Dec. 18

University Questions

Q. 1 Explain subnetting and masking with suitable examples. **(Dec. 06, 10 Marks)**

Q. 2 Explain subnetting. **(May 07, 10 Marks)**

Q. 3 Explain subnetting and supernetting. **(May 08, Dec. 08, 10 Marks)**

Q. 4 Explain in short subnetting. **(May 16, 4 Marks)**

- As discussed earlier, the originally designed IP addresses were with two level addressing with **net id** and **host id.**
- The two level addressing is based on the principle that in order to reach a host on the Internet, we have to reach the network first and then the host.
- But very soon it became evident that the two level addressing would not be sufficient for the following two reasons :
  1. First it was needed to divide a large network of an organization (to which a block in class A or B is allotted) into many smaller **subnets** (subnetworks) for improved management and security.
  2. Second reason is more important. The blocks in class A and B were almost depleted and the blocks in class C were smaller than the needs of most organization. Therefore the organizations had to divide their allotted class A or B block into smaller subnetworks and share them.

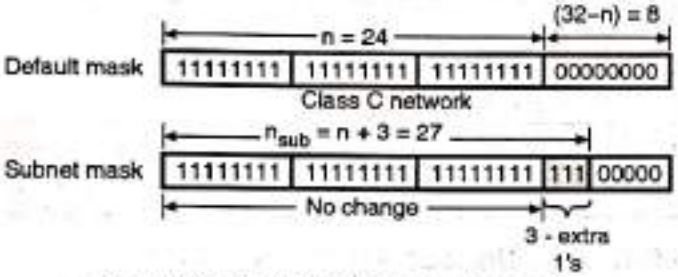
Definition of subnetting :

- We can define the **subnetting** as the principle of splitting a block of addresses into smaller blocks of addresses.
- In the process of **subnetting** we divide a big network into smaller subnetworks or **subnets.**
- Each such subnet has its own **subnet address.**

Scanned by CamScanner

Subnet mask :

- The **network mask** or **default** mask that we discussed earlier is used when the given network is **not** to be divided into smaller subnetworks i.e. when **subnetting is not** to be done.
- But when the given network is to be divided into smaller subnets i.e. when subnetting is to be done, we need to create a **subnet mask** for each subnet.
- Fig. 5.9.10 shows the format of a subnet mask. Each subnet has its own **net id** and **host id.**
- If we want to divide a network into 8 subnets then the corresponding subnet mask will have three extra 1's because $2^3 = 8$, as compared to the default mask, as shown in Fig. 5.9.10.
- In Fig. 5.9.10, we have shown the default mask and subnet mask when a class C network is to be divided into 8 subnets.



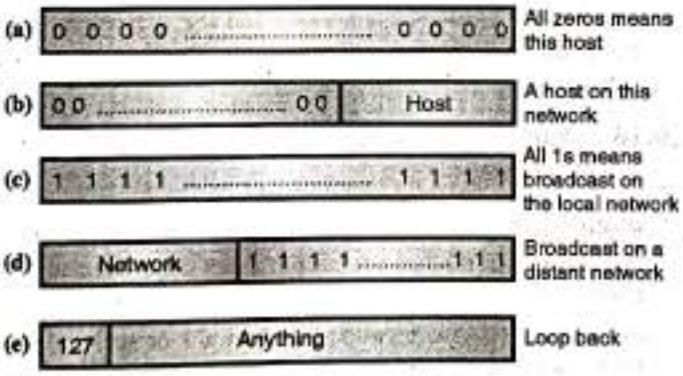
(G-2011) **Fig. 5.9.10 : Default and subnet masks**

5.9.11 Special IP Addresses : MU : May 09

University Questions

Q. 1 Discuss various special IP addresses. **(May 09, 10 Marks)**

- Fig. 5.9.11 shows some special IP addresses.



(G-540) **Fig. 5.9.11 : Special IP addresses**

- All zeros means this host or this network and all 1s means broadcast address to all hosts on the indicated network.
- The IP address 0.0.0.0 is used by the hosts when they are being booted but not used afterward.
- The IP addresses with 0 as the network number refer to their own network without knowing its number as shown in Fig. 5.9.11(b).
- The address having all ones is used for broadcasting on the local network such as a LAN as shown in Fig. 5.9.11(c).
- Refer Fig. 5.9.11(d). This is an address with proper network number and all 1s in the host field. This address allow machines to send broadcast packets to distant LANs anywhere in the Internet.
- If the address is "127. Anything" as shown in Fig. 5.9.11(e) then it is a reserved address **loopback testing.** This feature is also used for debugging network software.

5.9.12 Limitations of IPv4 :

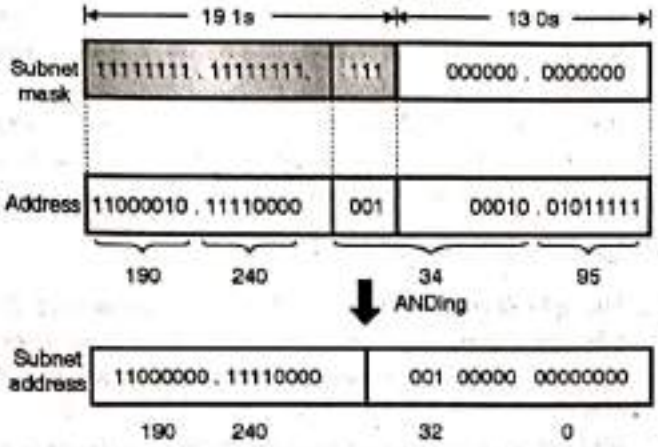
- The most obvious limitation of IPv4 is its address field. IP relies on network layer addresses to identify end-points on networks, and each networked device has a unique IP address.
- IPv4 uses a 32-bit addressing scheme, which gives it 4 billion possible addresses. With the proliferation of networked 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 use say a network has 300 hosts, this network needs either a single class B IP address or two class C IP addresses. If class B address is allocated to this network, as the number of hosts that can be defined in a class B network is (2 ∧ 16 – 2), a large number of host IP addresses are wasted.
- If two class C IP addresses are allocated, as the number of networks that can be defined using a class C address is only (2 ∧ 21), the number of available class C networks will quickly exhaust. Because of the above two reasons, a lot of IP addresses are wasted and also the available IP address space is rapidly reduced.
- Other identified limitations of the IPv4 protocol are: Complex host and router configuration, non-hierarchical addressing, difficulty in re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of Service), mobility and multi-homing, multicasting etc.
- To overcome these problems the internet protocol version 6 (IPv6) which is also known as internet protocol, next generation (IPng) was proposed.
- In IPv6 the internet protocol was extensively modified for accommodating the unforeseen growth of the internet.
- The format and length of the IP addresses has been changed and the packet format also is changed.

Ex. 5.9.4 : 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.

Scanned by CamScanner

Soln. :

- To find the subnet address, AND the destination address with the subnet mask as shown in Fig. P. 5.9.4.



(G-544) **Fig. P. 5.9.4**

Thus the subnet address is 190.240.32.0

5.9.13 Classless Addressing :

- Eventhough the number of actual devices connected to Internet is much less than 4 billion, the address depletion has taken place due to flaws in the classful addressing scheme.
- We have run out of class A and B addresses. To overcome these problems, the classless addressing is now being tried out.
- In the classless addressing, there are no classes but the address generation take place in blocks.

Address blocks :

- Address block is defined as the range of addresses.
- In the classless addressing, when an entity wants to get connected to the internet, a block (range) of addresses is granted to it.
- The size of this block i.e. number of addresses depends on the size of the entity as well as its nature.
- That means for a small entity such as a household only one or two addresses will be given whereas for a larger entity like an organization, thousands of addresses can be allotted.

Restrictions :

Some of the restriction on classless address blocks have been imposed by the internet authorities in order to simplify the process of address handling.

1. The addresses in a block should be continuous, i.e. serial in manner.
2. The total number of addresses in a block has to be equal to some power of 2 i.e. $2^1, 2^2, 2^3$ ...etc.
3. The first address should be evenly divisible by the number of addresses.

5.9.14 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.

5.9.15 Who Decides the IP Addresses ?

- No two IP addresses should be same. This is ensured by a central authority that issues the prefix or the network number portion of the IP address.
- Locally an ISP is to be contacted in order to get a unique IP address prefix.
- At the global level the Internet Assigned Number Authority (IANA) allots an IP address prefix to the ISP. Thus it is ensured that the IP addresses are not duplicated.
- Conceptually IANA is a wholesales and ISP is a retailer of the IP addresses because ISP purchases IP addresses from IANA and sells them to the customers.

5.9.16 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 5.9.3. These addresses are to be used for private networks and are called **unregistered addresses.**

Scanned by CamScanner

- We can choose any of these unregistered address while building our own private network.

Table 5.9.3 : IP addresses for private networks

Class	Network address
A	10.0.0.0 through 10.255.255.255
B	172.16.0.0 through 172.31.255.255
C	192.168.0.0 through 192.168.255.255

5.9.17 Solved Examples :

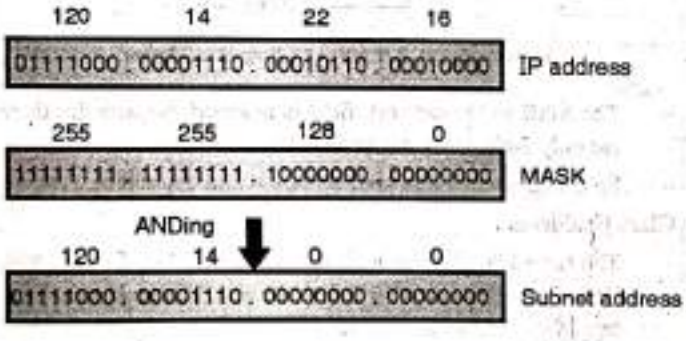
Ex. 5.9.5 : Find the sub-network address and the host id for the following :

Sr. No.	IP address	MASK
(a)	120.14.22.16	255.255.128.0
(b)	140.11.36.22	255.255.255.0
(c)	141.181.14.16	255.255.224.0
(d)	200.34.22.156	255.255.255.240

Soln. :

Step 1 : To find the subnet address :

In order to find the subnet address we have to AND the IP address and the mask as follows :



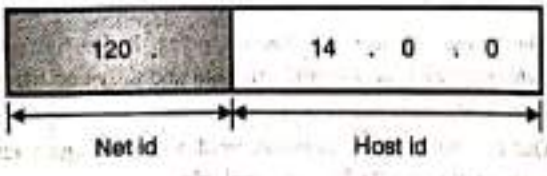
(G-553) **Fig. P. 5.9.5(a)**

So the subnet address is 120.14.0.0.

Similarly we can find the other subnet addresses.

Step 2 : Host id :

- Examine the first byte of the subnet address. It is 120 which is between 0 and 127. Hence this is a class A network.
- So only the first byte corresponds to the net id and the remaining three bytes correspond to the host id as shown in Fig. P. 5.9.5(b).



(G-554) **Fig. P. 5.9.5(b)**

So the host id is 14.0.0.

- Similarly we can find the other host id.

Ex. 5.9.6 : The IP address of a host on class C network is 198.123.46.237. Four networks are allowed for this network. What is subnet mask ?

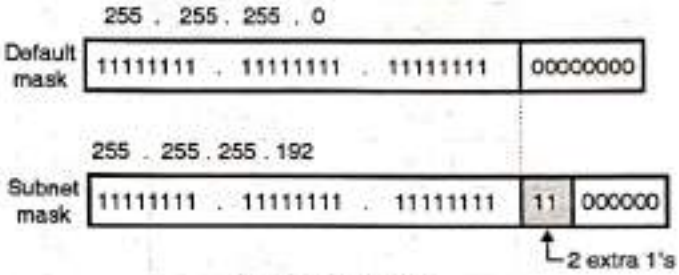
Soln. :

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. 5.9.6.



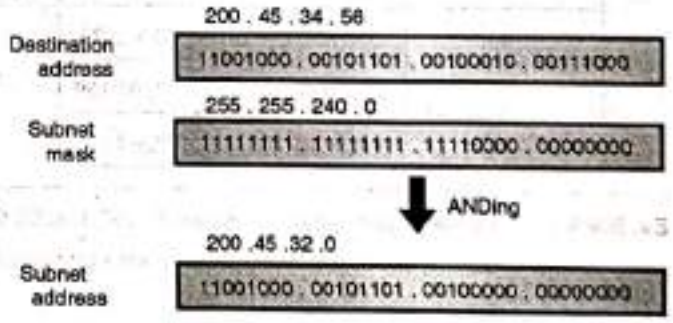
(G-555) **Fig. P. 5.9.6**

Thus the required subnet mask is 255.255.255.192.

Ex. 5.9.7 : 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. 5.9.7.



(G-556) **Fig. P. 5.9.7**

Thus the required subnet address is 200.45.32.0.

Ex. 5.9.8 : A company is granted a site address 201.70.64.0. The company needs six subnets. Design the subnets.

Soln. :

- This is a class C network. So the default mask is,

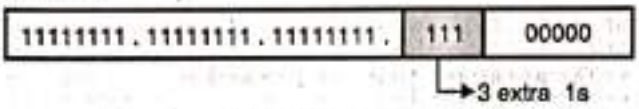
Scanned by CamScanner

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. 5.9.8.



(G-557) **Fig. P. 5.9.8**

- In order to have six subnets, we can have 6 different combinations of the 3-extra 1s as shown in Table P. 5.9.8(a).

Table P. 5.9.8(a)

Combination	Subnet number
0 0 0	Subnet 1
0 0 1	Subnet 2
0 1 0	Subnet 3
0 1 1	Subnet 4
1 0 0	Subnet 5
1 0 1	Subnet 6

- So the various addresses of 6 subnets are as shown in Table P. 5.9.8(b).

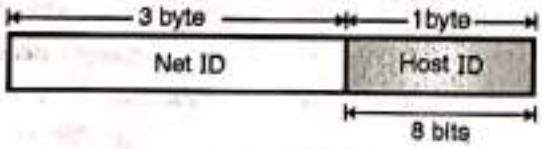
Table P. 5.9.8(b)

Subnet number	Addresses
1	201.70.64.0 to 201.70.64.31
2	201.70.64.32 to 201.70.64.63
3	201.70.64.64 to 201.70.64.95
4	201.70.64.96 to 201.70.64.127
5	201.70.64.128 to 201.70.64.159
6	201.70.64.160 to 201.70.64.191

Ex. 5.9.9 : For a given class C network 195.188.65.0 design equal subnets in such a way that each subnet has atleast 60 nodes.

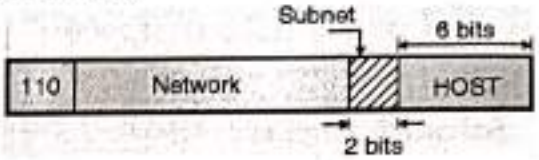
Soln. :

- Fig. P. 5.9.9(a) shows the structure of a class C address in which 3-bytes are reserved for net ID and 1-byte for host ID.



(G-558) **Fig. P. 5.9.9(a)**

- We are expected to design equal subnets such that each subnet has atleast 60 nodes (i.e. 60 users).
- In order to identify at least 60 users we need 6-bits in the host ID.
- The remaining 2-bits are assigned for subnetting as shown in Fig. P. 5.9.9(b).



(G-559) **Fig. P. 5.9.9(b)**

- This shows that there will be four equal subnets each one having at least 60 nodes.

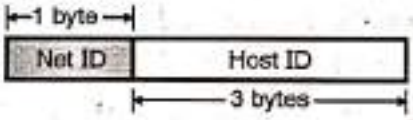
Ex. 5.9.10 : Show by calculations how many network each IP address class can have with one example ?

Soln. :

Number of networks in different IP address :

Class A address :

- The format of class A address is shown in Fig. P. 5.9.10(a). Here one byte defines the network ID and three bytes define the host ID.

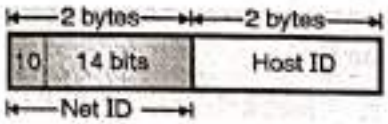


(G-560) **Fig. P. 5.9.10(a) : Class A address**

- 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. 5.9.10(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. 5.9.10(b) : Class B address**

- So the number of networks in class B address is $2^{14} = 16,368$.

Class C address :

- The format of class C is shown in Fig. P. 5.9.10(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.

Scanned by CamScanner

(G-562) **Fig. P. 5.9.10(c) : Class C address**

- So the number of networks in class C addresses is 2, 097, 152.

Ex. 5.9.11 : How many host per network in each IP address class can exist, show with example ?

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, 7772, 16.

Class B :

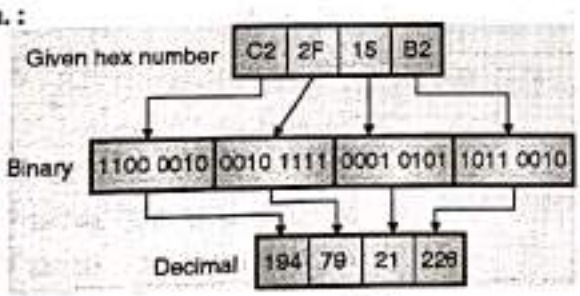
There are 2-bytes (16-bits) in the host field. So the number of hosts in class B address will be 65536 i.e. 2^{16} per network.

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. 5.9.12 : Convert the IP address whose hexadecimal representation is C22F15B2 to dotted decimal notation.

Soln. :



(G-563) **Fig. P. 5.9.12**

∴ The IP address in the dotted decimal notation is as follows :

194.79.21.226

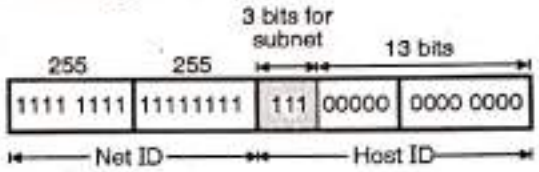
Ex. 5.9.13 : Perform the subnetting of the following IP address 160.111. X.X

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. 5.9.13.



(G-566) **Fig. P. 5.9.13**

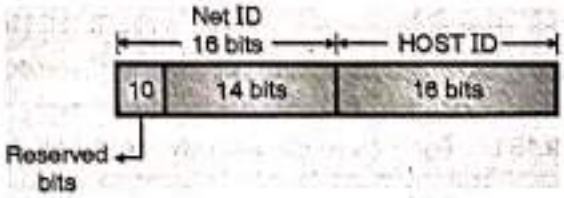
- The 3-bits reserved for subnetting will have 8 combinations from 000 to 111 out of which any six combinations can be used for 6 subnets.
- Let us decide that the combinations 000 to 001 are not to be used. Then the subnet masks for the 6 possible subnets will have the following addresses.

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. 5.9.14 : 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.

Soln. :

- Fig. P. 5.9.14(a) shows the original class B address format :



(G-567) **Fig. P. 5.9.14(a) : Original class B address format**

Scanned by CamScanner

- 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. 5.9.14(b).

∴ Number of class B networks = 2^{18} = 2, 61, 888

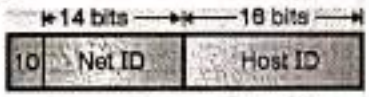
(G-568) **Fig. P. 5.9.14(b) : Modified class B address format**

The range of IP addresses in the decimal dotted form would be 128.0.0.0 to 191.255.255.255.

Ex. 5.9.15 : A network on the Internet has a subnet mask of 255.255.240.0. What is the maximum number of host it can handle ? Give the range of IP addresses in decimal dotted form.

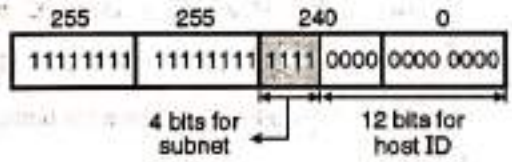
Soln. :

The structure of class B address is as shown in Fig. P. 5.9.15(a).



(G-564) **Fig. P. 5.9.15(a) : Class B address**

The given subnet mask is 255.255.240.0. So it is as shown in Fig. P. 5.9.15(b).



(G-565) **Fig. P. 5.9.15(b) : Subnet mask**

Thus there are 4 extra 1s as shown in Fig. P. 5.9.15(b). So there will be 16 subnets and each subnet can have 2^{12} = 4096 hosts.

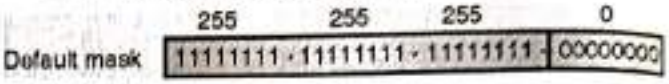
Ex. 5.9.16 : For a given class-C network, design 4 equal subnets having minimum 50 nodes in each subnetwork.

Soln. :

The default mask for a class C network is

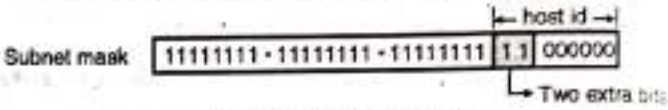
255.255.255.0

This is as shown in Fig. P. 5.9.16(a).



(G-571) **Fig. P. 5.9.16(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. 5.9.16(b).



(G-572) **Fig. P. 5.9.16(b)**

In order to have four subnets, we can have four different combinations of the two extra bits as shown in Table P. 5.9.16(a).

Table P. 5.9.16(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. 5.9.16(b).

Table P. 5.9.16(b)

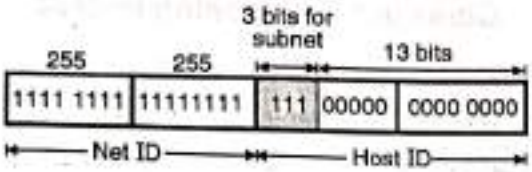
Subnet number	Addresses
1	201.70.64.0 to 201.70.64.63
2	201.70.64.64 to 201.70.64.127
3	201.70.64.128 to 201.70.64.191
4	201.70.64.192 to 201.70.64.255

Ex. 5.9.17 : 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. 5.9.17.

Scanned by CamScanner



(G-566) **Fig. P. 5.9.17**

- The 3-bits reserved for subnetting will have 8 combinations from 000 to 111 which can be used for 8 subnets.
- The subnet masks for the 8 possible subnets will have the following subnet masks :

Subnet	Mask
1	255.255.0.0
2	255.255.32.0
3	255.255.64.0
4	255.255.96.0
5	255.255.128.0
6	255.255.160.0
7	255.255.192.0
8	255.255.224.0

Number of hosts in each subnet :

Due to use of extra 3-bits for subnetting, now we have only 13-bits left in the host id field.

$\therefore$ No. of hosts in each subnet $= 2^{13} = 8192$ ...Ans.

Ex. 5.9.18 : A network on the internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts it can handle ? **Dec. 04, 2 Marks**

Soln. :

The maximum number of hosts a network handle can be almost 254 (28-2) host.

Ex. 5.9.19 : A class A network on the internet has a subnet mask of 255.255.224.0. What is the maximum number of hosts per subnet ? **May 05, 4 Marks**

Soln. :

A subnet mask of 255.255.224.0 corresponds to the following pattern.

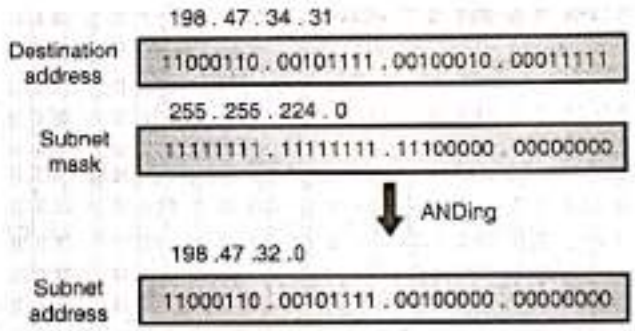
255	255	244	0
11111111	11111111	111 00000	00000000

Due to 3 additional 1s (shaded portion) there will be $2^3 = 8$ subnets and the number of hosts per subnet will be $2^{13} = 8192$.

Ex. 5.9.20 : What is subnet address if the destination address is 198.47.34.31 and subnet mask is 255.255.224.0 **Dec. 09, 5 Marks**

Soln. :

To find subnet address we have to AND the IP address and the subnet mark as shown Fig. P. 5.9.20.



(G-804) **Fig. P. 5.9.20**

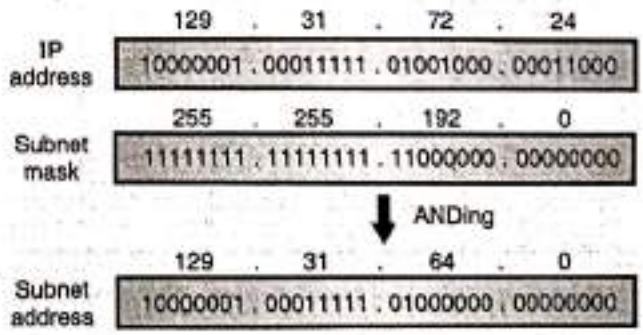
Thus the required subnet address is 198.47.32.0

Ex. 5.9.21 : What is subnetting ? What are the default subnet masks ? Find the subnet address if the IP address is 129.31.72.24 and subnet mask is 255.255.192.0. **Dec. 15, 5 Marks**

Soln. :

Please refer section 5.9.10 for subnetting.

To find the subnet address we have to AND the IP address and the subnet mask as shown in Fig. P. 5.9.21.



(G-1868) **Fig. P. 5.9.21**

Thus the required subnet address is 129.31.64.0.

Scanned by CamScanner

Ex. 5.9.22 : What is subnetting ? Given the class C network 192.168.10.0 use the subnet mask 255.255.255.192 to create subnets and answer the following :

1. What is the number of subnets created ?
2. How many hosts per subnet ?
3. Calculate the IP address of the first host, the last host and the broadcast address of each subnet.

May 17, 10 Marks

Soln. :

For subnetting refer section 5.9.10.

Given : IP address : 192.168.10.0 (class C)

Subnet mask : 255.255.255.192

Step 1 : Number of subnets and number of hosts :

255.255.255.192 ...(Given)

11111111 - 11111111 - 11111111 - 11000000

The number of subnets are determined by the number of extra 1's.

∴ Number of extra 1's = 2

∴ Number of subnets = $2^2 = 4$ **...Ans.**

The value of n is 26 which means the number of hosts per subnet is,

$$2^{32-26} = 2^6 = 64 \quad \text{...Ans.}$$

Step 2 : IP address of the first host, last host and broadcast address :

The following is the range of subnets :

Subnet	Subnet range
1	192.168.10.0 to 192.168.10.63
2.	192.168.10.64 to 192.168.10.127
3.	192.168.10.128 to 192.168.10.191
4.	192.168.10.192 to 192.168.10.255

IP address of first host : 193.129.65.1

IP address of last host : 254.190.126.62

Broadcast address : 255.191.127.63

5.10 Classless Addressing in IPv4 :

- Eventhough the number of actual devices connected to Internet is much less than 4 billion, the address depletion has taken place due to flaws in the classful addressing scheme.
- We have run out of class A and B addresses. To overcome these problems, the super netting and subnetting has been tried as discussed earlier.
- But subnetting and supernetting also could not solve the problem of address depletion in IPv4.
- Due to increased number of Internet users, it was evident that a larger address space would be required as a long term solution to this problem. For this the length of the IP address should be increased which means the IP packet itself must be changed.
- A long term solution is to switch to IPv6. But a short term solution which uses the same address space has been deviced for IPv4. It is known as **classless addressing.**
- In the classless addressing, there are no classes but the address generation take place in blocks.
- The classless addressing was announced by the Internet authorities in 1996 in which blocks of variable length which do not belong to any class are used.

5.10.1 Variable Length Blocks :

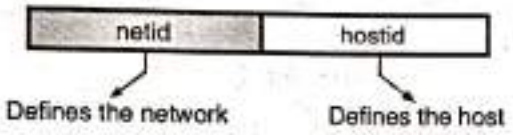
- Address block is defined as the range of addresses.
- In the classless addressing, when an entity wants to get connected to the internet, a block (range) of addresses is granted to it.
- The size of this block i.e. number of addresses depends on the size of the entity as well as its nature.
- That means for a small entity such as a household only one or two addresses will be given whereas for a larger entity like an organization, thousands of addresses can be allotted.
- Fig. 5.10.1 shows how the address space is divided into non overlapping address blocks.

Scanned by CamScanner

(G-1804) **Fig. 5.10.1 : Variable length blocks in classless addressing**

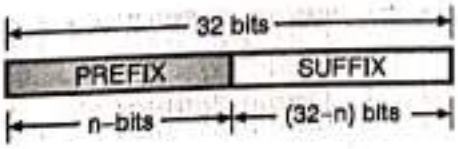
Two level addressing :

- We have discussed the two level addressing for classfull addressing which divided an address into two parts namely : net id and host id.



(G-1805) **Fig. 5.10.2 : Two layer addressing in classfull addressing**

- The **net id** and **host id** define the network and host respectively. It is possible to use the same idea in the classless addressing as well.
- A block of addresses granted to an organization is divided into two parts called as the **prefix** and the **suffix.**
- The role of prefix is same as that of the net id whereas as the role of suffix is same as that of the host id. Thus in a block granted to an organization, all the addresses will have the **same prefix** but each address will have a different **suffix.**
- Thus the prefix defines the network (organization to which the address block has been granted) while the suffix defines individual hosts on the network.
- The concept of two level addressing in classless addressing using the prefix and suffix is as shown in Fig. 5.10.1.
- The IPv4 address is 32 bit long out of which the prefix will be of length "n" which can take any value from 0 to 32 and the length of the suffix will be (32 – n) bits.
- Note that the value of "n" i.e. length of the prefix depends on the length of the address block allotted (granted) to an organization.



(G-1806) **Fig. 5.10.3 : Two level addressing using prefix and suffix for classless addressing**

Ex. 5.10.1 : Find out the values of prefix and suffix lengths in classless addressing if all the available addresses in IPv4 is to be considered as one single block.

Soln. :

- The total addresses in IPv4 is 2^{32} = 4,294,967,296.
- We have to consider this as one block hence the prefix length n = 0. Whereas all the hosts will have their individual addresses. So all the 32 bits will be allotted to the suffix length.

Ex. 5.10.2 : For the same data of the previous example find out the values of prefix and suffix lengths if all the available IPv4 addresses are divided into 4,294,967,296 blocks with each block having only one host.

Soln. :

- Here the prefix length for each block is n = 32, and the suffix length would be (32-n) = 0. The address of the single host in each block will be same as its block address itself.

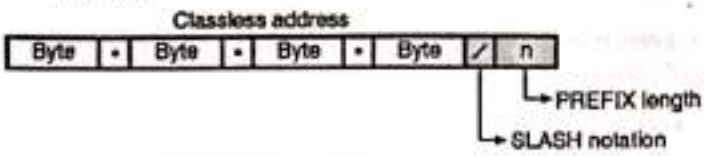
Note : The two previous examples show that the prefix number n and the number of addresses in a block are inversely proportional to each other. With increase in the value of n, the number of addresses in a block will decrease.

5.10.2 The Slash Notation (CIDR Notation) :

- If an address (classful or classless) is given to us and we want to extract information from it, then the net id in classful addressing or the prefix in classless addressing are extremely important and useful to us.
- However it is not easy to identify the prefix bits in a given classless address. It is easy to identify the net id from the given classful address.
- For a given classless address it is not possible to find the prefix length because the given address can belong to a block with any prefix length.
- Therefore, in classless addressing it is essential to include the prefix length to each address if the block of the given address is to be found.
- Hence the prefix length "n" is added to the classless address separated by a **slash** and the notation is known as the **slash notation.**

Scanned by CamScanner

- Fig. 5.10.4 demonstrates a classless address with slash notation.



(G-1807) **Fig. 5.10.4 : Slash notation**

- The slash notation is also called as Classless Interdomain Routing or CIDR notation.

5.10.3 Network Mask :

- We have discussed the concept of network mask in the classful addressing. The same concept is also applicable in the classless addressing as well.
- A network mask in classless addressing is a 32 bit number. With its "n" left most bits (corresponding to the prefix) all set to 1s and the remaining (32-n) bits corresponding to the suffix all set to 0s.

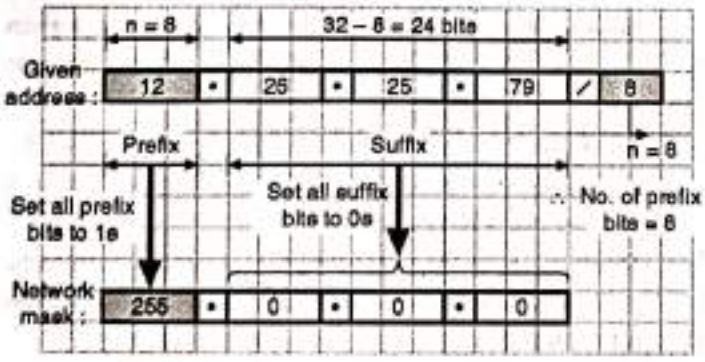
Ex. 5.10.3 : For the following addresses identify the number of prefix bits and write down the network mask :

1. 12.26.25.79 / 8
2. 130.12.230.156 / 16

Soln. :

1. Classless CIDR address : 12.26.25.79 / 8

- As per the slash notation we have n = 8 i.e. number of prefix bits is 8.
- Therefore the number of suffix bits = 32 – 8 = 24.
- In order to obtain the network mask the prefix bits all set to 1s and the suffix bits all set to zero as shown in Fig. P. 5.10.3(a).

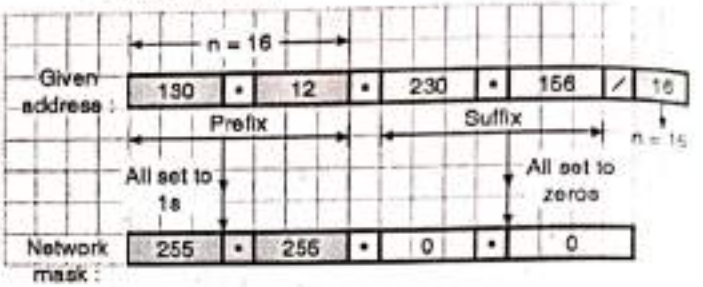


(G-1808) **Fig. P. 5.10.3(a)**

- Thus the network mask = 255.0.0.0

2. Classless CIDR Address : 130.12.230.156 / 16

- As per the slash notation, n = 16 i.e. number of prefix bits is 16.
- Number of suffix bits = 32 – 16 = 16
- In order to obtain the network mask, set all the prefix bits to 1s and set all the suffix bits to 0s as shown in Fig. P. 5.10.3(b).



(G-1809) **Fig. P. 5.10.3(b)**

- Thus the network mask = 255.255.0.0

5.10.4 Extracting the Block Information :

MU : May 16

University Questions

Q. 1 Explain Classless Inter Domain Routing (CIDR). **(May 16, 10 Marks)**

- We can extract all the required information from the given classless address in the CIDR notation. The information that we can obtain is as follows :
  1. The first address (network address)
  2. The number of addresses.
  3. The last address.
- We can obtain the number of addresses in a block as follows :

$$\text{Number of addresses in a block } N = 2^{(32-n)} \quad \text{...(5.10.1)}$$

Where n = Number of prefix bits.

- The first address or network address in block can be obtained by ANDing the address with the network mask.

$$\text{First address} = (\text{Any address}) \text{ AND } (\text{Network mask}) \quad \text{...(5.10.2)}$$

- OR what we can do is keep the "n" leftmost bits of any address as it is and set the remaining (32-n) bits to 0s. This is equivalent to the ANDing operation mentioned above.
- In order to obtain the last address in the block we have to add the first address with the number of addresses in the block directly.

$$\therefore \text{Last address} = \text{First address} + \text{Number of addresses in the block} \quad \text{...(5.10.3)}$$

- It is also possible to obtain the last address by ORing the address with complement of the network mask.

Scanned by CamScanner

∴ Last address = (Any address) OR [NOT (Network Mask)]

...(5.10.4)

- One more way of obtaining the last address of the block is to keep all the "n" left most bits (prefix bits) as it is and set all the (32-n) bits (suffix bits) to 1s.

Ex. 5.10.4 : If an address in a block is given in CIDR classless notation as 64.32.16.8 / 27 then find the following :

1. Number of addresses in the block (N)
2. The first address and
3. The last address.

Soln. :

Step 1 : Find n :

Given address = 64.32.16.8 / 27

Hence n = 27 from the slash notation.

∴ n = 27 bits.

∴ Prefix bits = 27, suffix bits = 32 – 27 = 5

Step 2 : Number of addresses in the block (N) :

$$N = 2^{(32-n)} = 2^5 = 32$$

Step 3 : Find the first address :

- Refer Fig. P. 5.10.4(a) to obtain the first address in the block. For this we have to AND the given address with the network mask.

	n	(32 – n)
Network mask =	27 ones	5 zeros

∴ Network mask = 255.255.255.224

- For ANDing write the given address and network mask in their binary notations as shown in Fig. P. 5.10.4(a).

∴ From Fig. P. 5.10.4(a) we get the first address in the block as :

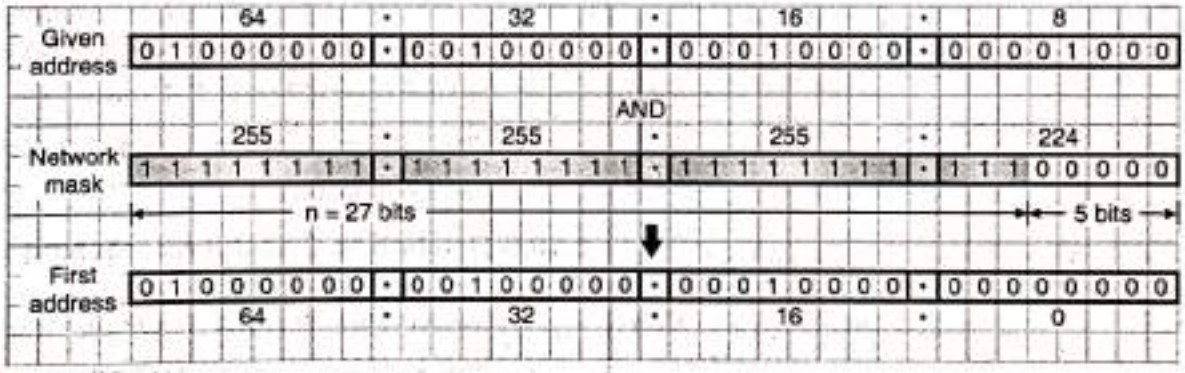
First address = 64.32.16.0 ...Ans.

Step 4 : Find the last address :

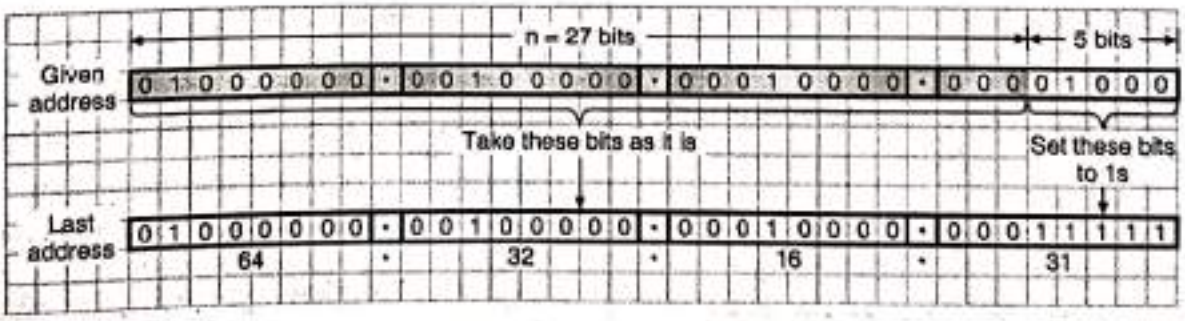
To obtain the last address in the block, we have to keep the left most 27 bits in the given address as it is and set the remaining 5 bits to 1s as shown in Fig. P. 5.10.4(b).

∴ From Fig. P. 5.10.4(b) we get the last address in the block as follows :

Last address = 64.32.16.31



(G-1810) **Fig. P. 5.10.4(a) : First address in the block**



(G-1811) **Fig. P. 5.10.4(b) : Last address**

Scanned by CamScanner

Ex. 5.10.5 : For the classless address 129.65.33.01 / 24 find the following :

1. Number of addresses in the block (N)
2. The first address.
3. The last address.

Soln. :

Step 1 : Find n :

Given address = 129.65.33.01 / 24 hence n = 24 from the slash notation.

$\therefore$ n = 24 bits

$\therefore$ Prefix bits = 24, suffix bits = 32 – 24 = 8

Step 2 : Number of addresses in the block (N) :

$$N = 2^{(32-n)} = 2^8 = 256 \quad \text{...Ans.}$$

Step 3 : Find the first address :

- Refer Fig. P. 5.10.5(a) to obtain the first address in the block. For this we have to AND the given address with the network mask.

	n	(32 – n)
Network mask =	24 ones	8 zeros

$\therefore$ Network mask = 255.255.255.0

- For ANDing write the given address and network mask in their dotted decimal notations as shown.

Address :		1	2	9	•	6	5		•		3	3	•		0	1
Network mask :	AND	2	5	5	•	2	5	5	•	2	5	5	•		0	
First address (AND) :		1	2	9	•	6	5		•		3	3	•		0	

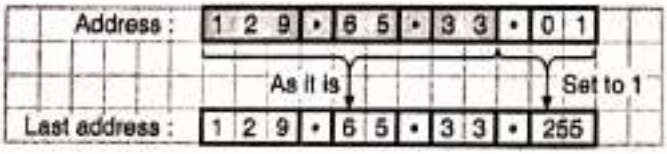
(G-1812) **Fig. P. 5.10.5(a) : First address in the block**

$\therefore$ From Fig. P. 5.10.5(a) we get the first address in the block as :

First address = 129.65.33.0 ...Ans.

Step 4 : Find the last address :

To obtain the last address in the block, we have to keep the left most 24 bits in the given address as it is and set the remaining 8 bits to 1s as shown in Fig. P. 5.10.5(b).



(G-1813) **Fig. P. 5.10.5(b) : Last address in the block**

- From Fig. P. 5.10.5(b) we get, the last address in the block is as follows :

Last address = 129.65.33.255 ...Ans.

5.10.5 Block Allocation :

- Now let us understand how to allocate the blocks in the classless addressing. The global authority for the block allocation is ICANA means Internet Corporation for Assigned Names and Addresses.
- But the individual addresses of the Internet users is not allotted by the ICANA. Instead ICANA will assign large blocks of addresses to various ISPs or large organizations. These ISPs or organization will assign addresses to the individual Internet users from their allotted blocks.

Restrictions :

Some of the restriction on classless address blocks have been imposed by the internet authorities in order to simplify the process of address handling.

1. The addresses in a block should be continuous, i.e. serial in manner.
2. The total number of addresses in a block has to be equal to some power of 2 i.e. $2^1, 2^2, 2^3$ ...etc.
3. The first address should be evenly divisible by the number of addresses.

5.10.6 Relation to Classful Addressing :

- The classful addressing may be imagined as the special case of classless addressing such that the blocks of addresses in class A, B and C type addresses will have the prefix lengths $n_A = 8$, $n_B = 16$ and $n_C = 24$.
- Table 5.10.1 lists the prefix lengths for class A to F classful addresses and using this information we can change a block in classful addressing to a block in classless addressing.

Table 5.10.1 : Prefix lengths for classful addressing

Class	Prefix length	Class	Prefix length
A	/ 8	D	/ 4
B	/ 16	E	/ 4
C	/ 24		

Scanned by CamScanner

5.10.7 Subnetting :

- The concept of subnetting in classless addressing domain is similar to that discussed for the classful addressing.
- The subnetting is used for creating a three level hierarchy in the classless addressing domain.
- An organization or an ISP have a block of addresses granted to them. It can divide these addresses into several subgroups and each subgroup of addresses is assigned to a **subnetwork or subnet.**
- The subnetworks may be subdivided further if the organization want it that way.

5.10.8 Designing Subnets :

Let N = Total number of addresses granted to an organization.

n = Prefix length

N_{sub} = Assigned number of addresses to each subnetwork

N_{sub} = Prefix length for each subnetwork

S = Total number of subnetworks.

- Now follow the steps given below to ensure that the subnetworks operate properly.

Steps to follow :

- The number of addresses in each subnetwork should always be equal to a power of 2. i.e. $2^0, 2^1, 2^2$....etc.
- We can use the following expression to find the prefix length of each sunetwork.

$$n_{sub} = n + \log_2 \left[\frac{N}{N_{sub}}\right] \quad ...(5.10.5)$$

- The starting address in each subnet should be divisible by the number of addresses in that subnework. To achieve this we need to first assign address to larger networks.

Note : These restrictions are similar to those applied when addresses to network were allocated.

5.10.9 Finding Information about Each Network :

- After designing the subnetworks, we can find the information about the subnets such as starting and last addresses, we can use the same procedure that was used to find the information about each network in the Internet.

Ex. 5.10.6 : A block of addresses granted to an ISP is given by 130.34.13.64 / 26. These addresses are to be divided into four subnetworks with equal number of hosts. Design the subnetworks and obtain all the information about each subnet.

Soln. :

Step 1 : Find total number of addresses (N) :

- From the given address we get n = 26 (prefix length).
- Hence the number of addresses in the whole network will be :

$$N = 2^{(32-n)} = 2^{(32-26)} = 2^6 = 64$$

- The first address in this block will be 130.34.13.64 / 26 whereas the last address will be 130.34.13.127 / 26. These values have been obtained using the procedure that we have discussed earlier.

Subnet design :

Step 2 : Find number of hosts per subnetwork :

- There are four subnetworks with equal number of guests.

∴ Number of hosts per subnetwork is given by,

$$N_1 = N_2 = N_3 = N_4 = \frac{N}{4} = \frac{64}{4} = 16 \quad ...\textbf{Ans.}$$

- 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,

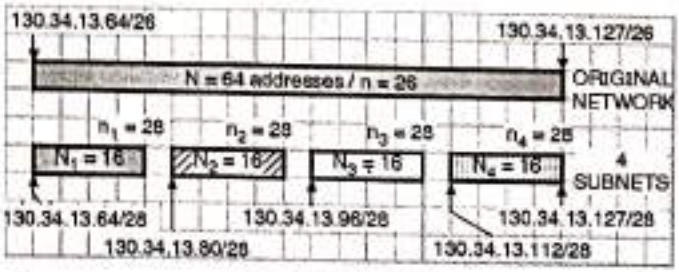
$$n_1 = n_2 = n_3 = n_4 = n + \log_2 \left[\frac{N}{N_{sub}}\right]$$

$$= 26 + \log_2 \left[\frac{64}{16}\right] = 26 + \log_2 4$$

$$\therefore n_1 = n_2 = n_3 = n_4 = 28 \quad ...\textbf{Ans.}$$

Step 4 : Starting and ending addresses of all the subnets :

- Refer Fig. P. 5.10.6 which shows all the starting and ending addresses of the 4-subnets.
- It should be noted from Fig. P. 5.10.6 that all the starting addresses should be divisible by the number of addresses in the subnet i.e. by 16.



(G-1814) **Fig. P. 5.10.6**

Scanned by CamScanner

5.10.10 Address Aggregation :

Address aggregation is considered to be one of the advantages of CIDR architecture. As we know, ICANN assigns a large block of addresses to an ISP which is divided into smaller subnets and assigned to the customers by the ISPs. Thus many blocks of addresses are aggregated in one block and assigned to one ISP.

Ex. 5.10.7 : A router has following CIDR entries in its routing table :

Address/Mask	Next Hop
135.46.56.0/22	Interface 0
135.46.60.0/22	Interface 1
192.53.40.0/23	Router 1
Default	Router 2

For each of the following IP addresses, what does the router do if a packet with that address arrives ?

1. 135.46.63.10 2. 192.53.56.7

MU : Dec. 10, 10 Marks

SPPU : Dec. 11, 8 Marks, May 16, 5 Marks

Soln. :

CIDR – Classless Inter Domain Routing :

- IP is being heavily used for decades. However, due to the exponential growth of internet, IP is running out of addresses.
- This is a potential disaster and the internet community has begun discussion over it. In this section we are going to discuss one of the solutions to this problem.
- One of the solutions is CIDR (Classless Inter Domain Routing). The CIDR is based on the principle of allocating the remaining IP addresses in variable-sized blocks regardless of the class.
- If a site needs say 2000 addresses, then a block of 2048 addresses on the 2048 byte boundary is given to it.
- However the classless routing makes forwarding of packets more complicated.

Forwarding algorithm in the old classful system :

- The steps followed in the old classful system for forwarding packets is as follows :
  1. As soon as a packet arrives at a router, a copy of the IP address was shifted right by 28 bits to obtain a 4 bit class number.
  2. A 16-way branch then sorts packets into class A, B, C and D (if supported) with eight of the cases for class A, four of the cases for class B, two of the cases for class C and one each for D and E.
  3. The code for each class then masked off the 8–, 16–, or 24– bit network number and right aligned it in a 32 bit word.
  4. The network number was then searched in the A, B or C table.
  5. As soon as the entry was found, the outgoing line was decided and the packet was forwarded upon it.

Forwarding with CIDR :

- The simple forwarding algorithm explain earlier does not work with CIDR.
- Instead now each router table entry is extended by giving it a 32 bit mask. So now there is a single routing table for all networks (no different tables for class A, B, C, etc.) which consists of an array of triples. Each triple consists of an IP **address, subnet mask and outgoing line.**
- When a packet arrives at the input, the router first extracts its destination IP address. Then the routing table is scanned entry by entry to look for a match.
- It is possible that different entries with different subnet mask lengths match. In such a case the longest mask is used. For example if there is a match for a/20 mask and a/24 mask then /24 entry is used.

Solution of problem :

- Convert the IP address to bits and then AND it with the subnet mask of the interface whose address is closest to that of the IP addresses.
- The result of the ANDing will give you the network address and the interface to send the packet to.

1. IP = 135.46.63.10 :

The interface whose address is closest to this IP is interface 1. This interface uses a 22 bit mask. So AND the given IP address with a 22 bit mask as follows :

```
IP =  135.46.63.10 = 10000111.00101110.00111111.00001010
22 bit mask = 255.255.252.0 = 11111111.11111111.11111100.00000000
                              ----------------------------------
IP AND Mask = 10000111.00101110.00111100.00000000
∴ IP AND Mask = 135.46.60.0
```

(G-1973)

This result of ANDing matches with the network address of interface 1. Hence the router will forward this packet to interface 1.

2. IP = 192.53.56.7 :

The interface whose address is closest to this IP is interface 2. This interface uses a 23 bit mask. So AND the packet IP address with a 23 bit mask as follows :

```
IP =  192.53.56.7  = 11000000.00110101.00111000.00000111
23 bit mask = 255.255.254.0 = 11111111.11111111.11111110.00000000
                              ----------------------------------
IP AND Mask = 11000000.00110101.00111000.00000000
            = 192.53.56.0
```

(G-1974)

Scanned by CamScanner

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.

5.11 Special Addresses :

In the classful addressing, some addresses were reserved for special purpose. Similarly in the classless addressing as well some addresses are reserved.

5.11.1 Special Blocks :

Some address blocks have been reserved for special purpose.

5.11.2 All Zeros Address :

- The block 0.0.0.0 / 32 contains only one address. It is called as the all zero address and has a prefix length of n = 32.
- This address has been reserved for communication when a host has to send an IPv4 packet but it does not know its own address.
- In such situations, the host sends an IPv4 packet to a DHCP server using this all zero address as the source address and a limited broadcast address (all one address) as the destination address, so as to find its own address.

5.11.3 All one Address-Limited Broadcast Address :

- The block 255.255.255.255 / 32 contains only one address. It is called as an all one address and has a prefix length of n = 32.
- This all one address has been reserved for limited broadcast address i.e. if a host wants to send message to all the hosts simultaneously then the sending host can use all one address as a destination address inside the IPv4 packet.
- Such a broadcasting is confined to the network only because routers do not allow the all one packet to pass through them.
- The datagram sent with the all zero address as destination will be received and processed by all the hosts on the network.

5.11.4 Loopback Address :

- A loopback address is the address which is used to test the software on a machine. The block 127.0.0.0 / 8 with a prefix length of 8 is used for the loopback address.
- On using this address, a packet does not leave the machine at all but it returns to the protocol software. It can be used for testing the IPv4 software.

5.11.5 Private Addresses :

- The address blocks that are not recognized globally still assigned for private use are known as private addresses.
- These addresses are neither connected to nor isolated from the Network Address Translation (NAT) techniques.
- Table 5.11.1 depict such address blocks.

Table 5.11.1 : Private addresses

Block	Number of addresses	Block	Number of addresses
10.0.0.0 / 8	16,777,216	192.168.0.0 / 16	65,536
172.16.0.0 / 12	1,047,584	169.254.0.0 / 16	65,536

5.11.6 Multicast Addresses :

The block 224.0.0.0 / 4 with a prefix length of n = 4 has been reserved for the multicast IP communication.

5.11.7 Special Addresses in Each Block :

- The usage of some address in each block for special addresses has been recommended. But it has not been made mandatory. These addresses are not assigned to any host.
- One important point to be remembered is that a very small block of addresses should not be used as special addresses.

5.11.8 Network Address :

- The network address is defined as the first address (with the suffix set all to 0s) in a block. It is used for defining the network itself. It does not define any host in the network.
- With the same principle, the first address in a subnetwork is called as the subnetwork address.

5.11.9 Direct Broadcast Address :

- We can use the last address in a block or subblock (with the suffix part set to all 1s), as a **direct broadcast address** for that block or subblock.
- A router generally uses this address for sending a packet to all the hosts connected to a specific network. This address is used as the destination address in the IPv4 packet and all the hosts will accept and process the datagram which has this destination address.

5.12 NAT – Network Address Translation :

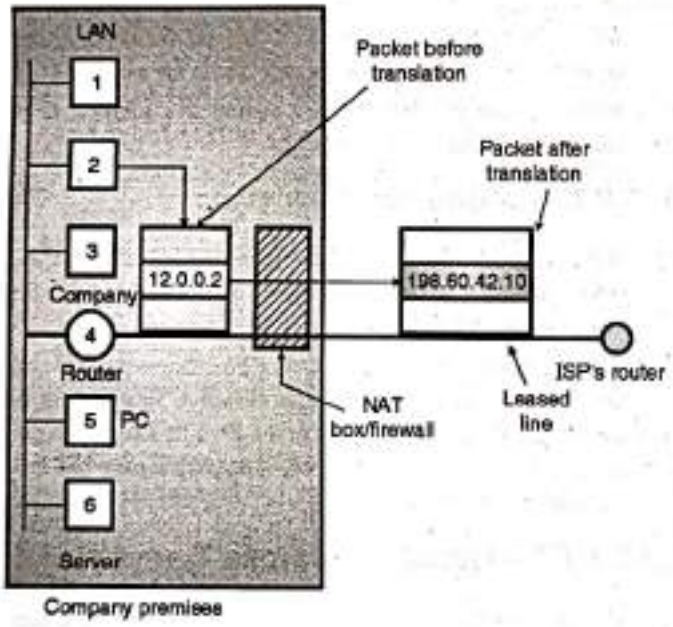
- The problem that existing number of IP addresses is less than the actually required ones is practically important.
- A long term solution to this problem is that the whole Internet should be migrated from IPv4 to IPv6. This has begun, but will take year to get complete. (That means all the computers 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.

Scanned by CamScanner

- But when a packet goes out of the company, and goes to ISP, the translation of IP address takes place there.
- In order to make this scheme work, three ranges of IP addresses have been declared as private. Companies can use these addresses internally as per their requirement. However no packet containing these addresses is allowed to appear on the Internet. The three reserved ranges are as follows :

Range 1	10.0.0.0 to 10.255.255.255/8	16777216 Hosts
Range 2	172.16.0.0 to 173.31.255.255/12	1048 576 Hosts
Range 3	192.168.0.0 to 192.168.255.255/16	65 536 Hosts

- Generally most companies choose the addresses from the first range.
- Refer Fig. 5.12.1 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. 5.12.1 to the company's true IP address 198.60.42.10.
- The NAT box is generally combined with a firewall. It is also possible to integrate the NAT box into company's router.



(G-551) Fig. 5.12.1 : NAT

5.13 Internet Protocol Version 4 (IPv4) :

MU : May 15, May 16, Dec. 17

University Questions

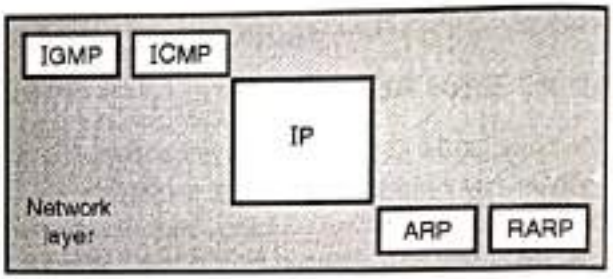
Q. 1 What is the function of IP protocol ? Discuss its header format. **(May 15, 10 Marks)**

Q. 2 What is IPv4 protocol ? Explain the IPv4 header format with diagram. **(May 16, Dec. 17, 10 Marks)**

- We have already discussed the addressing mechanism, delivery and forwarding for the IP packets.
- Now we will discuss the format of IP packet in the next few sections.
- In the discussion we will see that an IP packet consists of a base header and options which are sometimes useful in controlling the packet delivery.

5.13.1 Position of IP :

- 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. 5.13.1.



(G-524) **Fig. 5.13.1 : Protocols at network layer**

- Out of these protocols IP is the most important protocol. It is responsible for host to host delivery of datagrams from a source to destination. But IP needs to take services of other protocols.
- IP takes help from ARP in order to find the MAC (physical) address of the next hop.
- IP uses the services of ICMP during the delivery of the datagram packets to handle unusual situations such as presence of an error.
- IP is basically designed for unicast delivery. But some new Internet applications as well as multimedia need multicast delivery.
- So for multicasting, IP has to use the services of another protocol called IGMP.
- IPv4 is the current version of IP whereas IPv6 is the latest version of IP.

5.13.2 Internet Protocol (IP) :

MU : May 11, Dec. 11, May 15, May 16.

New Syll. : Dec. 18

University Questions

Q. 1 What is IPv4 protocol ? Explain the IPv4 header format with diagram. **(May 11, Dec. 11, 10 Marks)**

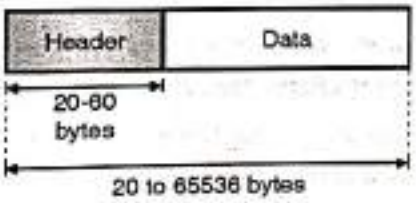
- The Internet Protocol is the host to host delivery protocol which belongs to the network layer and is designed for the Internet.
- IP is used as the transmission mechanism by the TCP / IP protocols. That means the TCP or UDP packets are encapsulated in the IP packet and the IP carries it from source to destination.
- IP is a connectionless datagram protocol with no guarantee of reliability.

Scanned by CamScanner

- It is an unreliable protocol because it does not provide any error control or flow control.
- IP can only detect the error and discards the packet if it is corrupted.
- If IP is to be made more reliable, then it must be paired with a reliable protocol such as TCP at the transport layer.
- Each IP datagram is handled independently and each one can follow a different route to the destination.
- So there is a possibility of receiving out of order packets at the destination. Some packets may even be lost or corrupted.
- IP relies on a higher level protocol to take care of all these problems.
- The version of IP that we are going to discuss is called as IPv4 i.e. IP version 4.
- IP is also called as a **best effort delivery protocol.** The meaning of the term best effort delivery is that the IP packet can get lost or corrupted or delayed. They may arrive out of order at the destination or may create congestion in the network.

5.13.3 Datagrams :

- Packets in IP layer are called datagrams. Fig. 5.13.2 shows the typical format of an IP packet.
- A datagram has two parts namely the header and data as shown. The length of datagram is not fixed. It varies from 20 bytes to 65536 bytes.
- The length of the header is 20 to 60 bytes. The information necessary for the routing and delivery of the datagram has been stored in the header.
- The other part of the datagram is the data field which is of variable length.



(G-525) **Fig. 5.13.2 : IPv4 datagram format**

- It is a custom in TCP/IP to show the header in 4-byte (32 bit) sections.

5.13.4 IPv4 Header Format :

MU : May 10, May 11, Dec. 11, May 12, May 13, Dec. 13, May 15, May 16, Dec. 17, New Syll. : Dec. 18

University Questions

Q. 1 Draw and explain the structure of IP Frame Header. **(May 10, 10 Marks)**

Q. 2 What is IPv4 protocol ? Explain the IPv4 header format with diagram. **(May 11, Dec. 11, 10 Marks)**

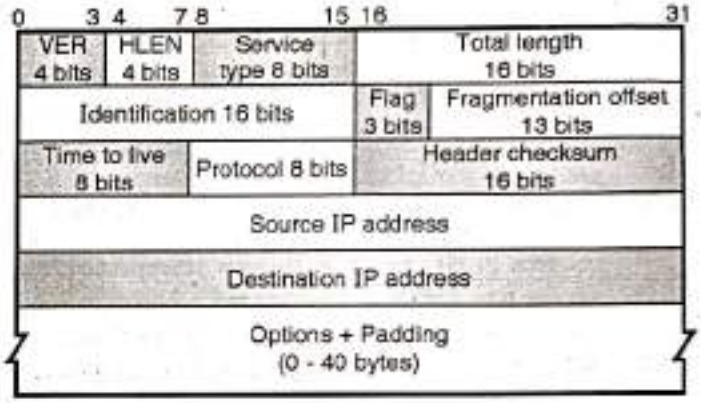
Q. 3 Describe the IPv4 header format in detail. **(May 12, May 13, 10 Marks)**

Q. 4 Write short notes on : IP header format. **(Dec. 13, 10 Marks)**

Q. 5 What is the function of IP protocol ? Discuss its header format. **(May 15, 10 Marks)**

Q. 6 What is IPv4 protocol ? Explain the IPv4 header format with diagram. **(May 16, Dec. 17, 10 Marks)**

- The IP frame header contains routing information and control information associated with datagram delivery. The IP header structure is as shown in Fig. 5.13.3.



(G-2082) **Fig. 5.13.3 : IPv4 header format**

- Various fields in the header format are as follows :

1. VER (Version) :

- This is a 4 bit field which is used to define the version of IP protocol. The current version of IP is 4 i.e. IPv4 but in future it may be completely replaced by the latest version of IP i.e. IPv6.
- This field will indicate the IP software running on the processing machine that this datagram belongs to IPv4 version.
- If the processing machine is using some other version of IP, then the datagram will be discarded.

2. HLEN (Header length) :

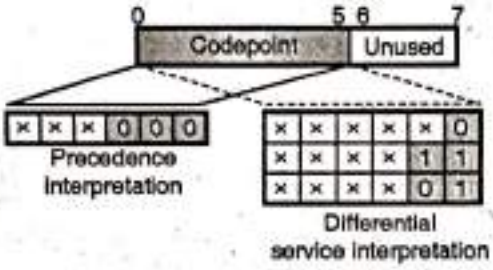
- This 4-bit long field is used for defining the length of the datagram header in 4-byte words.
- The value of this field is multiplied by 4 to get the length of the IPv4 header which varies between 20 and 60 bytes.
- When there are no options, the value of this field is 5 and the **header length** is $5 \times 4 = 20$ bytes.
- When the value of option field is maximum the value of HLEN field is 15 and the corresponding header length is maximum i.e. $15 \times 4 = 60$ bytes.

3. Service type :

- In the earlier designs of IP header, this field was called as **Type of Service (TOS)** field and its job was to define how the datagram should be handled.

Scanned by CamScanner

- At that time, a part of this field used to define the precedence of datagram and the remaining part used to define the type of service out of different possible services such as low delay, high throughput etc.
- But now the interpretation of this field has been changed by IETF. This field is now supposed to define a set of **differential services.** Fig. 5.13.4 illustrates the new interpretation of the **service type** field.



(G-2083) **Fig. 5.13.4 : New interpretation of service type field**

- As seen in Fig. 5.13.4, in the new interpretation, the service type field is divided into two subfields namely, the 6 bit **codepoint** subfield and a 2 bit **unused** subfield.
- We can use the 6-bit **codepoint** subfield in two different ways, as follows :
  1. For the purpose of precedence interpretation.
  2. For the differential service interpretation.

Precedence interpretation :

- If the three right most bits are zeros, then the three leftmost bits are interpreted the same as the precedence bits in the service field (old interpretation). That means it is compatible with the old interpretation of this field.
- The precedence interpretation is used for defining the priority level of this datagram (from 0 to 7) in the situations like congestion.
- In the event of congestion, the datagrams with lowest precedence (0) will be discarded first.

Differential service interpretation :

- When the three rightmost bits are not all zeros, the 6 bit codepoint subfield is used for differential service interpretation.
- In that case these 6 bits can be used for defining a total of 56 (64 – 8) services, on the basis of the priorities assigned by the Internet or local authorities as per Table 5.13.1.

Table 5.13.1 : Values of codepoints

Category	Codepoint	Assigning authority
1.	×××××0	Internet
2.	××××11	Local
3.	××××01	Temporary or Experimental

- The first, second and third categories contain 24, 16 and 16 service types respectively.
- The Internet authorities assign the first category. The local authorities assign the second while the third one is temporary and can be used for experimental purposes.

4. Total length :

- This 16 bit field is used to define the total length of the IP datagram. The total length includes the length of header as well as the data field.
- The field length of this fields is 16 bits so the total length of the IP datagram is restricted to $(2^{16} - 1)$ = 65535 bytes out of which 20 to 60 bytes constitute the header and the remaining bytes are reserved to carry data from upper layers.
- This field allows the length of a datagram to be upto 65,535 bytes, although such long datagrams are impractical for most hosts and networks.
- All hosts must be prepared to accept datagram of upto 576 bytes, regardless of whether they arrive whole or in the form of fragments.
- The hosts are recommended to send datagram larger than 576 bytes only if the destination is prepared to accept larger datagram.
- We can find the length of data by subtracting the header length from the total length.
- As stated earlier the header length can be obtained by multiplying the contents of HLEN field by four.

∴ Length of data = Total length – header length

- The total length (maximum value) of 65,535 bytes might seem to be large but in future the size of IP datagram is likely to increase further because the improvement in technology will allow more bandwidth.

Why do we need the total length field ?

- We might feel that the **total length** field is not at all required because the host or router will drop the header and trailer when it receives a frame. Then why to include this field ?
- The answer to this question is that in many situations we do not need this field at all.
- But in some special situations, only the datagram is not encapsulated in the frame but there are some padding bits as well that are included.
- In such situations, the machine (host or router) that decapsulates the datagram, needs to check the **total length** field so as to understand how much is the data and how much is the padding ?

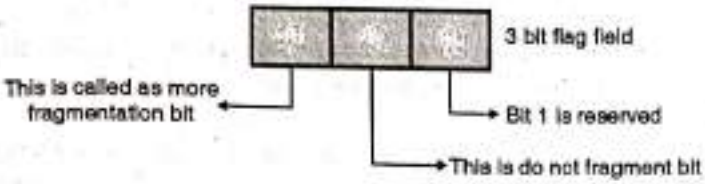
5. Identification :

- This field is used to identify the datagram originating from the source host. When a datagram is fragmented, the contents of the identification field get copied into all fragments. This identification number is used by the destination to reassemble the fragments of the datagram.

Scanned by CamScanner

6. Flags :

- **Flags :** This is a three bit field. The 3 bits are as shown in Fig. 5.13.5.

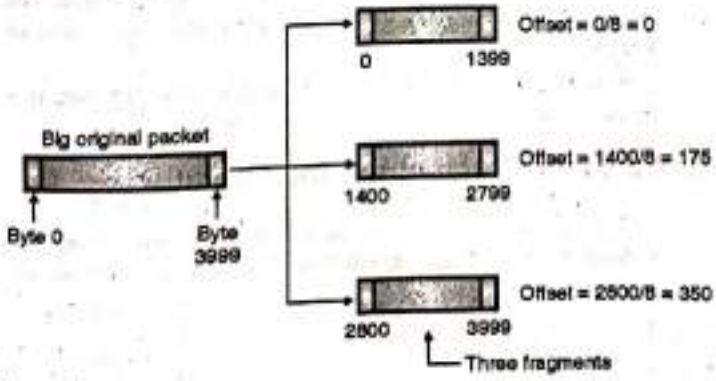


(G-527)**Fig. 5.13.5 : Flag bits**

- First bit is reserved, and it should be 0.
- The second bit is known as the "Do Not Fragment" bit. If this bit is "1" then machine understands that the datagram is not to be fragmented.
- But if the value of this bit is 0 then the machine should fragment the datagram if and only if necessary.
- The third bit is known as "More Fragment Bit" (M). M = 1 indicates that the datagram is not the last fragment and M = 0 indicates that this is the last or the only fragment.

7. Fragmentation offset :

- This is a 13 bit field which is used to indicate the relative position of this fragment with respect to the complete datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.
- To understand this refer Fig. 5.13.6.
- 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. 5.13.6.
- The offset is measured in units of 8 bytes. Because the length of the offset field is 13 bits, so the fragments should be of size such that first byte number is divisible by 8.



(G-528)**Fig. 5.13.6 : Example of fragmentation**

8. Time to Live (TTL) :

- This is an 8-bit field which controls the maximum number of routers visited by the datagram during its lifetime.
- A datagram has a limited lifetime for travelling through an Internet.
- Originally the TTL field was designed to hold the **timestamp.** This timestamp value was decremented by one, everytime the datagram visits a router.
- As soon as the timestamp value reduces to zero the datagram is discarded. But for this scheme to become successful, all the machines must have synchronized clocks and they must know the time taken by a datagram to travel from one router to the other.
- Today the TTL field is used to **control** the maximum number of hops i.e. router by a datagram.
- At the time of sending a datagram, the source host will store a number in the TTL field. This number is approximately twice the maximum number of routers present between any two hosts.
- Everytime this datagram visits a router, this value is decremented by one. If after decrementing, the value of TTL field reduces to zero then that router discards the datagram.

Need of TTL field :

- Sometimes the routing tables in the Internet get corrupted, due to which a datagram may travel between two or more routers for a very long time but never ever gets delivered to the destination host.
- The TTL field is needed in such situations for **limiting the lifetime of a datagram.**
- The TTL field is also used to **limit the journey of a packet intentionally.** For example if a packet is to be confined to a local network only then a 1 is stored in the TTL field of this packet.
- As soon as it reaches the first router, then TTL field value is decremented from 1 to 0 and the packet will be discarded.

9. Protocol :

- This is an 8-bit field which is used for defining the higher level protocol which uses the services of IP layer.
- The data from different high level protocols can be encapsulated into an IP datagram. These protocols could be UDP, TCP, ICMP, IGMP etc.
- The protocol field contents would tell the name of the protocol at the final destination to which this IP datagram is to be delivered.
- At the destination, the value of this field helps in the process of demultiplexing.
- Table 5.13.2 shows some of the values of this field corresponding to different high level protocols.

Scanned by CamScanner

Table 5.13.2

Value	Protocol	Value	Protocol
1	ICMP	17	UDP
2	IGMP	89	OSPF
6	TCP		

10. Header checksum :

A checksum in IP packet covers on the header only. Since some header fields change, this field is recomputed and verified at each point that the Internet header is processed.

11. Source address :

This field is used for defining the IP address of the source. It is a 32 bit field.

12. Destination address :

This field is used for defining the IP address of the destination. It is also a 32 bit field.

13. Options :

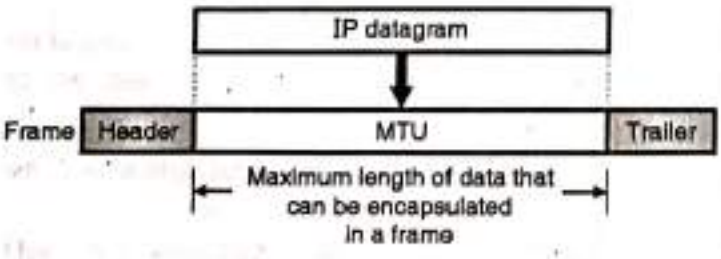
Options are not required for every datagram. They are used for network testing and debugging. We have discussed all the options in detail, later in this chapter.

5.14 Fragmentation :

- In the Internet, a datagram sent by a host has to travel through different networks before it is delivered to the destination host.
- At every router, the received frame is decapsulated, the IP datagram is extracted and processed and encapsulated in another frame.
- The size and format of the frame received by a router depends on the protocol used by the previous physical network to the router.
- As an example, imagine that a router connects a LAN to a WAN. Then the frame received by the router is in the LAN format and the one forwarded by it is in the WAN format.

5.14.1 Maximum Transfer Unit (MTU) :

- The frame format of each data link layer protocol is different in its own way. One of the important field in the frame format is the **maximum size of data field.**
- Therefore when we encapsulate an IP datagram in a frame, the datagram size should be less than the maximum data size specified by the maximum size field.
- The concept of MTU has been illustrated in Fig. 5.14.1.



(G-2084) **Fig. 5.14.1 : Concept of MTU**

- Now the problem is that the value of MTU changes from one protocol to the other used for the physical network.
- We have to make the IP protocol independent of the physical network. In order to do so the maximum length of IP datagram was decided to be equal to 65,535 bytes.
- If we use a physical network protocol which has MTU = 65,535 bytes, then the transmission will become more efficient.
- For the other protocols having MTU smaller than 65,535 bytes, the IP datagram is divided into small parts called **fragments** so that they can pass through the physical networks successfully.
- This processes of dividing the IP datagram in smaller parts is called as **fragmentation.**
- The fragmentation generally does not take place at the source because the transport layer there will adjust the segment size in such a way that they will fit in the IP datagrams and data link layer frames.
- After **fragmentation,** each fragment will have its own header. Most of the fields of the original header are copied into the fragment header but some fields are changed.
- Such a fragmented datagram can be fragmented further if it comes across a network with even smaller MTU.
- The fragmentation of a datagram can be carried by the source host or any router on the route of the datagram.
- But the process of reassembly of all the fragments will be carried out only by the **destination host.**
- All the fragments of a datagram are free to take any route and we do not have any control over them. In short each fragment acts as an independent datagram.
- The reassembly of fragments is not done during the transmission because of the loss of efficiency associated with it.
- At the time of fragmentation, all the required parts of the header are copied into the fragments. But the **options** field may or may not be copied as discussed later on.
- The following three fields are altered when the host or router fragments a datagram :
  1. Flags.
  2. Fragmentation offset.
  3. Total length.
- The remaining fields in the IP header are copied as it is. The value of checksum should be calculated again regardless of fragmentation.
- And the final point about fragmentation is that only data in a datagram is fragmented.

5.14.2 Fields Related to Fragmentation :

- The following three fields in an IP datagram header are related to the fragmentation and reassembly of an IP datagram.
  1. Identification.
  2. Flags and
  3. Fragmentation offset field.

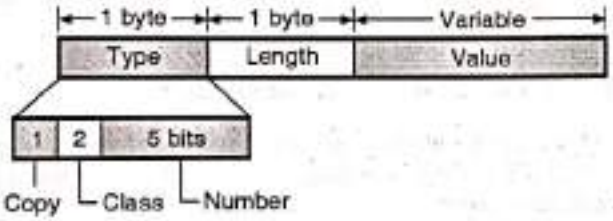
Scanned by CamScanner

5.15 Options :

- In the IP header there are two parts : A fixed part and a variable part. We have already discussed the fixed part of 20 byte length.
- At the most 40 byte long variable part consists of options which we are going to discuss in this section.
- Options as the name suggests are not required for a datagram. Their main application is for network testing and debugging.
- Options are not a required part of a datagram but **option processing** is very much a required part of the IP software.
- This implies that if the options are present in the header, then all the implementations should be able to handle them.

5.15.1 Format :

- The format of an option has been shown in Fig. 5.15.1. As shown, it consists of three fields namely, a type field (1-byte), length field (1-byte) and a variable length value field.



(G-2085) **Fig. 5.15.1 : Option format**

- Let us discuss these fields one by one.

1. Type :

- As shown in Fig. 5.15.1, the type field is an 8-bit field and it contains three subfields as follows :
  1. Copy (1 bit).
  2. Class (2 bits).
  3. Number (5 bits).

(a) Copy :

- This is a 1 bit subfield. So it can have only two possible values, 0 or 1. If copy = 0, then the option must be copied only into the first fragment.
- Whereas if copy = 1, then the option field must be copied into all the fragments.

Copy	Meaning
0	Copy option field only in first fragment.
1	Copy option field in all fragments.

(b) Class :

- This 2-bit subfield is used to define the purpose of option. It has four possible values, out of which only two (00 and 10) are defined right now. The other two possible values (01 and 11) are not yet defined.
- If class = 00, it indicates that the option is being used for datagram control. Whereas if copy = 10 then the option is used for debugging and management.

Copy	Meaning
00	Datagram control.
01	Not defined or reserved.
10	Debugging and management.
11	Not defined or reserved.

(c) Number :

- This 5-bit subfield is used for defining the type of option. This subfield has 32-possible values (types), but currently only 6-types are defined as shown in Table 5.15.1.

Table 5.15.1

Number	Type of option
00000	End of option.
00001	No option.
00011	Loose source route
00100	Timestamp
00111	Record root
01001	Strict source route

- We will discuss these later in this chapter.

2. Length :

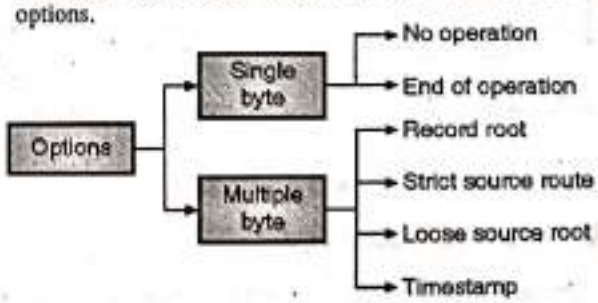
- This 8-bit field is used for defining the total length of the option with the type field and the length field included.
- The length field will not be present in all the option types.

3. Value :

- This is variable length field which contains the specific data which is required by that option.
- Similar to the length field, the value field also will not be present in all the option types.

5.16 Option Types :

- As we started earlier, only six options are being used currently. Fig. 5.16.1 shows the classification of these options.



(G-2086) **Fig. 5.16.1 : Categories of options**

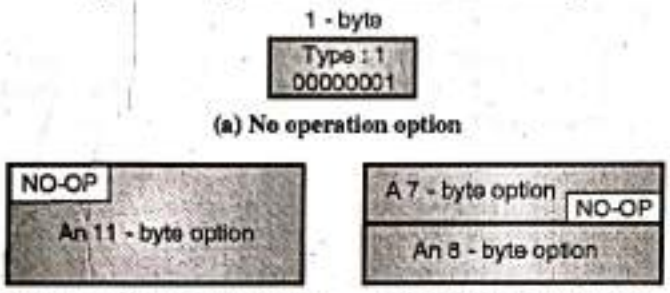
- Options are classified into two option types i.e. single byte options and multiple byte options.

Scanned by CamScanner

- There are two single byte options which do not require the data or length fields.
- The remaining four options are multibyte options which require the data and length fields.
- Let us now discuss these options one by one.

5.16.1 No Operation Option :

- This is **a single byte** option which is being used as a **filler** between options.
- As shown in Fig. 5.16.2, we can use the no operation option to align the next option on a 16 bit or 32 bit boundary.



(a) No operation option

(b) NO-OP is being used to align beginning of an option

(c) NO-OP is being used to align the next option

(G-2087) **Fig. 5.16.2 : No operation option**

5.16.2 End of Option Option :

- The second one byte option is the **end of option** option. It finds its application in **padding** at the end of the option field.
- Two important points about this option are as follows :
  1. We can use it only as the last option.
  2. We can use only one end of option. That means after this option, the receiver should expect the **payload data** to arrive.
- There if we need more than 1 byte to align the option field, then we must use more than one **no-operation** options and after that only one end-of-operation option as shown in Fig. 5.16.3.

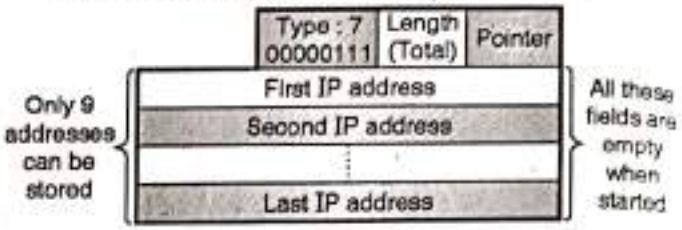
(a) End-of-option

(b) Used for padding

(G-2088) **Fig. 5.16.3**

5.16.3 Record-Route Option :

- The record route option is a multiple byte option and it is used for recording the Internet routers which handle the datagram.
- Since the maximum size of the header is 60 bytes, including 20 bytes of base header, this option can list upto 9-IP addresses of the routers.
- So actually only 40 bytes are left for the option part. The format of the record-root option is as shown in Fig. 5.16.4. The source creates fields that are to be filled by each router visited by the datagram.

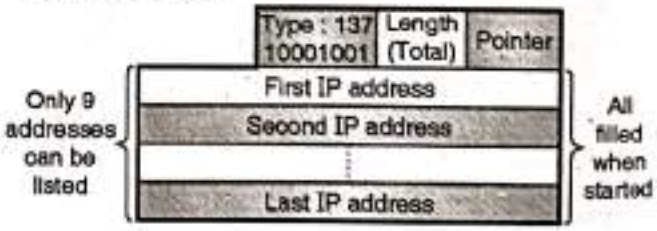


(G-2089) **Fig. 5.16.4 : Round trip option**

- The pointer field is an offset integer field which contains the byte number of the first empty entry. That means it points towards the first available entry.
- All the empty fields for the IP address are empty when the datagram leaves the source. The value of pointer field is 4 which points to the first empty field.
- When the datagram starts travelling, each router visited by this datagram, will insert its outgoing IP address in the next empty field and increments the value of pointer by 4.

5.16.4 Strict-Source-Route Option :

- This is also a multi byte option which is used by the source to determine the route in advance for the datagram travelling over the Internet.
- Due to this it becomes possible for the sender to choose root to get a specific type of service (i.e. minimum delay, maximum throughput etc.).
- It is also possible for a sender to choose a safer and more reliable root.
- If a datagram specifies a strict source route, then the datagram must visit all the routers which are defined in the option.
- It should not visit any router whose IP address is not listed in the datagram. If it does so then that datagram will be discarded and an error message will be issued.
- However the strict source routing is not generally preferred even by the regular users of the Internet, as they are not much aware of the physical topology of the Internet.
- Fig. 5.16.5 shows the format of the strict source route option. You will see that it is very similar to the format of the **record-root option** that we have discussed earlier with one exception that all the nine IP addresses of routers are entered by the sender itself.



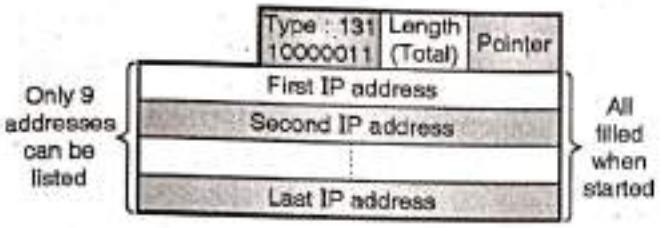
(G-2090) **Fig. 5.16.5 : Format of strict source root option**

5.16.5 Loose-Source-Root Option :

- This option is similar to the strict source root option discussed earlier. However this option is not as strict as the strict source root option, it is more relaxed.

Scanned by CamScanner

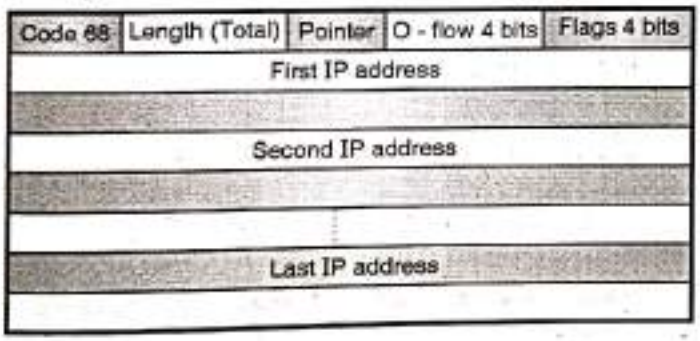
- Here each router whose IP address is mentioned in the list must be visited by the datagram as before but the datagram is allowed to visit the other routers also.
- Fig. 5.16.6 shows the format of the loose-source-root option.



(G-2091) **Fig. 5.16.6 : Format of loose-source root option**

5.16.6 Time Stamp Option :

- The time stamp option is a multiple byte option and it is used for recording the time of datagram processing by a router, i.e. the time instant at which the datagram is processed by a router.
- This time is measured from midnight universal time and expressed in milliseconds.
- The users and managers can use the time of processing a datagram to track the behavior of the router in the Internet.
- With the help of the time stamp option, we can estimate the time taken by a datagram to travel from one router to the other.
- However this option is not used by most of the Internet as they are not aware of the physical topology of the Internet. Fig. 5.16.7 shows the format of the time stamp option.



(G-2092) **Fig. 5.16.7 : Format of timestamp option**

5.17 Checksum :

- Most TCP/IP protocol use the error detection method which is called as **checksum.** The purpose of using the checksum is to protect the packet from the corruption that may happen when the packet travels from source to destination.
- Checksum does not carry any information. Therefore it is the **redundant** bits added to the packet.
- The sending machine calculates the checksum and send its value with the packet. At the receiver the same calculation is performed on the whole packet including the checksum.
- The receiver will accept the packet if the result of the calculation is **satisfactory.** Otherwise the packet will be rejected.

5.17.1 Checksum Calculation at the Sender :

- At the sending end, the packet header is divided into n-bit sections (the value of n is generally 16).
- All these sections are added together using the one's complement arithmetic. The addition (sum) will also be 16 bit long.
- The **checksum** is obtained by inverting (complementing) all the bits in the sum.

Steps to calculate the checksum :

1. Divide the packet into K sections with each section containing n-bits.
2. Add all the K-sections together using one's complement arithmetic.
3. Complement the final result of addition to obtain the checksum.

5.17.2 Checksum Calculation at the Receiver :

- The receiver receives the packet and divides it into K sections and then adds all the sections.
- The result of addition is then complemented. The packet is accepted if the final result is zero, otherwise it is rejected.

Checksum in the IP packet :

- If we want to implement the checksum in an IP packet then we should follow the same principle discussed earlier in this section.
- The stepwise procedure for calculating the checksum is as follows :
  1. Set the value of the checksum field to 0.
  2. Divide the entire header into 16 bit sections and add all of them together.
  3. Complement the result (sum).
  4. Insert the complemented result into the checksum field.
- In the IP packet, the checksum covers only the header and not the data due to the following three reasons :
  1. All the high level protocols, which encapsulate their data in the IP datagram have a checksum field which takes into account the whole packet. Therefore the IP datagram need not consider the encapsulated data again while calculating its own checksum.
  2. The second reason is that when an IP packet visits a router, only its header changes but there is no change in data. Therefore, the checksum should take into account only that part which changes i.e. the header.
  3. If the data were included in the checksum calculation, then each router would have to recalculate the checksum for the whole packet which would increase the **processing time.**

5.18 Routing :

- Routing is a very important issue in the network layer. A router creates its routing table so as to help forwarding a

Scanned by CamScanner

datagram in the connectionless services. It also helps in creating a virtual circuit in the connection oriented service.

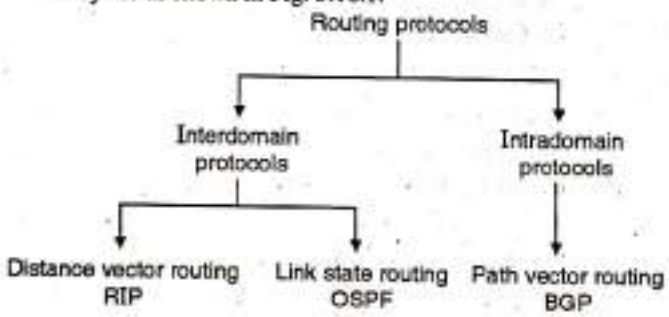
- In the following sections we are going to discuss about the types of routing and different routing algorithms such as distance vector routing, link state routing and hierarchical routing.

5.18.1 Types of Routing :

- Routing can be broadly classified into three types :
  1. Unicast routing.
  2. Broadcast routing
  3. Multicast routing.
- We can also classify the routing into two types as follows :
  1. Intradomain routing.
  2. Interdomain routing.

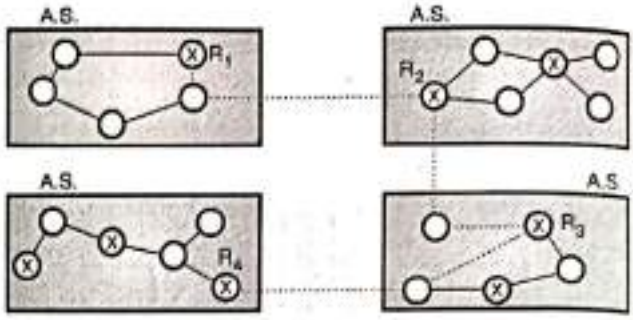
5.18.2 Intra and Interdomain Routing :

- Today the size of the internet is so big that one routing protocol cannot handle the task of updating the routing tables of all the routers.
- Hence an internet is divided into **Autonomous Systems** (AS). An Autonomous System (AS) is a group of networks and routers which is controlled by a single administrator. An AS is shown in Fig. 5.18.1.
- The **intradomain routing** is defined as the routing inside an autonomous system whereas the routing between autonomous system is known as the **interdomain routing.**
- Several intradomain and interdomain protocols are used. They are as shown in Fig. 5.18.1.



(G-1291) **Fig. 5.18.1 : Classification of routing protocols**

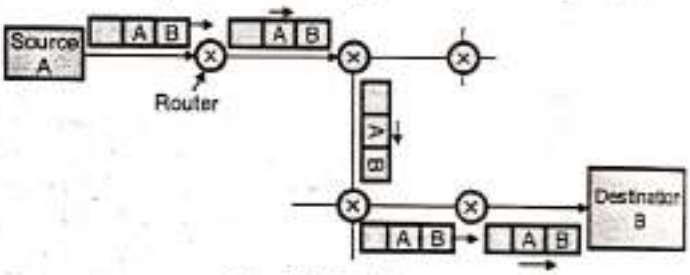
- The examples of interdomain routing protocols are :
  1. Distance vector routing
  2. Link state routing.
- An example of intradomain routing protocol is path vector routing.
- Each A.S. is allowed to choose one or more intradomain routing protocols in order to handle the routing inside the A.S. But only one interdomain routing protocol will handle routing between autonomous systems.
- The Routing Information Protocol (RIP) is an implementation of distance vector routing. Whereas the OSPF is an implementation of link state protocol. The BGP is an implementation of the path vector protocol.



(G-1292) **Fig. 5.18.2 : Autonomous systems**

5.18.3 Unicast Routing :

- In unicast routing there is a one to one relation between the source and the destination. That means only one source sends packets to only one destination.
- The type of source and destination addresses included in the IP datagram are unicast addresses assigned to the hosts.
- The concept of unicast routing is illustrated in Fig. 5.18.3.



(G-448) **Fig. 5.18.3 : Unicast routing**

- In unicast routing when a router receives a packet, it forwards that packet through only one of its ports which corresponds to the optimum path.
- The router can discard the packet if it can not find the destination address.

Metric :

- A metric is defined as the cost assigned for passing through a network.
- The metric assigned to each network depends on the type of protocol.

Interior and exterior routing :

- An Internet is so large that for one routing protocol it is impossible to handle the task of updating the routing tables of all the routers.
- So an Internet is divided into a number of Autonomous Systems (AS). An AS is group of networks and routers.

Interior routing :

The routing that takes place inside an AS is called as interior routing.

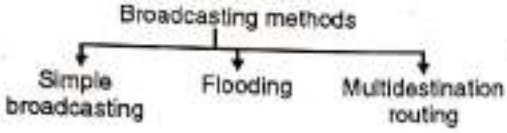
Exterior routing :

The routing that takes place among various autonomous systems is called as exterior routing.

Scanned by CamScanner

5.18.4 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.**
- Various methods of broadcasting are as follows :



(G-449) **Fig. 5.18.4 : Various methods of broadcasting**

1. Simple broadcasting :

- In this method the source will simply send a distinct (a separate) packet to each destination.
- This method has two drawbacks :
  1. A lot of bandwidth is wasted.
  2. The source has to have a complete list of all destinations.

2. Flooding :

- Flooding is another method used for broadcasting. The problem with flooding is that it has a point to point routing algorithm.
- So it consumes a lot of bandwidth and generates too many packets.

3. Multidestination routing :

- This is the third algorithm used for broadcasting.
- In this algorithm each packet will contain a list of destinations or a bit map which indicates the desired destination.
- When such a packet arrives at a router, the router first checks all the destinations. Then it decides the set of output lines that will be required based on the destination addresses.
- The router then generates a new copy of the received packet for each output line to be used. It includes a list of only those destinations that are to use the line in each packet going out on that line. This will save bandwidth to a great extent. Also generation of too many packets right from the sending end will also be avoided.

5.18.5 Multicast Routing :

- In multicasting a message from a sender is to be sent to a group of destinations but not all the destinations in a network.
- A process has to send a message to all other processes in the group. For a small group it is possible to send a point-to-point message.
- But this is expensive if the group is large. So we have to send messages to a well defined groups which are small compared to the network size.
- Sending message to such a group is called **multicasting** and the routing algorithm used for multicasting is **multicast routing.**
- Multicast routing is a special class of broadcast routing.

5.19 Routing Algorithms :

- One of the important functions of the network layer is to route the packets from the source machine to the destination machine.
- The major area of network layer design includes the algorithms which choose the routes and the data structures which are used.
- **Routing algorithm** is a part of network layer software. It is responsible for deciding the output line over which a packet is to be sent.
- Such a decision is dependent on whether the subnet is a virtual circuit or it is datagram switching.

5.19.1 Desired Properties of a Routing Algorithm :

- There are certain desirable properties of a routing algorithm as follows :
  1. Correctness 2. Robustness
  3. Stability 4. Fairness and
  5. Optimality.

5.19.2 Types of Routing Algorithms :

MU : Dec. 04, May 05, May 07, May 08, Dec. 08, May 09, Dec. 12, May 13, Dec. 15

University Questions

Q. 1 What are the different types of Routing Algorithms ? Explain any one in detail. **(Dec. 04, May 05, May 07, May 13, 10 Marks)**

Q. 2 Explain different types of routing algorithm. **(May 08, Dec. 08, May 09, 10 Marks)**

Q. 3 What are the different types of routing ? Explain distance vector routing. **(Dec. 12, 10 Marks)**

Q. 4 What are the different types of routing algorithms ? When would we prefer to use hierarchical routing over link state routing ? **(Dec. 15, 10 Marks)**

- Routing algorithms can be divided into two groups :
  1. Non-adaptive algorithms.
  2. Adaptive algorithms.

1. Non-adaptive algorithms :

- For this type of algorithms, the routing decision is not based on the measurement or estimation of current traffic and topology.
- However the choice of the route is done in advance, off-line and it is downloaded to the routers.

Scanned by CamScanner

- This is called as static routing.

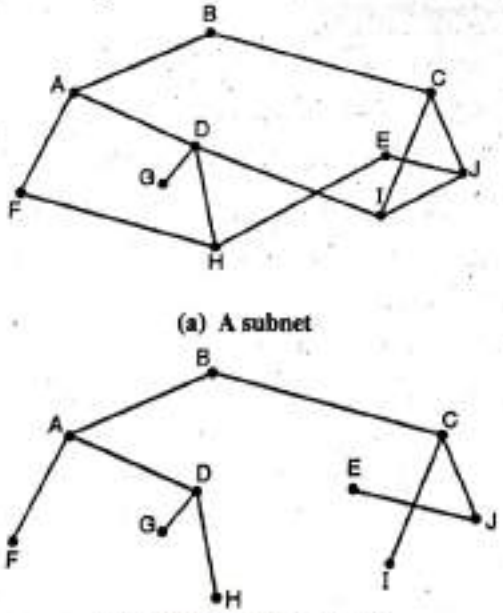
2. **Adaptive algorithms :**
   - For these algorithms the routing decision can be changed if there are any changes in topology or traffic etc.
   - This is called as dynamic routing.
   - In the following sections we are going to discuss various static and dynamic algorithms.

5.19.3 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. 5.19.1. 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. 5.19.1, the distance metric is the number of hops. In Fig. 5.19.1(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. 5.19.1

5.20 Static Algorithms :

MU : Dec. 04, May 05, Dec. 05, May 13

University Questions

Q. 1 What are the different types of routing algorithms ? Explain any one in detail. **(Dec. 04, May 05, May 13, 10 Marks)**

Q. 2 What is static routing ? What are advantages of dynamic routing ? Explain shortest path routing in detail ? **(Dec. 05, 5 Marks)**

The examples of static algorithms are :

1. Shortest path routing. 2. Flooding.
3. Flow based routing.

5.20.1 Shortest Path Routing : MU : Dec. 05

University Questions

Q. 1 What is static routing ? What are advantages of dynamic routing ? Explain shortest path routing in detail ? **(Dec. 05, 5 Marks)**

- This algorithm is based on the simplest and most widely used principle. Here a graph of subnet is prepared in which each node represents either a host or a router and each arc represents a communication link.
- So as to choose a path between any two routers, this algorithm simply finds the shortest path between them.

How to decide the shortest path ?

- One way of measuring the path length is the number of hops. Another way (metric) is the geographical distance in kilometres.
- Some other metrics are also possible. For example we can label each arc (link) with the mean queuing and transmission delay and obtain the shortest path as the fastest path.

Labels on the arcs :

- The labels on the arcs can be computed as a function of distance bandwidth, average traffic, mean queue length, cost of communication, measured delay etc.
- The algorithm compares various parameters and calculates the shortest path, on the basis of any one or combination of criterions stated above.

Various shortest path algorithms :

- There are many algorithms for computing the shortest path between two nodes.
- One of them is Dijkstra algorithm. The other one is Bellman-Ford algorithm.

Scanned by CamScanner

5.20.2 Dijkstra's Algorithm :

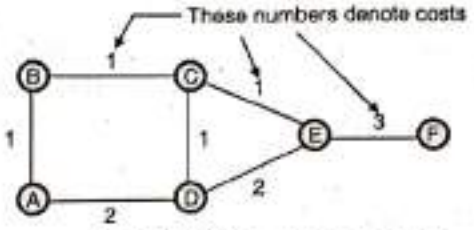
MU : May 10, Dec. 11

University Questions

Q. 1 Explain Dijkstra's algorithm as shortest path routing with example. **(May 10, Dec. 11, 10 Marks)**

- 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 react n.
  4. Stop when T is empty.
- This algorithm will be clear after solving the following example.

Ex. 5.20.1 : For the network shown in Fig. P. 5.20.1(a), show the computations at node A using the Dijkshtra's algorithm.



(G-451) **Fig. P. 5.20.1(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. 5.20.1(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. 5.20.1(a).

(G-451(a)) **Table P. 5.20.1(a)**

Permanent (P)	Temporary (T)
A	B(A,1),D(A,2)

A•

Note : B(A,1) means B is reached by A, and the cost is 1. Similarly D(A,2) means D is reached by A and the cost is 2.

Step 2 :

- Now pick up the neighbour with the smallest cost and add it to P set. Here the neighbour with smallest cost is B. So let us add B(A,1) to P group as shown in Table P. 5.20.1(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. 5.20.1(b).

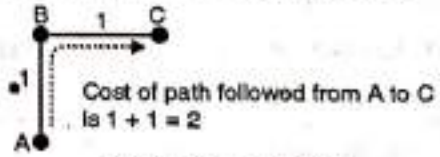
(G-452) **Table P. 5.20.1(b)**

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. 5.20.1(b).



(G-453) **Fig. P. 5.20.1(b)**

Step 3 :

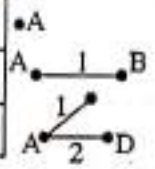
- Now pick up the neighbour in T set with the smallest cost in Table P. 5.20.1(b) and add it to the P set. Here we choose neighbour D because it is the immediate neighbour of A.

Scanned by CamScanner

- 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. 5.20.1(c). Note that C(B,2) goes as it is, and E(D,4) is a new entry to Table P. 5.20.1(c). But C(D,3) can not be entered because its cost is 3.

(G-454) **Table P. 5.20.1(c)**

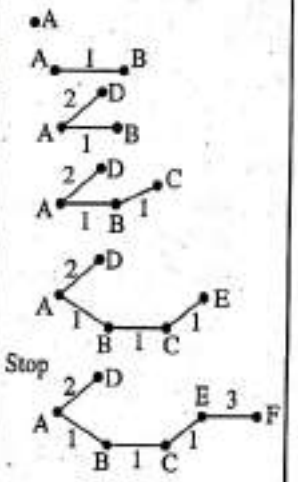
Permanent (P)	Temporary (T)
A	B(A,1),D(A,2)
A,B(A,1)	D(A,2),C(B,2)
A,B(A,1),D(A,2)	E(D,4),C(B,2)



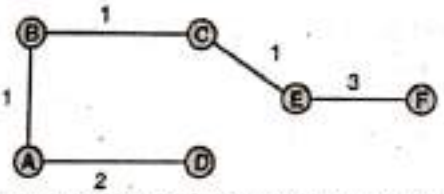
- Where E(D,4) means E is reached by A via D and the cost is 4.
- Similarly we can proceed further. The final table is as shown in Table P. 5.20.1(d).

(G-455) **Table P. 5.20.1(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)

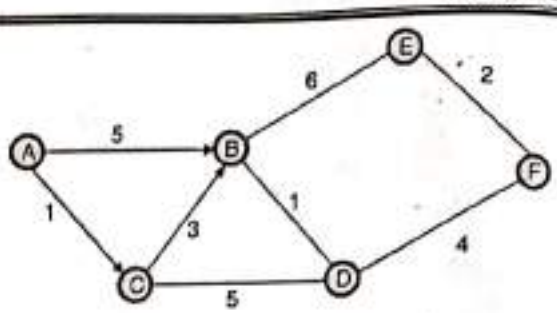


- The shortest paths from A to all other nodes are as shown in Fig. P. 5.20.1(c).



(G-456) **Fig. P. 5.20.1(c) : Shortest paths from A to all other nodes**

Ex. 5.20.2 : For the network shown in Fig. P. 5.20.2(a) show the computations at node A using the Dijkshtra's algorithm.



(G-457) **Fig. P. 5.20.2(a) : Given network**

Soln. :

Step 1 :

- The starting node is A. Enter it in to group P as shown in Table P. 5.20.2(a).
- Add the neighbours B and C to the temporary group T.

(G-457(a)) **Table P. 5.20.2(a)**

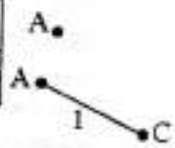
Permanent (P)	Temporary (T)
A	B(A,5),C(A,1)

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. 5.20.2(b).

(G-458) **Table P. 5.20.2(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)



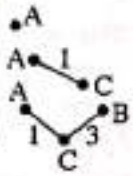
- B(C, 4) is another entry in T group which shows that B is approached by A via C and the cost is 4.

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. 5.20.2(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. 5.20.2(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)



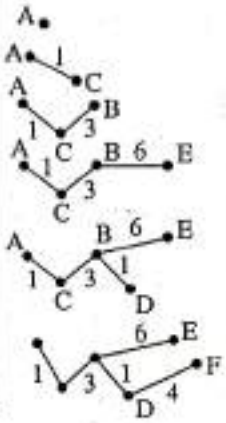
Step 4 :

- Now continue in the same manner to get the final table as shown in Table P. 5.20.2(d).

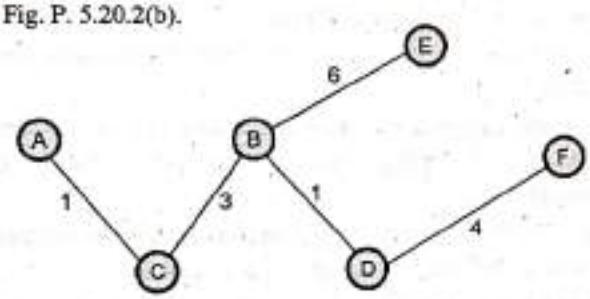
Scanned by CamScanner

(G-460) **Table P. 5.20.2(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)



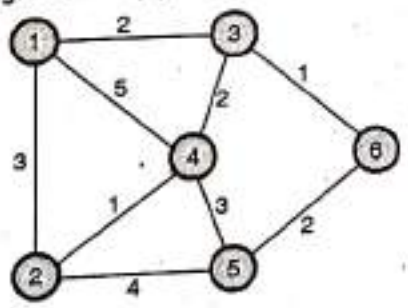
- The shortest path from A to other nodes is shown in Fig. P. 5.20.2(b).



(G-461) **Fig. P. 5.20.2(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. 5.20.3 : Write Dijkstra's algorithm. Find shortest path Fig. P. 5.20.3(a) to destination node 6.



(G-1383) **Fig. P. 5.20.3(a)**

Soln. :

For Dijkstra's algorithm refer section 5.20.2.

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. 5.20.3(a).
- Add neighbours B, C and D to the temporary group T.

Table P. 5.20.3(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. 5.20.3(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.

(G-2303) **Table P. 5.20.3(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. 5.20.3(c).

Table P. 5.20.3(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)

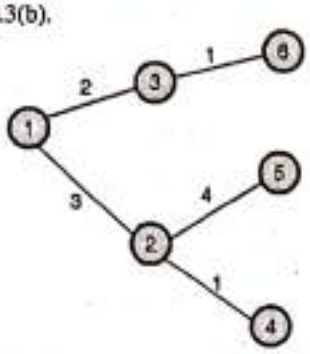
Step 4 : Now continue in the same manner to get the final table as shown in Table P. 5.20.3(d).

Table P. 5.20.3(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)
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)

Scanned by CamScanner

- Shortest path from node 1 to other nodes is shown in Fig. P. 5.20.3(b).



(G-1384) Fig. P. 5.20.3(b) : Shortest path from 1 to all other nodes

5.20.3 Flooding :

- This is another static algorithm.
- In this algorithm every incoming packet is sent out on every outgoing line except the line on which it has arrived. That is why the name flooding. Each line except the incoming lines are flooded with the copies of the same packet.
- One disadvantage of flooding is that it generate 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.

5.21 Dynamic Routing Algorithms :

MU : Dec. 05

University Questions

Q. 1 What is static routing ? What are advantages of dynamic routing ? Explain shortest path routing in detail ? **(Dec. 05, 5 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.

5.21.1 Distance Vector Routing Algorithm :

MU : May 07, Dec. 07, May 11, May 12, Dec. 12, May 17
New Syll. : Dec. 18

University Questions

Q. 1 What are the different types of routing algorithms ? Explain any one in detail. **(May 07, 10 Marks)**

Q. 2 Differentiate forwarding versus routing. Explain distance vector routing. **(Dec. 07, 10 Marks)**

Q. 3 Explain distance vector routing and its count to infinity problem. **(May 11, 10 Marks)**

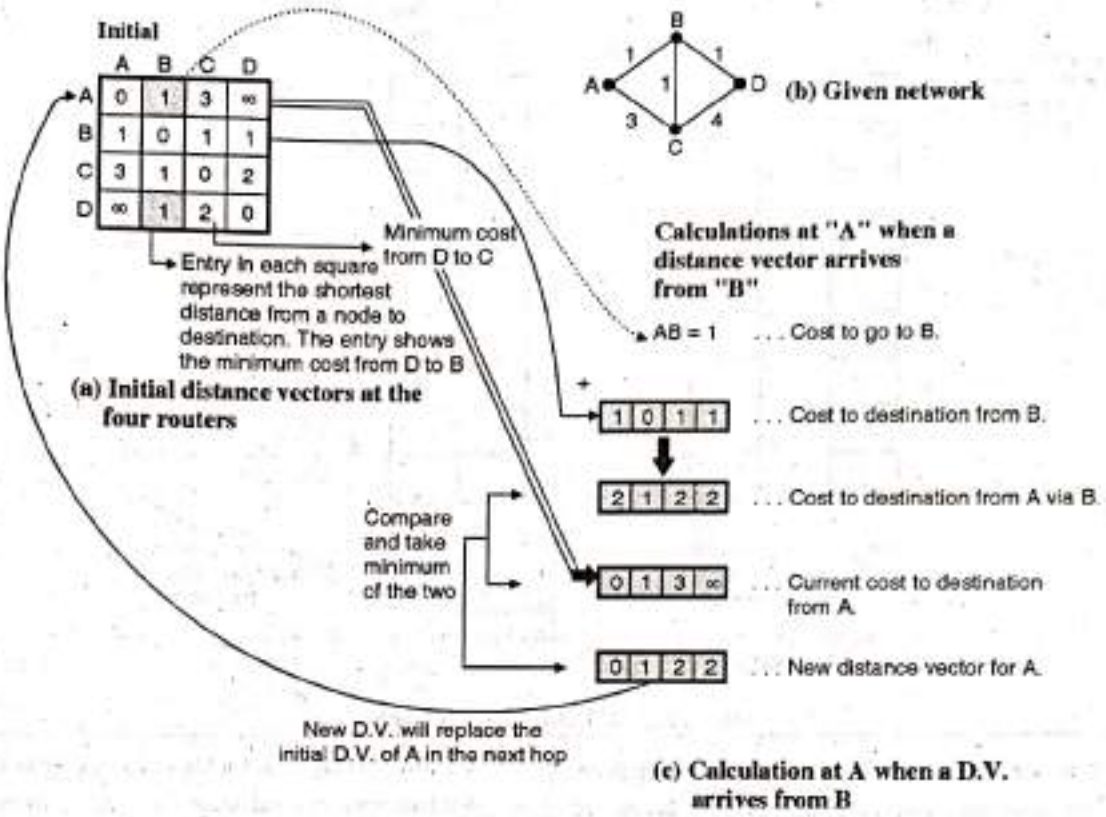
Q. 4 Explain DVR algorithm and mention the drawbacks of the algorithm when put into practice. **(May 12, 10 Marks)**

Q. 5 What are the different types of routing ? Explain distance vector routing. **(Dec. 12, 10 Marks)**

Q. 6 Explain distance vector routing. What are its limitations and how are they overcome ? **(May 17, 10 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.

Scanned by CamScanner



(G-463) **Fig. 5.21.1 : Distance vector algorithm at router A**

- This algorithm is sometimes called by other names such as :
  1. Distributed Bellman-Ford routing algorithm.
  2. Ford-Fulkerson algorithm
- In distance vector routing, each router maintains a routing table. It contains one entry for each router in the subnet.
- This entry has two parts :
  1. The first part shows the preferred outgoing line to be used to reach the specific destination.
  2. Second part gives an estimate of the time or distance to that destination.

Distance vector :

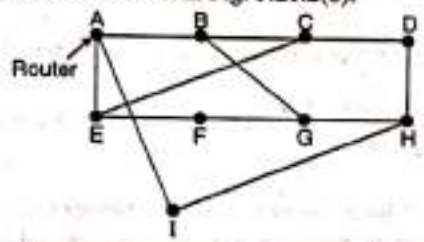
- In distance vector routing, we assume that each router knows the identity of every other router in the network, but the shortest part to each router is not known.
- A **distance vector** is defined as the list of <destination, cost> tuples, one tuple per destination. Each router maintains a distance 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. 5.21.1.
- Fig. 5.21.1 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. 5.21.1(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.

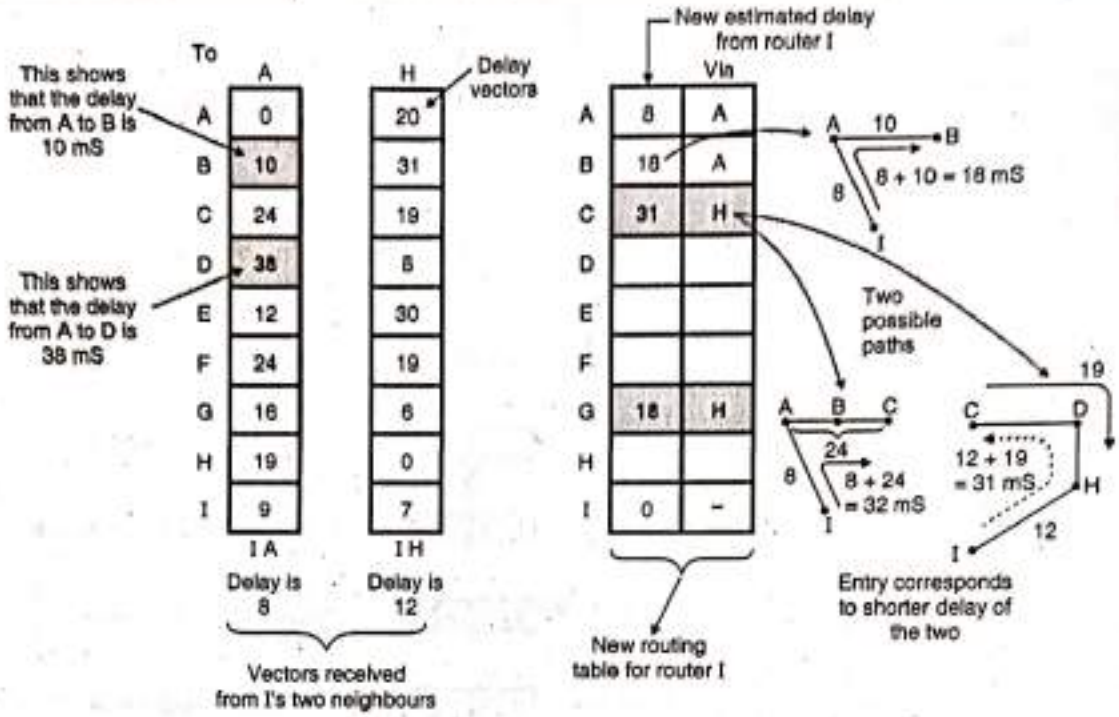
Routing procedure in distance vector routing :

- The example of a subnet is shown in Fig. 5.21.2(a) and the routing tables are shown in Fig. 5.21.2(b).



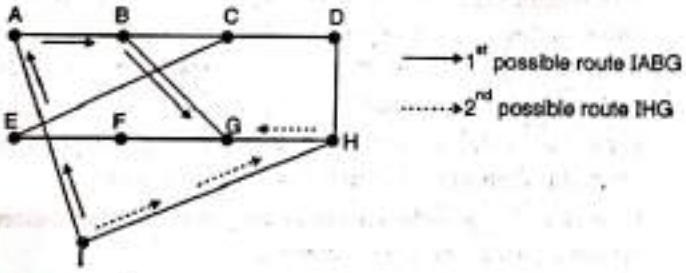
(G-464) **Fig. 5.21.2(a) : A subnet**

Scanned by CamScanner



(G-465) **Fig. 5.21.2(b) : Routing tables**

- The entries in router tables of Fig. 5.21.2(b) are the delay vectors. For example consider the shaded boxes of Fig. 5.21.2(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. 5.21.2(c) shows the two possible routes between I and G.



(G-466) **Fig. 5.21.2(c)**

- I knows that the reach G via A, the delay required is :

I to A Delay = 8mS
A to G Delay = 16mS
∴ I to G Delay = 8 + 16 = 24 msec (L-891)

- Whereas the delay between I and G via H (route IHG) is :

I to H Delay = 12mS
H to G Delay = 6mS
∴ I to G Delay = 12 + 6 = 18 msec (L-892)

- 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. 5.21.2(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 :

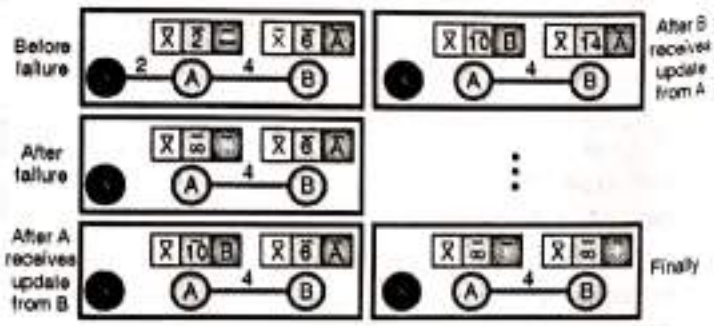
1. The distance vector routing takes a long time in converging to the correct answer. This is due to a problem called count-to-infinity problem. This problem can be solved by using the split horizon algorithm.
2. Another problem is that this algorithm does not take the line bandwidth into consideration when choosing a root. This is a serious problem due to which this algorithm was replaced by the Link State Routing algorithm.

Looping in distance vector routing protocol :

- A problem in distance vector rooting is its instability. A network using this protocol can become unstable.

Two node loop instability :

- A network with three nodes has been shown in Fig. 5.21.3. Note that the routing tables are shown partially for discussion.



(G-1499) **Fig. 5.21.3 : Two node loop instability**

Scanned by CamScanner

- At the beginning both nodes A and B know how to reach node X. But the link joining A and X fails suddenly. So node A changes its table. If A could send its changed routing table to B immediately, everything is okay. No problem will occur.
- But the system becomes unstable if B sends its routing table to A before receiving A's routing table.
- This is because node A receives the updated B's routing table and assumes that B has found a new path to reach node X. So A immediately updates its routing table (which is incorrect).
- Based on this update now A sends its new update to B. Now B thinks that something has changed around A and so it updates its routing table.
- Due to this process, the cost of reaching X increases gradually and finally becomes infinite. At this moment both A and B understand that now it is impossible to reach X.
- Note that during this entire time the system is unstable. A thinks that the route to X goes via B whereas B thinks that the route is via node A.
- So if A receives a packet for X, it goes to B and then again returns back to A. Similarly if B receives a packet destined for X, it goes to A and returns back to B.
- This bouncing of packets between nodes A and B is known as the **two-node loop problem.**
- This problem can be solved by using one of the following strategies :
  1. Defining infinity
  2. Split horizon
  3. Split horizon and poison reverse.
- There is a similar problem called three node loop problem present in the system using distance vector routing.

5.21.2 Count to Infinity Problem :

MU : Dec. 04, Dec. 09, May 10, May 11, May 15, May 17

University Questions

Q. 1 Explain count-to-infinity problem with the help of an example. It is a drawback of which algorithm. **(Dec. 04, 10 Marks)**

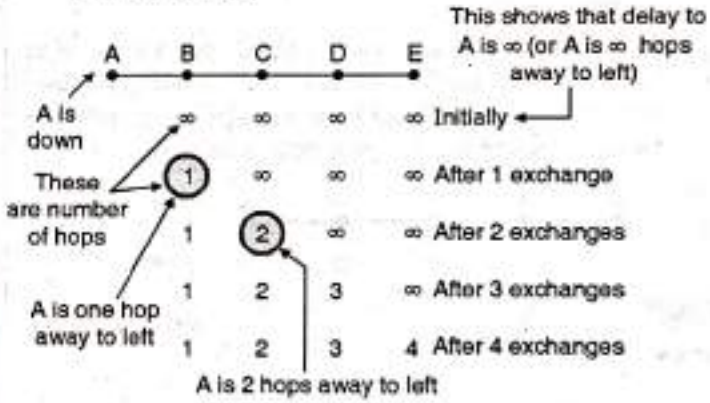
Q. 2 What is count to infinity problem in distance vector routing ? **(Dec. 09, May 10, 10 Marks)**

Q. 3 Explain distance vector routing and its count to infinity problem. **(May 11, 10 Marks)**

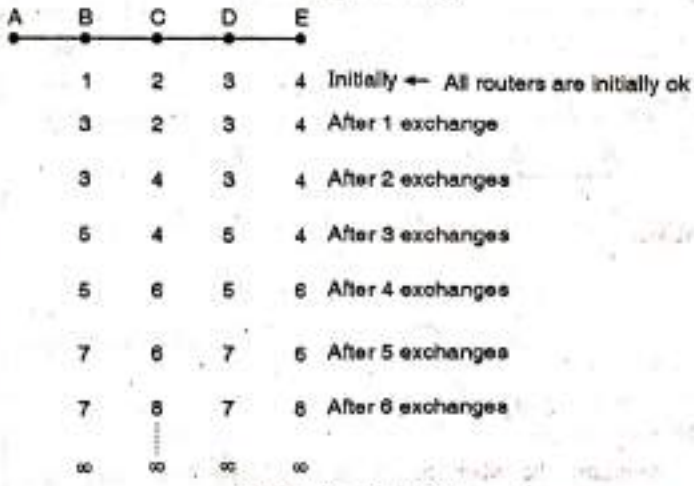
Q. 4 What is count to infinity problem in distance vector routing ? Discuss in detail. **(May 15, 10 Marks)**

Q. 5 Explain distance vector routing. What are its limitations and how are they overcome ? **(May 17, 10 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. 5.21.4 which has five nodes. The delay metric used is the number of hops.
- Assume that A is initially down and that all the other routers know this. So all the routers have recorded that the delay to A is infinity.
- When A becomes OK, the other routers come to know about it via the vector exchanges. Then suddenly a vector exchange at all the routers will take place simultaneously.
- At the time of first vector exchange, B comes to know that its left neighbour has a zero delay to A. So as shown in Fig. 5.21.4(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. 5.21.4(a), the entries below C D E are ∞.
- On the second vector exchange, C comes to know that B has a path of 1 hop length to A, so C updates its routing table and indicates a path of 2 hop length. But D and E do not change their table entries.



(G-467) **Fig. 5.21.4(a)**



(G-468) **Fig. 5.21.4(b)**

Scanned by CamScanner

- So after the second vector exchange the entries in the third row of Fig. 5.21.4(a) are :

(G-468(a))

A	B	C	D	E	
	1	2	∞	∞	After 2 exchanges

- 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. 5.21.4(b) :

- Now refer Fig. 5.21.4(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. 5.21.4(b) is as follows :

(G-468(b))

A	B	C	D	E	
	1	2	3	4	Initially ← First row of Fig. 5.21.4(b)

These are distances of B,C,D,E to A

- Now imagine that suddenly A goes down or line between A and B is cut.
- At the first packet exchange B does not hear anything from A (because A is down). But C says " I have a path of length 2 to A". But poor B does not understand that this path is through B itself.
- So B thinks that it can reach A via C with a path length 3. (B to C 1 hop and C to A 2 hops) so it accordingly updates its routing table. But D and E do not update their entries. So the second row of Fig. 5.21.4(b) looks as follows :

(G-469)

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. 5.21.4(b). It is repeated below.

(G-470)

A	B	C	D	E	
	1	2	3	4	
	3	2	3	4	
	3	4	3	4	After 2 exchanges

C changes its entry

- 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. 5.21.4(b) but after a very long time.
- The conclusion is bad news propagates slowly. This problem is called as **count-to-infinity** problem.
- The solution to this problem is to use the split horizon algorithm.

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.

5.21.3 Link State Routing :

MU : Dec. 13, May 16, Dec. 16

University Questions

Q. 1 What are the steps involved in link state routing. Explain the contents and the requirements of link state packets.

(Dec. 13, May 16, Dec. 16, 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 :

1. Each router should discover its neighbours and obtain their network addresses.
2. Then it should measure the delay or cost to each of these neighbours.
3. It should construct a packet containing the network addresses and the delays of all the neighbours.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

- The complete topology and all the delays are experimentally measured and this information is conveyed to each and every router.
- Then a shortest path algorithm such as Dijkshtra's algorithm can be used to find the shortest path to every other router.

Scanned by CamScanner

Protocols :

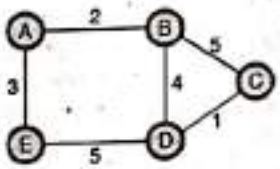
- Link state routing is popularly used in practice.
- The OSPF protocol which is used in the Internet uses the link state algorithm.
- IS-IS i.e. Intermediate system – Intermediate system is the other protocol which uses the link state algorithm.
- IS-IS is used in Internet backbones and in some digital cellular systems such as CDPD.

Building a routing table in link state routing :

Link state routing :

Now we will discuss the development of routing table in link state routing. Here the term **link state** is used for defining the characteristic of a link or edge, which represents a network in the Internet. The **cost** associated with each link is important. The links having lower costs are preferred to the links having higher costs. A nonexisting or broken link is indicated by an ∞ cost. In this method, each node must have a complete map of the network. That means each node should have complete information about the state of each link.

The collection of states of all the links in an Internet is called as **Link-State Database (LSDB).** For the entire Internet, there is only one LSDB and its copy is available with each node. Each node uses it to create the least cost tree. The example of LSDB is as shown in Fig. 5.21.5(b) for the Internet shown in Fig. 5.21.5(a). The next step is creation of LSDB (which contains all the information about the Internet) at each node.



(a) Internetwork

	A	B	C	D	E
A	0	2	∞	∞	3
B	2	0	5	4	∞
C	∞	5	0	1	∞
D	∞	4	1	0	5
E	3	∞	∞	5	0

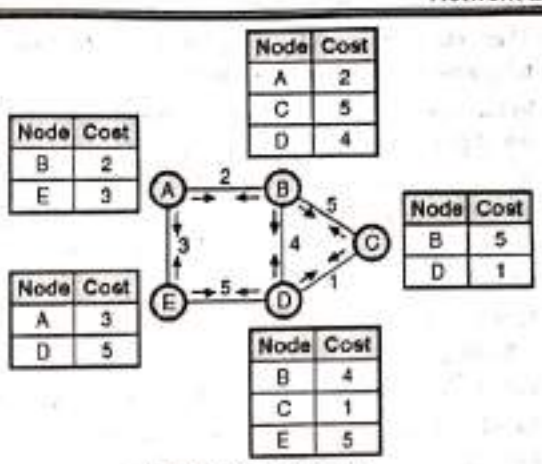
(b) Link state database (LSDB)

(G-2201) Fig. 5.21.5

This can be achieved by a process called **flooding.** Each node sends a greeting message to all its immediate neighbours, so as to collect two important pieces of information as follows :

1. The identity of the neighbouring node.
2. Cost of the link.

The packet containing this information is called as **LS Packet** (LSP), which is sent out of each interface. After receiving all the new LSPs each node will create the comprehensive LSDB as shown in Fig. 5.21.5(c). This LSDB is same for each node which shows the whole map of the Internet. That means a node can use the LSDB to make the whole map of the Internet.



(G-2202) Fig. 5.21.5(c)

5.21.4 Comparison of Link State Routing and Distance Vector Routing :

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.

5.21.5 Hierarchical Routing :

MU : Dec. 13, Dec. 15

University Questions

Q. 1 What are the advantages and disadvantages of hierarchical routing ? **(Dec. 13, 5 Marks)**

Q. 2 What are the different types of routing algorithms ? When would we prefer to use hierarchical routing over link state routing ? **(Dec. 15, 10 Marks)**

- As the size of the network increases, the size of the routing tables of the routers also increases.
- As a result of large routing tables, the router memory is consumed to a great extent, more CPU time is needed to scan the tables and more bandwidth is required to send status report about the tables.
- Sometimes the network becomes so large that the size of the router table becomes excessively large and practically it becomes impossible for every router to have an entry for all the other routers except itself.

Scanned by CamScanner

- 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

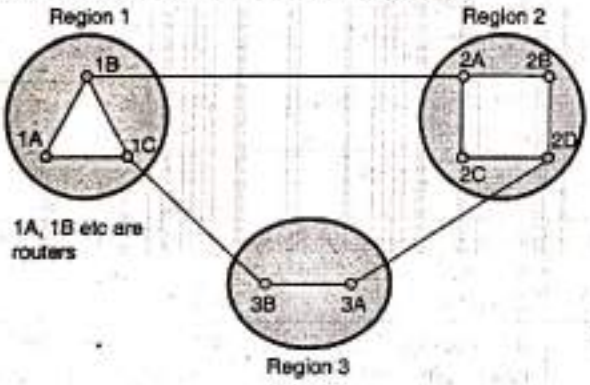
  Level 2 : Clusters : It is a group of regions.

  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. 5.21.6(a) shows network containing 3 regions. Fig. 5.21.6(b) shows the full routing table of router 1A which has 9 entries because in all there are 9 routers.



(G-471) **Fig. 5.21.6(a) : A network**

Full routing table for 1A

Destination	Line	Hops
1 A	–	–
1 B	1 B	1
1 C	1 C	1
2 A	1 B	2
2 B	1 B	3
2 C	1 B	3
2 D	1 B	4
3 A	1 C	3
3 B	1 C	2

(G-2304) **Fig. 5.21.6(b) : Full routing table for router 1A**

- Now with a two level hierarchical routing, the routing table of the same router reduces to a much smaller size as shown in Fig. 5.21.6(c). This table has only 5 entries.

Hierarchical routing table for 1A

Destination	Line	Hops
Region 1 { 1 A	–	–
1 B	1 B	1
1 C	1 C	1
Region 2 → 2	1 B	2
Region 3 → 3	1 C	2

(c) Hierarchical routing table for router 1A

(G-2305) **Fig. 5.21.6**

- In the hierarchical table of Fig. 5.21.6(c), there are entries for all local routers (1 A, 1 B and 1 C) belonging to the region of 1 A as before. But there are no detailed entries for the other regions.
- Instead all other regions have been compressed into a single router per region. For example traffic from 1A to any router in region-2 is via 1 B-2 A line as shown by the shaded entry in Fig. 5.21.6(c). Similarly all the traffic from 1A to region 3 is routed through the line 1C-3B.
- Comparison of Figs. 5.21.6(b) and (c) shows how hierarchical routing reduces the size of routing tables.

Disadvantage : The reduced table size has a price tag attached to it. It comes at the expense of increased path length. But it is practically acceptable.

How many levels a hierarchy should have ?

Kamoun and Kleinrock have discovered that for an N router subnet, the optimum number of hierarchy levels is $\log_e N$ and it requires a total of $\log_e N$ entries per router table.

Ex. 5.21.1 : 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.

Level 3 : Clusters
|
Level 2 : Regions
|
Level 1 : Routers

- If the number of clusters is x, number of regions per cluster is y, and the number of routers in each region is z then the each router needs z entries for the local routers, (y – 1) entries for routing to other regions within its own cluster and (x – 1) entries for distant clusters.

∴ Total number of entries in the router table

$= (x - 1) + (y - 1) + z = x + y + z - 2$

Scanned by CamScanner

- 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,

$$x \times y \times z = 10 \times 20 \times 24 = 4800$$

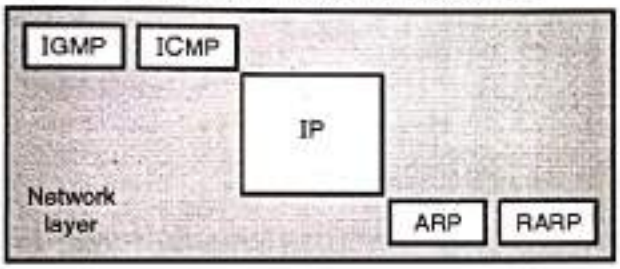
- For this arrangement the number of entries in a router table would be,

$$\text{Entries} = x + y + z - 2 = 10 + 20 + 24 - 2 = 52$$

- It is possible to find the values of x, y and z be trial and error to minimize the number of entries.

5.22 Network Layer Protocols :

- 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. 5.22.1.



(G-524) **Fig. 5.22.1 : Protocols at network layer**

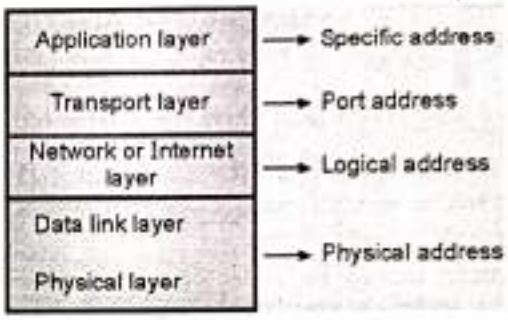
- Out of these protocols IP is the most important protocol. It is responsible for host to host delivery of datagrams from a source to destination. But IP needs to take services of other protocols.
- IP takes help from ARP in order to find the MAC (physical) address of the next hop.
- IP uses the services of ICMP during the delivery of the datagram packets to handle unusual situations such as presence of an error.
- IP is basically designed for unicast delivery. But some new Internet applications as well as multimedia need multicast delivery.
- So for multicasting, IP has to use the services of another protocol called IGMP.
- IPv4 is the current version of IP whereas IPv6 is the latest version of IP.

5.23 Addressing :

- When the computers wish to communicate with one another, they need to know the address of each other. Each computer has its own address.
- The addresses can be of different types such as physical addresses or logical address.
- In an internet employing the TCP/IP protocols, four levels of addresses are used by the computers.
  1. Physical address
  2. Logical address (IP)
  3. Port address and
  4. Specific address
- Fig. 5.23.1 shows the classification of addresses.

(G-75) **Fig. 5.23.1 : Classification of addresses in TCP/IP**

- Each of these addresses is associated with a specific layer of TCP/IP architecture as demonstrated in Fig. 5.23.2.



(G-76) **Fig. 5.23.2 : Relation between TCP/IP structure and addresses**

5.23.1 MAC Address (Physical Address) :

MU : May 08, May 09, Dec. 15

University Questions

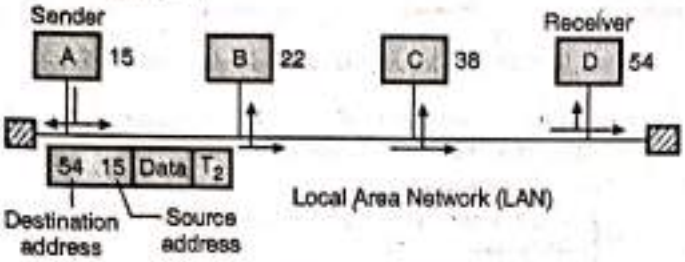
Q. 1 Explain with example MAC address. **(May 08, May 09, 10 Marks)**

Q. 2 Differentiate between an IP address and a MAC or physical address. What is the need to map IP address to MAC address ? Explain which protocol does this similarly give a protocol which does reverse mapping. **(Dec. 15, 5 Marks)**

- The packets from source to destination hosts pass through physical networks. At the physical level the IP address is not useful but the hosts and routers are recognized by their MAC addresses.
- A MAC address is a local address. It is unique locally but it is not unique universally.
- The IP and MAC address are two different identifiers and both of them are needed, because a physical network can have two different protocols at the network layer at the same time.
- Similarly a packet may pass through different physical networks.
- So to deliver a packet to a host or a router, we require two levels of addressing namely IP addressing and MAC addressing.
- Most importantly we should be able to map the IP address into a corresponding MAC address.
- The size and format of the physical address varies depending on the nature of network.

Scanned by CamScanner

- The Ethernet (LAN) uses a 48-bit (6-byte) physical address which is imprinted on the network interfacing card (NIC).
- Refer Fig. 5.23.3 which explains the concept of physical addressing.



(G-77) **Fig. 5.23.3 : Physical addresses**

- The sender computer with a physical address of 15 wants to communicate with the receiver computer with a physical address 54.
- The frame sent by the sender consists of the destination address, sender's address, encapsulated data and a trailer (T_2) that contains the error control bit.
- When this frame travels over the bus topology, every computer receives it and tries to match it with its own physical address.
- If the destination address in the frame header does not match with the physical address it will simply drop the frame.
- At receiver computer (D), the destination address matches with its physical address (54). So the frame is accepted and decapsulation is carried out to recover the data.
- The example of a 48 bit or 6 byte physical address is as follows. It contains 12-hexadecimal digits.

08 : 63 : 4C : 81 : 08 : 1D

5.23.2 Logical Addresses (IP Addresses) :

MU : Dec. 15

University Questions

Q. 1 Differentiate between an IP address and a MAC or physical address. What is the need to map IP address to MAC address ? Explain which protocol does this similarly give a protocol which does reverse mapping. **(Dec. 15, 5 Marks)**

- Logical addresses are required to facilitate universal communications in which different types of physical networks can be involved.
- The logical address is also called as the IP (Internet Profocol) address.
- The internet consists of many physical networks interconnected via devices like routers.
- Internet is a packed switched network that means the data form 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.

5.23.3 Port Address :

- The modern computers are designed to run multiple processes on it simultaneously.
- The main objective of internet is the process to process communication. For this purpose it is necessary to lable or name the processes.
- Thus the processes need addresses. The lable assigned to a process is called as a port address. It is a 16 bit address.

5.23.4 Specific Addresses :

- Some applications have user friendly addresses. The examples of specific addresses are the e-mail addresses or the University Resource Locators (URL).

5.23.5 Address Mapping :

MU : Dec. 15

University Questions

Q. 1 Differentiate between an IP address and a MAC or physical address. What is the need to map IP address to MAC address ? Explain which protocol does this similarly give a protocol which does reverse mapping. **(Dec. 15, 5 Marks)**

- 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.

Scanned by CamScanner

- 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.

5.23.6 Mapping of IP Address to a MAC Address (ARP) :

MU : Dec. 04, Dec. 09, Dec. 15

University Questions

Q. 1 ARP and RARP both map addresses from one space to another. In this respect they are similar. In what major way do they differ ? **(Dec. 04, 4 Marks)**

Q. 2 What is Address Resolution Protocol (ARP) ? **(Dec. 09, 5 Marks)**

Q. 3 Differentiate between an IP address and a MAC or physical address. What is the need to map IP address to MAC address ? Explain which protocol does this similarly give a protocol which does reverse mapping. **(Dec. 15, 5 Marks)**

- We have seen the need of mapping an IP address into a MAC address.
- Such a mapping can be of two types :
  1. Static mapping and 2. 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 :
  1. Address Resolution Protocol (ARP).
  2. 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.

5.24 Address Resolution Protocol (ARP) : New Syll. : MU : Dec. 18

- The IP protocol is supposed to deliver a packet from the source host to destination host via different routers over the Internet.
- The first step in this entire process is that the IP protocol should know how to deliver the packet to the next hop (router).
- In order to do this, the IP packet should refer to its routing table to find the IP address of the next hop.
- However, IP is using the services of the data link layer. Therefore IP must know the physical address of the next hop (knowing only its IP address won't be enough).
- Thus the IP address of the next hop must be converted (or mapped) into its physical address. This mapping can be done using the protocol called address resolution protocol or ARP which we are going to discuss in this section.

5.24.1 Address Mapping :

- 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 (Logical address) :

- An IP address is an internetwork address. It is a universally unique address.
- Every protocol involved in internetworking requires IP addresses.
- An IP address is basically a logical address. It is known as a logical address because it is implemented in software.
- The logical addresses in TCP / IP suite are the IP addresses and as discussed earlier, they are 32 bit long.

MAC address (Physical 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.

Scanned by CamScanner

- 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.
- We have seen the need of mapping an IP address into a MAC address.
- Such a mapping can be of two types :
  1. Static mapping 2. 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.
- The physical address of a machine can change due to the following reasons :
  1. The physical address can change if a machine changes its NIC (Network Interfacing Card).
  2. In certain types of LANs, a machine's physical address changes everytime it is turned on.
  3. The physical address of a mobile computer will change when it moves from one network to the other.

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 :
  1. Address Resolution Protocol (ARP).
  2. 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.

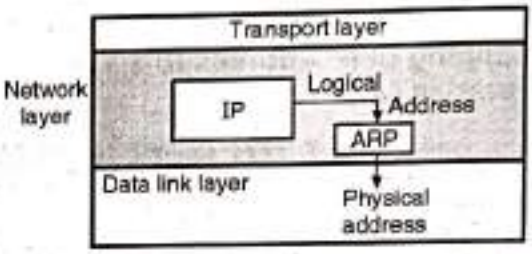
5.24.2 The ARP Protocol : MU : May 04, May 15

University Questions

Q. 1 Describe address resolution protocol what are the difficulties for having a mobile IP ? What can be the solution. **(May 04, 10 Marks)**

Q. 2 Write short note on Address Resolution Protocol (ARP). **(May 15, 5 Marks)**

- If a host or a router wants to send an IP datagram to another host or router, it has the IP address of the receiving host or router.
- But this IP datagram is going to be encapsulated in a frame (data link layer) so as to make it capable of passing through the physical network.
- For this the sender must know the physical address of the receiver.
- The position of ARP in the TCP/IP suite has been shown in Fig. 5.24.1. It shows that IP sends the logical address to ARP which maps the logical address into its corresponding physical address and passes it to the data link layer.



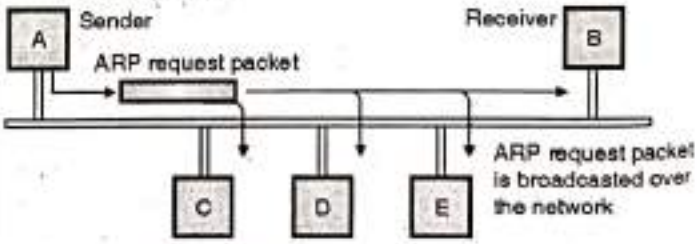
(G-2093) **Fig. 5.24.1 : Position of ARP in TCP / IP suite and its principle of operation**

- 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 :

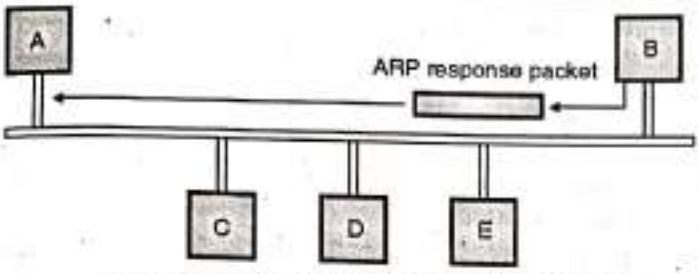
1. The router or host A who wants to find the MAC address of some other router, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender A and the IP address of the receiver (B).
2. This request packet is broadcasted over the network as shown in Fig. 5.24.2(a).



(G-575)**Fig. 5.24.2(a) : ARP request is broadcast**

3. 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.
4. 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. 5.24.2(b). Thus host A has obtained the MAC address of B using ARP.

Scanned by CamScanner



(G-576) **Fig. 5.24.2(b) : ARP response unicast**

5.24.3 ARP Cache Memory :

- 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.

5.24.4 ARP Packet Format :

The ARP message format is as shown in Fig. 5.24.3. The various fields in it are as follows :

1. **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.
2. **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.
3. **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.

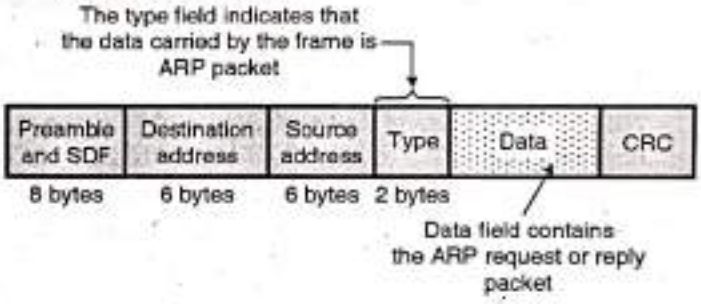
Hardware type (16 bits)		Protocol type (16 bits)
Hardware length	Protocol length	Operation request 1, Reply 2
Sender hardware address		
Sender protocol address		
Target hardware address		
Target protocol address		

(G-577) **Fig. 5.24.3 : ARP message format**

4. **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.
5. **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).
6. **SHA (Sender Hardware Address) :** This field is used for defining the physical address of the sender. The length of this field is variable.
7. **SPA (Sender Protocol Address) :** This field defines the logical address of the sender. The length of this field is variable.
8. **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 receivers physical address is not known to the sender.
9. **TPA (Target Protocol Address) :** This field defines the logical address of the target. It is a variable length field.

5.24.5 Encapsulation :

- An ARP packet (request or reply) is inserted directly into the data link frame. Such an insertion is known as encapsulation.
- Fig. 5.24.4 shows an example of encapsulation in which an ARP packet being encapsulated in an Ethernet frame. The type field shows that the data carried by the frame is an ARP request or reply packet.



(G-578) **Fig. 5.24.4 : Encapsulation of ARP packet**

5.24.6 Operation of ARP on Internet :

Working conditions :

- 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. The seven steps involved are as follows :

Steps :

1. The sender (host or router) knows the IP address of the destination.

Scanned by CamScanner

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. Therefore a 0 is filled in the target physical address field.
3. The ARP request packet is sent to the data link layer. Here the message is encapsulated into a DLL frame alongwith the sender's physical address as source address and the physical broadcast address as destination address.
4. Every router or host receives this DLL frame because it is a broadcast. All the machines except the target will drop the packet. Only the target machine will recognize the IP address.
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.

5.24.7 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.

5.24.8 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.

5.25 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.

5.25.1 The Reverse Address Resolution (RARP) Protocol :

MU : Dec. 04, Dec. 16, New Syll. : Dec. 18

University Questions

Q. 1 ARP and RARP both map addresses from one space to another. In this respect they are similar. In what major way do they differ ? **(Dec. 04, 4 Marks)**

Q. 2 Write short notes on : RARP **(Dec. 16, 5 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.

Scanned by CamScanner

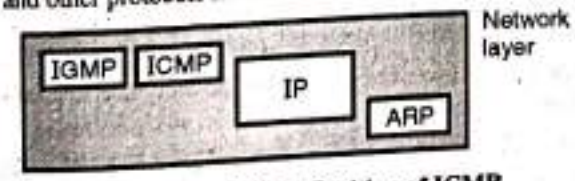
- The disadvantage of RARP is that it uses a destination address of all 1s (limited broadcasting) to reach the RARP server.
- But such broadcasts are not forwarded by routers, so a RARP server is needed on each network.
- In order to get around this problem, another bootstrap protocol called BOOTP has 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.

5.26 ICMPv4 (Internet Control Message Protocol) : MU : Dec. 16, New Syll. : Dec. 18

University Questions

Q. 1 What is ICMP protocol ? Explain the ICMP header format with diagram. **(Dec. 16, 10 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).
- Fig. 5.26.1 shows the position of ICMP with respect to the IP and other protocols in the network layer.

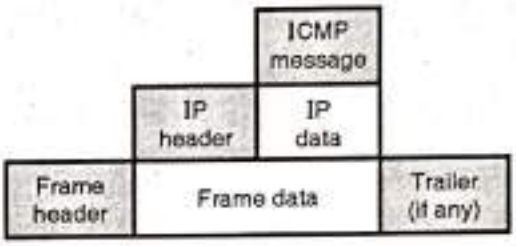


(G-2102) **Fig. 5.26.1 : Position of ICMP**

- There are two versions of ICMP protocol namely ICMPv4 and ICMPv6. In the following sections, we are going to discuss ICMPv4.

5.26.1 ICMP Encapsulation :

- 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. 5.26.2.



(G-2103) **Fig. 5.26.2 : 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 :

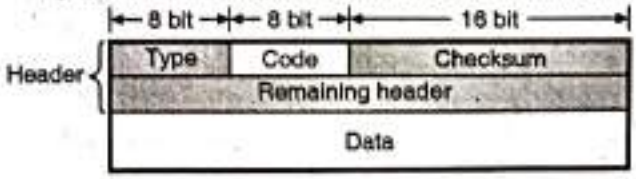
  ping 100.50.25.1
- When the destination receives the echo request message, it responds by sending an ICMP echo reply message. If a reply is not returned within a set time, ping resends the echo request several more times. If no reply arrives, ping indicates that the destination is unreachable.
- Another utility that uses ICMP is trace route, which provides a list of all the routers along the path to a specified destination.

5.26.2 ICMP Messages :

- ICMP messages are of two types :
  1. Error reporting messages
  2. Query messages.
- If a host or a router encounters a problem after processing an IP problem, then it uses the **error reporting messages** for reporting the problem.
- A host or a network manager can use the **query messages** to get some specific information from a router or another host.

5.26.3 Message Format : New Syll. : MU : Dec. 18

- Fig. 5.26.3 shows the general format of ICMP messages.



(G-2105) **Fig. 5.26.3 : General format of ICMP messages**

- As shown in Fig. 5.26.3, the header of an ICMP message is 8-byte long and the data section is of a variable size.

Scanned by CamScanner

- The general header format for each ICMP message is different. But the first four bytes are common to all the message types.

1. **Type :**

   This 8-bit field is used for defining the types of message.

2. **Code :**

   This 8-bit field is used for specifying the reason for the particular message type.

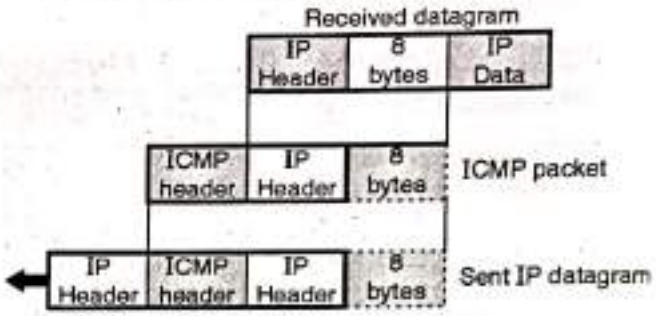
- The last common field is the **checksum** field which is 16 bit (2 byte) long. We will discuss it later in this chapter.
- The information to find the original packet that had error is included in the **data section** of the error messages.
- Whereas the **data section** in the query messages contains extra information depending on the type of query.

5.27 Error Reporting Messages (ICMPv4) :

- 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. 5.27.1 shows different types of error reporting messages.

(G-2104) **Fig. 5.27.1 : Error reporting messages**

- ICMP makes use of the source IP address for sending the error message back to original source of erroneous datagram.
- Some of the important points about ICMP error messages are as follows :
  1. If a datagram containing and ICMP error message is received, then no ICMP error message will be generated in response to it.
  2. An ICMP error message will not be generated for a fragmented datagram that is not the first fragment.
  3. Any ICMP error message will not be generated for a datagram which has a multicast address.
  4. An ICMP error message will not be generated for a datagram which has a special address such as 127.0.0.0 or 0.0.0.0
- It is important to note that the data section of every error message, contains the IP address of the original datagram in addition to the 8 bytes of data in that datagram.
- The header of the original datagram is included in the error message, to ensure that the error message will reach the original source.
- The additional 8 byte data is included because in TCP and UDP, the first 8 bytes of information contains information about the port numbers for TCP and UDP and sequence number for TCP.
- The source can use this information and convey to TCP and UDP protocols that an error has occurred.
- Then the **error packet,** formed by ICMP, is encapsulated in an IP datagram as shown in Fig. 5.27.2.



(G-2106) **Fig. 5.27.2 : Data field contents for the error message**

- Now let us discuss the ICMP error messages one by one.

5.27.1 Destination Unreachable :

- When it is not possible for a router to route the datagram or when a host is unable to deliver a datagram, then the datagram is **discarded** and the **destination unreachable** error message is sent back by the respective host or router to the source host which originated the datagram.
- The format of the destination unreachable error message is as shown in Fig. 5.27.3.

8 bits	8 bits	16 bits
Type : 3	Code : 0 to 15	Checksum
Unused (All 0's)		
Data section : Contains a part of received IP datagram including IP header + 8 byte datagram data		

(G-2107) **Fig. 5.27.3 : Destination unreachable format**

- The code field for the destination unreachable error message has 16 different values (0 to 15) and each one specifies a reason for discarding a datagram.

1. **Code 0 :** This code specifies the reason for discarding the datagram as : network is not reachable, possibly due to hardware failure.
2. **Code 1 :** The host is not reachable, possibly due to hardware failure.
3. **Code 2 :** It is not possible to reach the **protocol.** This code is used when a higher level protocol such as TCP, UDP, OSPF is not running at the destination host.
4. **Code 3 :** It is not possible to reach the **port.** This code is used when the application program (process) to which the datagram is to be finally delivered is not running at the moment.

Scanned by CamScanner

5. **Code 4 :** The error message with code 4 is produced in the following situation : Fragmentation is required to be done but the do not fragment (DF) field of the datagram has been set by the sender of the datagram which says that fragmentation should not be done. But unless fragmentation is done, the routing of the datagram is not possible.
6. **Code 5 :** It is not possible to accomplish the source routing, i.e. it is not possible for the datagram to visit one or more routers that are specified in the routing options.
7. **Code 6 :** The destination network is not known, (we are not saying it is unreachable). Here the router does not have any information about the destination network.
8. **Code 7 :** The destination host is not known, (again we are not saying that the destination host is unreachable as is the case for code 1). For code 7, the router does not have any information about the destination host.
9. **Code 8 :** The source host has been isolated.
10. **Code 9 :** The communication with the destination network has been prohibited by the administration.
11. **Code 10 :** The communication with destination host is prohibited by the administrator.
12. **Code 11 :** It is not possible to reach the network for a particular type of service. Here it is not possible for the router to route the datagram because the source is asking for an unspecified type service.
13. **Code 12 :** It is not possible to reach the host for a particular type of service.
14. **Code 13 :** It is not possible to reach the host because a filter has been installed by the administrator.
15. **Code 14 :** The host is not reachable because the host precedence has been violated.
16. **Code 15 :** It is not possible to reach the host because its precedence is cut off. This message is generated when the datagram is sent with a precedence below a level of precedence set by the network operator, for the operation of the network.

Notes :

1. The destination host or routers can produce the destination unreachable message.
2. Only the destination host can create code 2 and code 3 messages.
3. The messages of other codes except codes 2 and 3 can be created only by the routers.
4. The noncreation of destination unreachable message does not guarantee the delivery of datagram.
5. It is not possible for the router to detect all the problems that prevent the packet delivery.

5.27.2 Source Quench Error 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 :
  1. It tells the source that the packet has been discarded and,
  2. It gives a warning to the source that the source should slow down (quench) because congestion has taken place somewhere.
- Fig. 5.27.4 shows the format of the source quench error message.

8 bits	8 bits	16 bits
Type : 4	Code : 0	Checksum
Unused (All zeros)		
Data : Part of the received IP datagram including IP header + the first 8 bytes of datagram data		

(G-2108) **Fig. 5.27.4 : Source quench format**

- A source - quench message, one per discarded datagram due to congestion is sent back by a router or destination host, to the source host.
- But, the **congestion relieved** message cannot be sent to the source host as no such mechanism exists.
- As no such message could be sent back, the source host assumes that the congestion has continued to exist, and therefore it continues to reduce the rate of data transmission, until no more source-quench messages are received.
- The congestion can happen due to two types of communications :
  1. Due to one to one communication or
  2. Due to many to one communication.
- In the one to one communication, a single source host will be responsible for congestion because of its high data transmission rate. The source quench message will be useful under such operating conditions, for reducing the transmission rate of the source host and clear the congestion.
- But this message will not prove to be successful if congestion occurs in the many to one type communication. This is because the router or destination host does not know which source is fast and responsible for the congestion.
- As a result, it may discard the packets received from the slowest source instead of dropping them from a fast source which is actually responsible for congestion.

5.27.3 Time Exceeded Error Message :

- This message is generated in two cases :
  1. 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.
  2. 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.

Scanned by CamScanner

- The format of the time exceeded message is as shown in Fig. 5.27.5.

8 bits	8 bits	16 bits
Type : 11	Code : 0 or 1	Checksum
Unused (All zeros)		
Data : Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

(G-2109) **Fig. 5.27.5 : Message format of time exceeded error message**

- Refer the **code field.** Its value can be either 0 or 1. If **code = 0,** then the router will discard the datagram because the value of TTL (time to live) field is zero.
- If **code = 1,** then destination host discards the fragments of datagram because some fragments could not arrive at the destination host within the time limit.

5.27.4 Parameter Problem Error Message :

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.
- This message can be created either by a router or the destination host.
- The message format of the parameter problem error message is as shown in Fig. 5.27.6. Refer to the **code field** which has two possible values, 0 and 1. This field, depending on its value will specify the reason for discarding the datagram as follows :

1. **Code = 0 :** If code = 0, then the datagram is discarded because of an error or ambiguity present in one of the header fields. The erroneous byte is pointed at by the value of the pointer field. For example if pointer field = 0, then the first byte is an invalid field.
2. **Code = 1 :** If code =1, then the datagram is discarded because required part of an option is missing.

- The format of the parameter problem is as shown in Fig. 5.27.6.

8 bits	8 bits	16 bits
Type : 12	Code : 0 or 1	Checksum
Pointer	Unused (All zeros)	
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

(G-2110) **Fig. 5.27.6 : Format of parameter problem error message**

5.27.5 Redirection Error 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.
- In order to ensure higher efficiency, the hosts do not participate in the process of routing table update. This is because the number of hosts in the Internet is much higher than the number of routers.
- If the routing tables of hosts are updated dynamically then it creates an unwanted traffic.
- Generally the static routing is used by the hosts. That means the routing table of a host contains limited number of entries. Generally a host knows the IP address of only one router that is the default router.
- Due to this, a host can send a datagram which is destined for another network, to a wrong router.
- Here the datagram receiving router will route the datagram the correct router. However it sends a redirection message to the host to update the routing table of the host.
- Fig. 5.27.7 shows the format of the redirection error message.

8 bits	8 bits	16 bits
Type : 5	Code : 0 to 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

(G-2111) **Fig. 5.27.7 : Format of the redirection message**

- As shown in Fig. 5.27.7, the second row of the redirection message contains the IP address of the appropriate target router.
- It is important to understand that the redirection message is different from the other error message eventhough it is considered as an error reporting message.
- What is the difference ? In this case the router does not discard the erroneous datagram. Instead it is sent to the appropriate router.
- This process of redirection is narrowed down by the contents of the **code field** as follows :

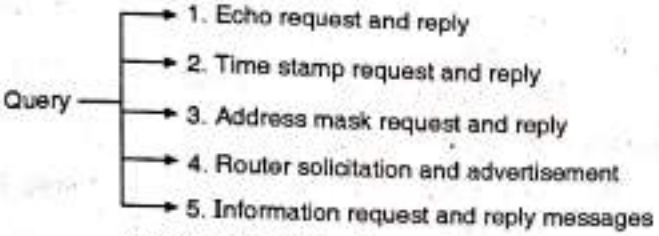
1. **Code = 0 :** Redirection will be for a network specific route.
2. **Code = 1 :** Redirection is to be done for a host specific route.
3. **Code = 2 :** Redirection is to be done for a network specific route and based upon a specific type of service.
4. **Code = 3 :** Redirection is to be done for a host specific route on the basis of a specified type of service.

Note : A router sends the redirection message back to a host on the same local network.

Scanned by CamScanner

5.28 Query Messages (ICMPv4) :

- 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 five different pairs of messages as shown in Fig. 5.28.1.



(G-2112) **Fig. 5.28.1 : Query messages**

- However out of these five pairs of messages, only two pairs are being used today. They are :
  1. Echo request and reply.
  2. Timestamp request and reply.
- Let us discuss them one by one.

5.28.1 Echo Request and Reply :

- This pair of query messages has been designed for the diagnostic purpose. This pair of messages is utilized by the network managers and users for identifying the network problems.
- This pair of query messages would determine whether the two given systems (either hosts or routers) can communicate with each other or not.
- The communication will take place as follows :
  1. A host or router sends the **echo-request** message to another host or router it wants to communicate to.
  2. The host or router which receives the echo request message will create an **echo-reply** message and sends it back to the original sender.
- We can also use the echo-request echo-reply pair to determine if the IP level communication is present or not.
- The network managers can use the echo request and echo reply pair of messages to check the operation of IP protocol.
- A host can also use this message pair to see if another host is reachable or not. At the users level, this is done by invoking the **packet Internet groper** command (ping).
- Now a days a version of ping command is provided by most systems which can create a string of echo-request and echo-reply messages for providing statistical information.
- It is also possible to check whether a node is functioning properly or not with the help of the echo-request echo reply pair of messages. The format of the echo request echo reply pair of messages is as shown in Fig. 5.28.2.

	8 bits	8 bits	16 bits
Type 8 : Echo request Type 0 : Echo reply	Type : 8 or 0	Code : 0	Checksum
	Identifier		Sequence number
	Optional data : Sent by the request message, repeated by the reply message		

(G-2113) **Fig. 5.28.2 : Echo request and echo reply messages**

- In Fig. 5.28.2, the protocol does not formally define the identifier and sequence number fields. Therefore the sender can use them in an arbitrary manner.

5.28.2 Timestamp 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).
- Fig. 5.28.3 shows the format of these two messages.

	8 bits	8 bits	16 bits
Type 13 : Request Type 14 : Reply	Type : 13 or 14	Code : 0	Checksum
	Identifier		Sequence number
	Original timestamp		
	Receive timestamp		
	Transmit timestamp		

(G-2114) **Fig. 5.28.3 : Format of timestamp request and timestamp reply messages**

- As shown in Fig. 5.28.3, there are three timestamp fields and each field is 32-bit long. The number in each of these fields represents time in milliseconds from the midnight in Universal time.
- Eventhough, the 32 bit field can represent a number between 0 and 4,294,967,295 but a timestamp in this case can have the maximum value of $86,400,000 = 24 \times 60 \times 60 \times 1000$.
- The **timestamp request** message is created by the source. It fills the original timestamp field at departure time, and fills the other two timestamp fields will zeros.
- The **timestamp** reply message is created by the destination host. The original timestamp value from the timestamp request message is copied as it is into the original timestamp field in the timestamp reply message, by the destination.
- The destination then fills up the **receive timestamp** field by the time at which the request was received.
- At the end the destination fills up the **transmit timestamp** field with the **departure time of the reply** message.

Computation of one way or round trip time (RTT) :

- We can use the pair of timestamp messages to compute the one way or RTT i.e. the time required by the datagram to travel from source to destination and then come back to source again, as follows :

  Sending time = receive timestamp - original timestamp.

  Receiving time = returned time – transmit timestamp.

Scanned by CamScanner

Rount trip time = sending time + receiving time.

- If we want the calculations of the sending time and receiving time to be accurate, then the two clocks in the source and destination computers should be synchronized.
- But the calculation of RTT will be correct even if the clocks at the source and destination machines are not synchronized.
- We can calculate the one way time duration by dividing the RTT by two.

5.28.3 Deprecated Messages :

IETF has declared the following three pairs of query messages as obsolete :

1. Information request and reply messages.
2. Address mask request and reply messages.
3. Router solicitation and advertisement.

1. The information request and reply messages :

- These messages are not used now a days because the Address Resolution Protocol (ARP) is doing their duties.

2. 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.
- These messages are not being used today because their duties are done by the Dynamic Host Configuration Protocol (DHCP).

3. 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.
- These messages are not being used today because their duties are done by the DHCP.

5.28.4 Checksum :

Earlier we have discussed the concept of checksum. In ICMP, the entire message (including the header and data) is considered for calculation of checksum.

Checksum calculation :

- The checksum calculation is done at the sending end by following the steps given below :
  1. Set the checksum field to zero.
  2. Calculate the sum of all the 16 bit words including header and data.
  3. Obtain the checksum by complementing the sum calculated in step 2.
  4. Store the checksum in the checksum field.

Checksum testing :

- The following steps are followed by the receiver using 1's complement arithmetic :
  1. Calculate the sum of all words (header and data).
  2. Complement the sum calculated in step 1.
  3. Accept the message if the result obtained in step 2 is 16 zeros. Otherwise the message is rejected.

5.29 IGMP (Internet Group Management Protocol) :

- IGMP is a necessary but not sufficient protocols used in multicasting environment. It is always used along with IP.

Group management :

- In the multicasting environment we need to use the multicast packets. So in an Internet we have to use the routers which can route multicast packets.
- A multicast routing protocol should be used to update the routing tables of these routers.
- But note that IGMP is not a multicasting routing protocol. Instead its job is to manage the group membership.
- It helps the multicast routers to create and update a list of loyal members related to each router interface.

5.29.1 Messages :

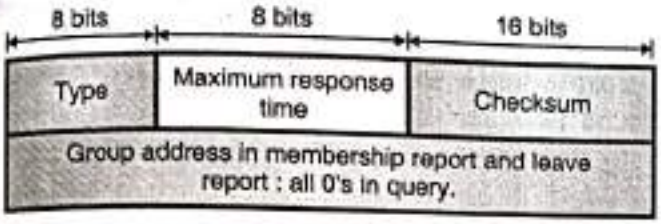
- There are two versions of IGMP called IGMPv1 and IGMPv2. In the second version there are three types of messages.
- The IGMP messages are shown in Fig. 5.29.1.
- Fig. 5.29.1 shows that there are three types namely query message, membership report and leave report. The query message has been divided into two types namely general and special types.

(G-586) **Fig. 5.29.1 : IGMP message types**

Scanned by CamScanner

Message format :

- The IGMP (version-2) message format is shown in Fig. 5.29.2.



(G-587) **Fig. 5.29.2 : IGMP message format**

1. Type :

- It is an 8 bit field that defines the type of message as given in Table 5.29.1. The type and its value in hexadecimal and binary notation have also been shown in Table 5.29.1.

Table 5.29.1 : IGMP type field

Type	Value
General or special query	0x11 or 0001 0001
Membership report	0x16 or 0001 0110
Leave report	0x17 or 0001 0111

2. Maximum response time :

- This is the next 8-bit field which defines the amount of time allowed to answer a query.
- The value in this field shows the maximum response time in tenths of seconds.
- This value is a non zero number if the message is a query message and it is equal to zero for the other two message types.

3. IGMP checksum :

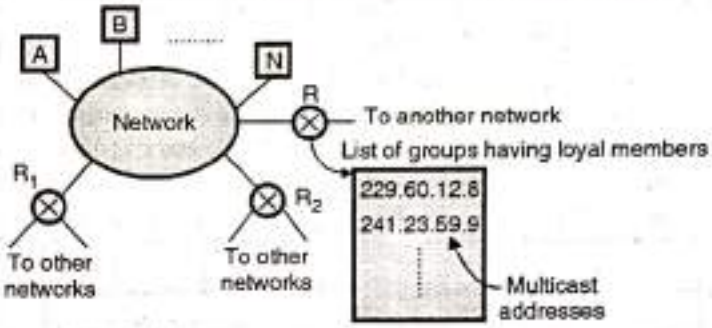
- The checksum is the 16-bit one's complement of the one's complement sum of the 8-byte IGMP message. When the checksum is computed, the checksum field should first be cleared to 0.
- When the data packet is transmitted, the checksum is computed and inserted into this field.
- When the data packet is received, the checksum is again computed and verified against the checksum field. If the two checksums do not match then an error has occurred.

4. Group address :

- This is a 32-bit field and its value depends on the type of message. For example the value of this field is zero for a general query message.
- The value in this field defines the multicast address of the group called **groupid**, in the other three types of messages.

5.29.2 Operation of IGMP :

- Refer Fig. 5.29.3 to understand the IGMP operation.
- IGMP operates locally. As shown in Fig. 5.29.3 multicast router R has a list of multicast addresses of the groups for which the router distributes packets. These packets are distributed to groups with at least one loyal member in that network.
- There is one router per group. Its duty is to distribute the multicast packets which are supposed to reach that group.

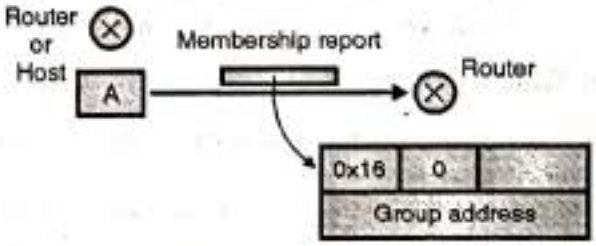


(G-588) **Fig. 5.29.3 : IGMP operation**

- So if there are three multicast routers (R_1, R_2 and R) connected to the network, then the lists of group identifications (ids) of all the routers are mutually exclusive i.e. they do not contain the same addresses.

5.29.3 How to Join a Group ?

- Who can join a group ? The answer is a host or a router can join a group. A host has a list of processes which are members of a group.
- If a processes wants to join a new group, then it has to send its request to do so to the host.
- The host adds the name of requesting process and the name of the group it wants to join to his list.
- If this is the first entry to this particular group, then the host sends a membership report message otherwise it is not necessary to send such a message.
- The same procedure is followed in case of a router. The process of joining a group with the format of membership report is shown in Fig. 5.29.4.



(G-589) **Fig. 5.29.4 : Membership report**

- The membership report needs to be sent twice one after the other within a quick succession, so that even if the first one is lost or damaged, the second one can be used.

Scanned by CamScanner

5.29.4 How to Leave a Group ?

- If no process of a group is interested in a specific group then a host sends a leave report.
- Similarly if a router understands that none of the networks connected to its interfaces is interested in a particular group then it sends a leave report about that group.
- On receiving the leave report the multicast router sends a special query message and inserts the multicast address or groupid which specifies the particular group.
- The router then allows some time for any host or router to answer to this query message.
- During this time if no interest in the form of membership report is received from any one then, the router purges the group from its list. This is the mechanism to leave a group.
- Fig. 5.29.5(a) shows the format of the leave report while Fig. 5.29.5(b) shows the format of special query message.

0x17	0	
Group address		

(a) Leave report

0x11	100	
Group address		

(b) Special query

Fig. 5.29.5

5.29.5 Monitoring Membership :

- Imagine a situation in which a host is interested in a particular group but that host has been shut down or removed from the group.
- Then the multicast router will never receive any leave report.
- To handle this situation, the router periodically sends a general query message after every 125 seconds.
- The general query message does not intend to define a specific group. So the group address field contents should be 0.0.0.0, and the router will expect an answer for each group in its list. Even the new groups are allowed to respond.
- The maximum response time allowed for this message is 10 sec.
- The query message should be sent only by one router which is normally called as a query router.
- The format of general query message is shown in Fig. 5.29.6.

0x11	100	
0.0.0.0		

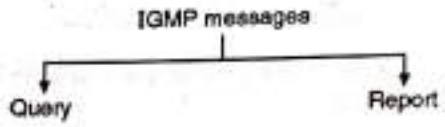
Fig. 5.29.6 : General query message

5.29.6 Query Router :

- Generally query messages create a lot of responses, which results in unnecessary traffic.
- To avoid this, the IGMP designates one router as a query router for each network.
- Only the query router is allowed to send the query message. All the other routers are passive. They reject responses and update their lists.

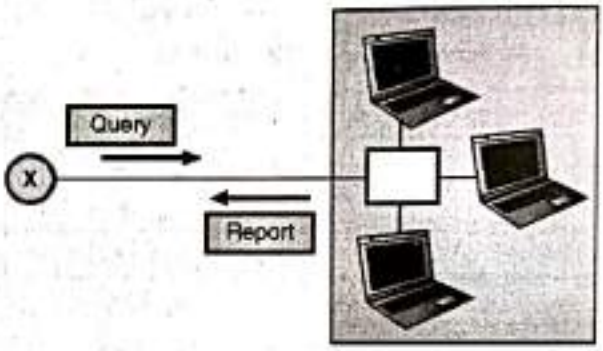
5.29.7 IGMP Messages :

- Today, for collection of information about group membership the IGMP (Internet group management protocol) is used.
- IGMP is one of the auxiliary protocol defined at the network layer which is considered as a part of Internet protocol.
- IGMP messages are encapsulated in datagram similar to ICMP messages.
- Fig. 5.29.7 shows two types of messages in IGMP version 3.



(G-2241) Fig. 5.29.7

- Fig. 5.29.8 shows the operation of IGMP :



(G-2242) Fig. 5.29.8 : Operation of IGMP

1. Query message :

- A router sends query message periodically to all hosts which are attached to it to ask them for reporting their membership interest in group. In IGMPv3, a query message can be in any one of three forms :

a. a general query message,
b. a group specific query message,
c. a source and group specific message.

a. General query message :

- In any group a general query message is sent about membership. With the destination address 224.0.0.1, a general query message is encapsulated in a datagram.
- All routers which are connected to the same network receive this general query message and inform them about the message which is already sent and avoid them from resending the message.

b. Group specific query message :

- To ask about a specific group membership, this message is sent from a router.
- If router do not receive any response about specific group and router want to make sure about a membership of that group in the network, then this group specific query message is sent. Multicast address (group identifier) is mentioned in the message.

Scanned by CamScanner

- In a datagram, the message is encapsulated with destination address set to the corresponding multicast address.
- This message is received by all the hosts and those who are not interested they will drop this message.

c. Source and group specific query message :

- When the message comes from a specific source, router sends this message to ask about membership related to a specific group.
- If router is not able to hear a specific group related to a specific host, then again this message is sent.
- With the destination address set to the corresponding multicast address the message is encapsulated in a datagram.
- This message is received by all the host and those who are not interested they will drop this message.

2. Report message :

- To give a response to a query message host sends report message.
- Report message contains :

1. List of records (in which each record gives the identifier of corresponding group i.e. multicast address).
2. Addresses of all sources in which the host is interested in receiving messages.

3. Addresses of sources from which the host do not want to receive a group message.

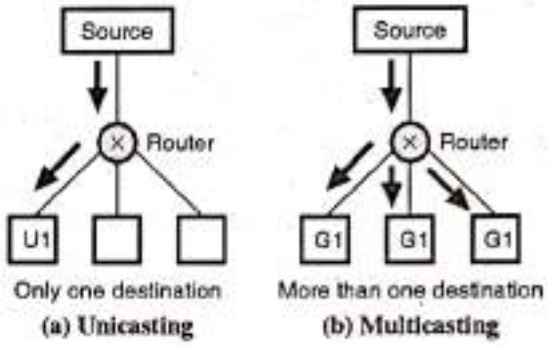
- In a datagram, the message is encapsulated with the multicast address 224.0.0.22 which is allocated to IGMPv3.
- In IGMPv3, if any host want to join a group, it will wait to receive a query message and then host sends a report message.
- If host want to leave the group then it will not respond to a query message.
- The group is eliminated from the router database if no hosts responds to corresponding message.

5.29.8 Multicast Forwarding :

- In multicasting, another issue is about the decision a router want to make for forwarding a multicast packet.
- In unicast and multicast communication, forwarding is different in two aspects which are discussed as follows :

1. Destination in unicasting and multicasting :

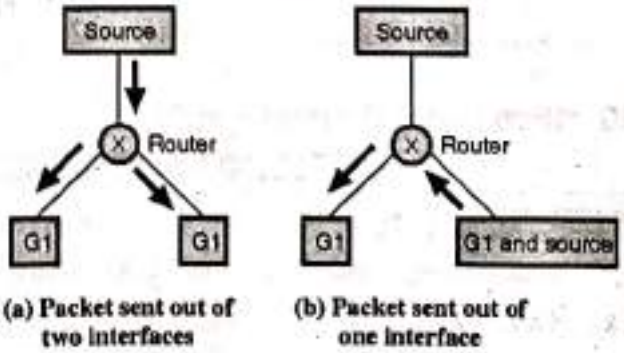
- In unicasting, only one single destination is defined by the destination address of the packet.
- It is necessary to send packet only out of one of the interface. And such interface is used which is the branch in shortest path tree which reaches the destination with minimum cast.
- In multicasting, one group is defined by the destination address of packet, but in the Internet that group can have more than one member.
- A router have to send the packet by using more than one interface to reach all of the destinations.
- This concept is as shown in Fig. 5.29.9. In unicast communication in the Internet U1 (destination network) cannot be in more than one part whereas G1(group) can have members in more than one part.



(G-2243) **Fig. 5.29.9 : Destination in unicasting and multicasting**

2. Forwarding decision :

- In unicasting, forwarding decision depends on the destination address of packet whereas in multicasting, it depends on both source and destination address of the packet.
- Forwarding in unicasting is based on where the packet should go, whereas forwarding in multicasting is based on where the packet has come from and where it should go.
- Forwarding concept is as shown in Fig. 5.29.10.
- Fig. 5.29.10(b) shows that, the source is present in the part of the Internet where there is group member available. To avoid sending second copy of packet from the interface it has arrived at the router must send the packet from only one interface. Fig. 5.29.10(b) shows that the member/members of the group G1 have already obtained a copy of packet. At the router when it arrives, if packet sent out in that direction does not help furthermore it generates more traffic. From this it is clear that in multicast communication forwarding depends on both source and destination address.



(G-2244) **Fig. 5.29.10 : Forwarding**

Scanned by CamScanner

5.29.9 Multicasting Approaches :

- Similar to unicast routing, multicast routing need to generate routing tress to route optimally the packets from their source to destination. As discussed earlier the multicast routing decision at each router depends on the destination and source of the packet.
- As compared to the unicasst routing, the involvement of the source in the routing process makes multicast routing more difficult. For this reason following two approaches are designed in multicast routing :
  1. Routing using source based trees.
  2. Routing using group shared trees.

1. Routing using source-based trees :

- In this approach, each router is required to generate a separate tree for each combination of source and group.
- Suppose in the Internet there are m number of groups and n number of sources. Then a router need to generate (m × n) routing trees.
- In each tree, source is the root, the members of the group are leaves and router itself is present somewhere on the tree.
- In unicast routing router needs only one tree in which router itself acts as root and in the Internet all networks acts as the leaves. But it can appear, about all these trees router needs to store and create a large amount of information.
- In the Internet recently there are two protocols which use this approach which we will disuss later in this chapter.

2. Routing using group shared tree :

- In this approach, for each group we assign a router to act as the phony source. The allocated router which is known as **core router** which acts as the representative for the group.
- If source has a packet to send to a member of group then it send that packet to the core centre (i.e. unicast communication) and for multicasting core centre is responsible. One single routing tree is created by the core centre and itself is the root and in group any routers with active members acts as leaves.
- If there are m core routers and each has a routing tree for m trees. That means number of routing trees are m in this approach which are reduced from (m × n) in the source based tree.

5.30 IPv6 (Next Generation IP) :

MU : Dec. 07, Dec. 08, Dec. 10

University Questions

Q. 1 Write short notes on : IPv6. **(Dec. 07, 5 Marks)**

Q. 2 List 10 important features of IPv6 protocol. **(Dec. 08, 10 Marks)**

Q. 3 Write short notes on : Features of IPv6 protocol. **(Dec. 10, 5 Marks)**

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 :

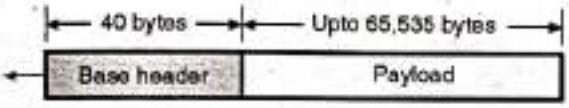
- IPv6 includes plug and play in the standard specification. It therefore must be easier for novice users to connect their machines to the network, it will be done automatically.

Scanned by CamScanner

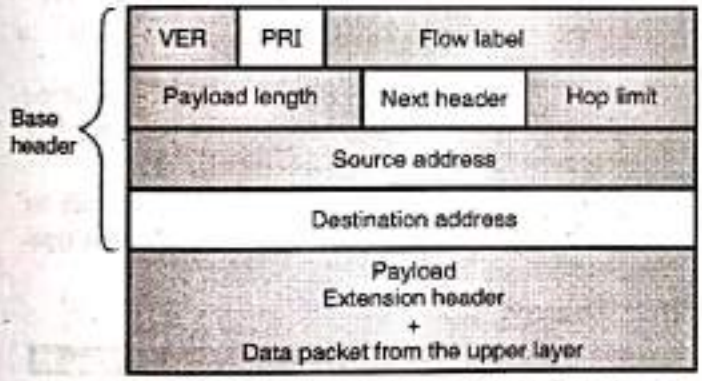
8. **Clearer specification and optimization :**
   - IPv6 follows good practices of IPv4, and omits flaws/obsolete items of IPv4.

5.30.1 IPv6 Packet Format :

- Fig. 5.30.1(a) shows IPv6 packet. Fig. 5.30.1(b) shows the packet format (Base header) of IPv6. Each packet can be divided into two parts viz : base header and payload.
- Base header is the mandatory part and payload is an optional one. The payload follows the base header.
- The payload is made up of two parts.
  1. An optional extension headers and
  2. The upper layer data.
- The base header is 40 byte long whereas the payload consisting of the extension header and upper layer data can have information worth upto 65, 535 bytes.



(G-2245)**Fig. 5.30.1(a) : IPv6 packet**



(G-550) **Fig. 5.30.1(b) : Format of an IPv6 datagram (Base header)**

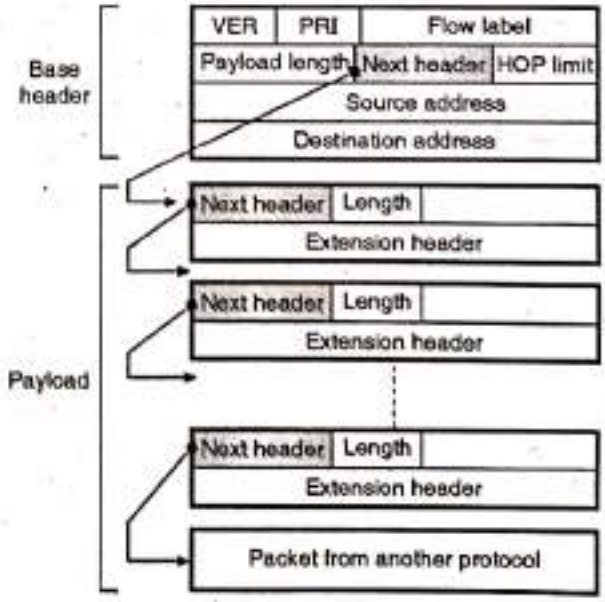
Base header :

Fig. 5.30.1(b) shows the base header. It has eight fields. These fields are as follows :

1. **Version (VER) :** The contents of this 4 bit field defines the version of IP such as IPv4 or IPv6. If VER = 6, then the version is IPv6.
2. **Priority :** This 4 bit field contents defines the priority of the packet which is important in connection with the traffic congestion.
3. **Flow label :** It is a 24 bit (3 byte) field which is supposed to provide a special handling for a particular flow of data.
4. **Payload length :** The contents of the 16 bit or 2 byte length field are used to indicate the total length of the IP datagram excluding the base header. That means it gives the length of only the payload part of the datagram.
5. **Next header :** It is an 8 bit field which defines the header which follows the base header in the datagram.
6. **Hop limit :** Contents of this 8 bit (1 byte) field have the same function as TTL (time to live) in IPv4.
7. **Source address :** It is a 16 byte (128 bit) Internet address which corresponds to the originator or source which has produced the datagram.
8. **Destination address :** This is a 16 byte (128 bit) internet address which corresponds to the address of the final destination of datagram. But this field will contain the address of the next router and not the final destination if source routing is being used.

5.30.2 Payload :

- The meaning and format of payload field in IPv6 is different as compared to payload field in IPv4.
- Fig. 5.30.2 shows payload field in IPv6.
- In IPv6, the payload is combination of zero or more extension headers (options) which is followed by data from other protocols such as UDP, TCP etc.
- In IPv4, option is a part of the header, whereas in IPv6 it is designed as extension headers.
- Depends on the situation the payload can have as many extension headers as required.
- Extension header is made up of two mandatory fields : next header and the length which is followed by information which is related to the particular option.
- Value of next header field i.e. code defines which type of the next header is (e.g. source routing options, fragmentation option etc.)
- The last next header describes the protocol which carries the datagram.
- Some next header codes are listed in Table 5.30.1.



(G-2246) **Fig. 5.30.2 : IPv6 payload**

Scanned by CamScanner

Table 5.30.1 : Next header codes

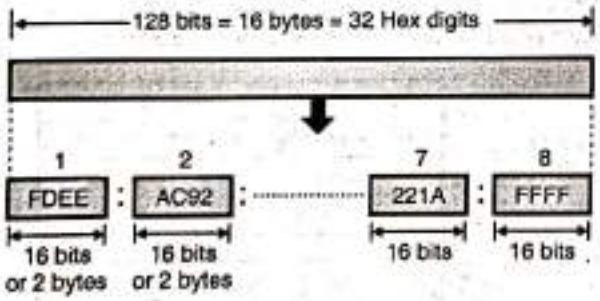
Sr. No.	Code	Next header code
1.	00	HOP by hop option
2.	02	ICMPv6
3.	06	TCP
4.	17	UDP
5.	43	Source routing option
6.	44	Fragmentation option
7.	50	Encrypted security payload
8.	51	Authentication header
9.	59	Null (no next header)
10.	60	Destination option

5.31 IPv6 Addressing :

- IPv6 is the next generation Internet Protocol designed as the next step of the IP version 4. IPv6 was designed to enable high-performance and larger address space. This was achieved by overcoming many of the weaknesses of IPv4 protocol and by adding several new features.
- The IPv6 was developed due to the address depletion of IPv4.
- The structure of IPv6 address is fundamentally different than that of IPv4. Therefore there is absolutely no possibility of address depletion taking place in future.

5.31.1 IPv6 Address :

- An IPv6 address is 128 bit long. It consists of 16 bytes as shown in Fig. 5.31.1. Thus the IPv6 address is 4 times longer than that of IPv4.



(G-545) **Fig. 5.31.1 : IPv6 address**

5.31.2 Notations :

- An address is stored in the computers in the binary form. But it is impossible for humans to handle a 128 bit binary address.
- Therefore many notations have been proposed to represent the IPv6 addresses, so that they become easier to handle for human beings.
- Some of the proposed notations are :
  1. Dotted decimal notation.
  2. Colon hexadecimal notation.
  3. Mixed representation.
  4. CIDR notation.

1. Dotted decimal notation :

- In order to maintain the compatibility with IPv4 addresses. We may feel tempted to use the dotted decimal notation.
- But practical observation is that this notation is convenient only for the 4 byte address of IPv4. It is not at all convenient for the 16 byte IPv6 addresses as it seems too long.
- Therefore this notation is very rarely used.

2. Colon hexadecimal notation :

- The 128 bit address can be made more readable and easy to handle. IPv6 has specified the **colon hexadecimal notation.**
- IPv6 uses a special notation called hexadecimal colon notation. In this, the total 128 bits are divided into 8 sections, each one is 16 bits or 2 bytes long.
- The 16 bits or 2 bytes in binary correspond to four hexadecimal digits of 4-bits each. Hence the 128 bits in hexadecimal form will have $8 \times 4 = 32$ hexadecimal digits. These are in groups of 4 digits as shown and every group is separated by a colon as shown in Fig. 5.31.2.

AC 81 : 9840 : 0086 : 3210 : 000A : BBFF : 0000 : FFFF

Fig. 5.31.2 : Colon hexadecimal notation

- IPv6 uses 128-bit addresses. Only about 15% of the address space is initially allocated, the remaining 85% being reserved for future use.
- These unused addresses may be used in the future for expanding the address spaces of existing address types or for totally new uses.

5.31.3 Abbreviation :

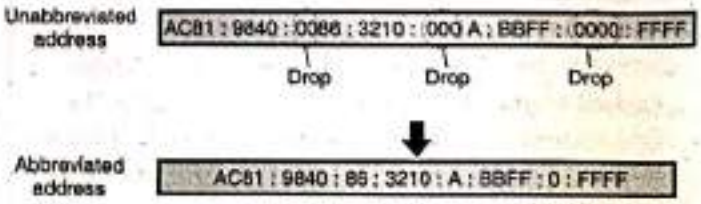
MU : Dec. 09, May 11, May 13

University Questions

Q. 1 Explain Classless Inter Domain Routing (CIDR) **(Dec. 09, May 11, 5 Marks)**

Q. 2 Write short notes on : CIDR. **(May 13, 5 Marks)**

- 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. 5.31.3.



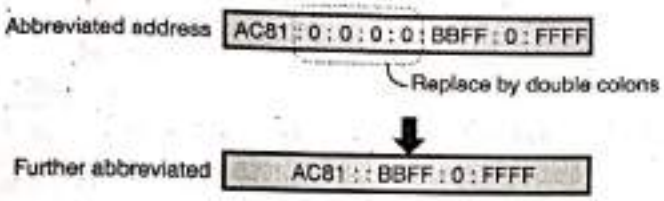
(G-546) **Fig. 5.31.3 : Abbreviated address**

Scanned by CamScanner

- Note that only the leading zeros can be dropped but the trailing zeros can not be dropped. This is illustrated in Fig. 5.31.3. Thus due to abbreviation the length of the address has reduced to 24 hex digits from 32.

Further abbreviation :

- We can make further abbreviation if there are consecutive sections consisting of only zeros. This is known as **zero compression.**
- We can remove the zeros completely and replace them with double colon as shown in Fig. 5.31.4.



(G-547) **Fig. 5.31.4 : Further abbreviation (Zero compression)**

- This further abbreviation has reduced the address length to just 13 hex digits.
- It is important to note that abbreviation can be done only once per address. Also note that if there are two sets of zero sections, then only one of them can be abbreviated.

3. Mixed representation :

- Sometimes, the IPv6 address is represented using a mixed representation which combines the **colon hex** and **dotted decimal** notations.
- This notation is appropriate during the transition time during which an IPv4 address is being embedded in IPv6 address.
- In the mixed representation the rightmost 32 bits correspond to the IPv4 address Hence they are represented by the dotted decimal notation.
- Whereas the leftmost 96 bits (6 sections) are represented in colon hex notation.

4. CIDR notation :

- The type of addressing used in IPv6 is **hierarchical addressing.** Therefore IPv6 allows classless addressing and CIDR notation.
- Fig. 5.31.5 illustrates the CIDR address with a 60 bit prefix. It has been discussed later on in this chapter, how we can divide an IPv6 address into a prefix and a suffix.

(G-2132) **Fig. 5.31.5 : CIDR address**

Ex. 5.31.1 : IPv6 uses 16-byte addresses. If a block of 1 million addresses is allocated every picosecond, how long will be the addresses last ?

Soln. :

1. Total number of address bits = $16 \times 8 = 128$
2. Number of addresses = $2^{128} = 3.4 \times 10^{38}$
3. One picosecond = 1×10^{-12} seconds
4. 1 million addresses = 1×10^{6} address

$\therefore$ 1 picosecond = 1×10^{6} addresses

$$\therefore x = 3.4 \times 10^{38}$$

$$\therefore x = \frac{3.4 \times 10^{38}}{1 \times 10^{6}} \times 1 \text{ picoseconds}$$

$$= 3.4 \times 10^{32} \text{ picoseconds}$$

$$= 3.4 \times 10^{20} \text{ seconds}$$

$$= 9.44 \times 10^{16} \text{ hours}$$

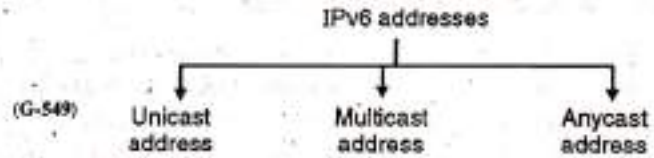
$$= 3.9352 \times 10^{15} \text{ days} = 1.0781 \times 10^{13} \text{ years}$$

5.32 Address Space :

- The address space of IPv6 contains 2^{128} addresses which is a very big number. If we compare it with the address space of IPv4, then it can be seen that, the address space of IPv6 is 2^{96} times bigger than that of IPv4.
- Therefore there is no possibility of address depletion in IPv6.

5.32.1 Three Address Types :

- IPv6 defines three different types of addresses. The destination address can be one of these types :



(G-549)

1. Unicast address :

- A unicast address is meant for a single computer as a destination. A packet sent to a unicast address is meant to be delivered to the computer specified by the address.
- In IPv6 a large block of addresses has been designated from which it is possible to assign unicast addresses to the interfaces.

2. Anycast address :

- This is a type of address which is used to define a group of computers with addresses which have the same prefix.
- A packet sent to an anycast address must be delivered to only one of the member of the group which is the closest or the most easily accessible.
- No special or separate address block is assigned for anycasting in IPv6. Instead the anycast addresses are assigned from the block of unicast addresses.

Scanned by CamScanner

3. Multicast addresses :

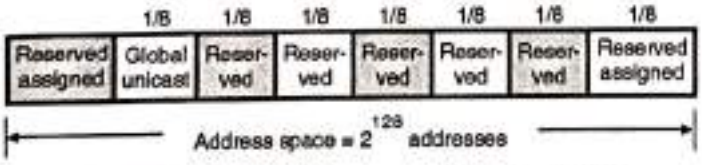
- A multicast address defines a group of computers which may or may not share the same prefix and may or may not be connected to the same physical network.
- A packet sent to a multicast address is meant to be delivered to each member of the group.
- There are no broadcast addresses in IPv6, because multicast addresses can perform the same function. The type of address is determined by the leading bits.
- All the multicast addresses start with FF (1111 1111) and all other addresses are unicast addresses.
- Anycast addresses are assigned from the unicast address space and they do not differ syntactically from unicast addresses.
- Anycast addressing is a rather new concept and there is not much experience about the widespread use of anycast addresses.
- Therefore, some restrictions apply to anycast addressing in IPv6 until more experience is gained.
- An anycast address may not be used as the Source Address of an IPv6 packet and anycast addresses may not be assigned to hosts but to routers only.
- As will be discussed later, a block is designated for multicasting in IPv6, from which the same address is assigned to the members of the group.

5.32.2 Broadcasting and Multicasting :

In IPv6 the broadcasting is not defined at all, as in case of IPv4. In IPv6 broadcasting is considered as a special case of multicasting.

5.33 Address Space Allocation :

- Address space allocation in IPv6 is a process which divides the address space of IPv6 in several blocks. Each block is allocated for some special purpose and has a different size.
- Most of the blocks in IPv6 are not assigned yet and will be used in future.
- The entire address space in IPv6 has been divided into eight equal ranges, as shows in Fig. 5.33.1.

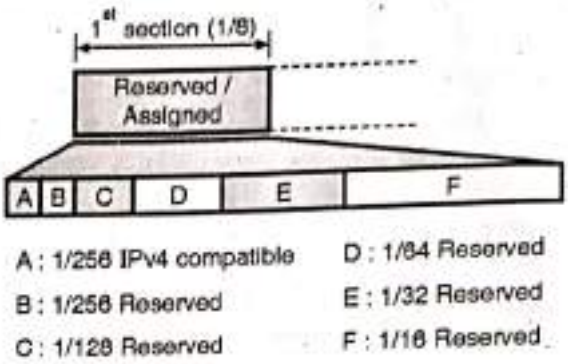


(G-2133) **Fig. 5.33.1 : Address space allocation in IPv6**

- As shown in Fig. 5.33.1, the number of addresses in each section is one eighth of the total address space. So number of addresses in each section is equal to 2^{125} addresses.

5.33.1 The First Section :

- The first section is market as Reserved/Assigned in Fig. 5.33.2. That means some address blocks in this section are reserved and the remaining are assigned as shown in Fig. 5.33.2(a).



(G-2134) **Fig. 5.33.2(a) : The first section**

- As shown in Fig. 5.33.2(a), the first section is divided in six blocks of variable sizes (blocks A to F). Out of these six blocks, three blocks have been reserved and remaining three are not assigned.

5.33.2 Second Section :

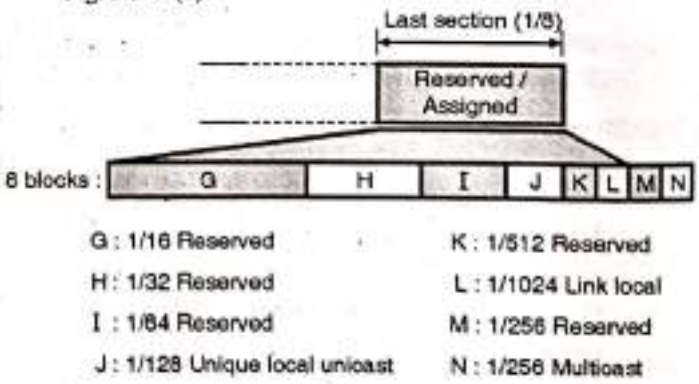
- The second section is not divided into blocks. So it is considered as one single block and is used for the global **unicast** addresses.

Sections three to seven :

These five sections from third to seventh are unassigned.

Last section :

- The last section in Fig. 5.33.2 which is marked as Reserved /Assigned is further divided into eight blocks of different sizes as shown in Fig. 5.33.2(b).
- Some of these blocks are not assigned while the other blocks are reserved for some special purpose as shown in Fig. 5.33.2(b).



(G-2135) **Fig. 5.33.2(b) : The last section**

- From all this discussion it is very clear that out of the total address space of IPv6 more than 5/8th of the space is still not assigned, and only 1/8th of the address space has been assigned for the global unicast addresses for unicast communication between the users.

Scanned by CamScanner

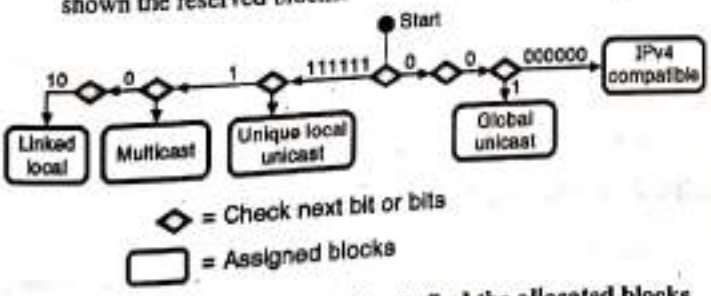
- The prefix for each type of address has been shown in Table 5.33.1.

Table 5.33.1 : Prefixes for IP addresses

	Block Prefix	CIDR	Block Assignment	Fraction
1	0000 0000	0000::/8	Reserved (IPv4 compatible)	1/256
	0000 0001	0100::/8	Reserved	1/256
	0000 001	0200::/7	Reserved	1/128
	0000 01	0400::/6	Reserved	1/64
	0000 1	0800::/5	Reserved	1/32
	0001	1000::/4	Reserved	1/16
2	**001**	**2000::/3**	**Global unicast**	**1/8**
3	010	4000::/3	Reserved	1/8
4	011	6000::/3	Reserved	1/8
5	100	8000::/3	Reserved	1/8
6	101	A000::/3	Reserved	1/8
7	110	C000::/3	Reserved	1/8
8	1110	E000::/4	Reserved	1/16
	1111 0	F000::/5	Reserved	1/32
	1111 10	F800::/6	Reserved	1/64
	1111 110	FC00::/7	Unique local unicat	1/128
	1111 1110 0	FE00::/9	Reserved	1/512
	1111 1110 10	FE80::/10	Link local addresses	1/1024
	1111 1110 11	FEC0::/10	Reserved	1/1024
	1111 1111	FF00::/8	Multicast addresses	1/256

5.33.3 Algorithm :

- The diagram shown in Fig. 5.33.3 has been created to illustrate that the prefixes given in Table 5.33.1 really find the block to which the IPv6 address belongs to.
- Note that, in order to make this diagram simpler we have not shown the reserved blocks.



(G-2136) **Fig. 5.33.3 : An algorithm to find the allocated blocks**

5.33.4 Assigned or Reserved Blocks :

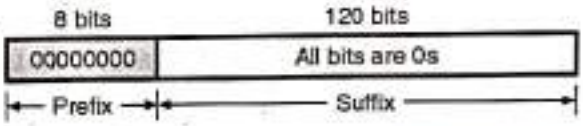
- In this section, we are going to discuss the purposes and characteristics of the reserved as well as assigned blocks starting from the first row of Table 5.33.1.

1. **IPv4 compatible addresses :**
   - The addresses which use the prefix (00000000) are reserved, however a part of it is used for defining some IPv4 compatible addresses.
   - There are 2^{120} addresses in this block because it occupies 1/256 the fraction of the total address space.
   - This block can be defined using CIDR notation as follows :

     0000::/8
   - This address block is further divided into many smaller subblocks. We will discuss them later in this chapter.

5.33.5 Unspecified Address :

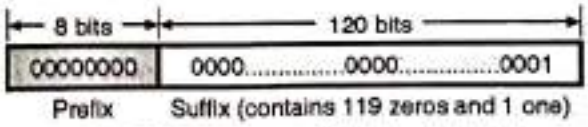
- The unspecified address is a subblock which contains only one address. By letting all suffix bits to zero, this address can be defined. That means this address is an all zeros address.
- During the bootstrapping process, when a host does not know its own address, the unspecified address is used to send an enquiry to find the unknown address of the host.
- This address is used by the host as a **source address.** However it is important to note that the unspecified address cannot be used as the **destination address.**
- This one-address subblock can be represented as ::/128 in the CIDR notation, and its format has been shown in Fig. 5.33.4.



(G-2137) **Fig. 5.33.4 : Format of the unspecified address**

5.33.6 Loopback Address :

- Like the previous one, this subblock also contains only one address which a host uses for testing itself without going into the network.
- Here the application layer creates an address, sends it to the transport layer and then passes it to the network layer.
- However it does not go to the physical layer. Instead, it returns to the transport layer and finally passed on to the application layer.
- This feature is very useful because using it we can test the functions of software package in these layers even before the computer is connected to the network.
- Fig. 5.33.5 shows the format of the loopback address which has the prefix of 00000000 and a suffix containing 119 zeros and one 1.
- We can represent this address in the CIDR notation as ::1/128.



(G-2138) **Fig. 5.33.5 : Format of the loopback address**

Scanned by CamScanner

5.33.7 Difference between Loopback Address of IPv4 and IPv6 :

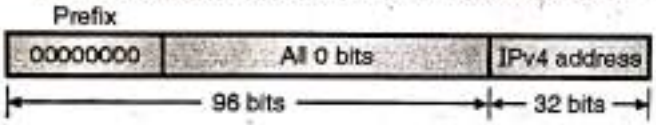
- In IPv4 classful addressing, the loop back addresses get a whole block allotted to them but in IPv6 loopback addresse is only one single address.
- In IPv4 the loop back addresses are accommodated as a part of class A address but in IPv6 it is only one single address in the reserved block.

5.33.8 Embedded IPv4 Addresses :

- As discussed in the migration from IPv4 to IPv6 in this transition period, the hosts can continue to use their IPv4 address which are embedded in IPv6 addresses.
- In order to achieve this, IPv6 has designed two formats namely **compatible format** and **mapped** format.

5.33.9 Compatible Address :

- The compatible address is an IPv6 address with 96 bits of zeros followed by 32 bits of IPv4 address.
- Fig. 5.33.6 shows the format of IPv6 compatible address.

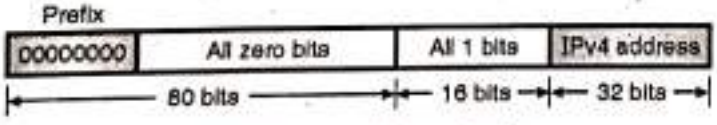


(G-2139) **Fig. 5.33.6 : Format of compatible address**

- The situation in which the compatible address is required to be used is as follows : If an IPv6 host wants to communicate with another IPv6 host but the packet is going to pass through a region in which still the IPv4 is being used by the networks.
- In order to ensure a successful passage of this packet the sender will have to use the **compatible address.**
- This is a reserved subblock which contains 2^{32} addresses and has a CIDR notation of ::/96.

5.33.10 A Mapped Address :

- The format of a mapped address is shown in Fig. 5.33.7. It shows that this address consists of 80 bits of zeros, followed by 16 bits of 1s, followed by 32 bits of IPv4 address.
- It is used when an IPv6 computer wants to communicate with an IPv4 computer.



(G-2140) **Fig. 5.33.7 : Mapped address**

- This packet can travel for an IPv6 guest, through a mostly IPv6 network and finally delivered to an IPv4 destination host.

5.33.11 Calculation of Checksum :

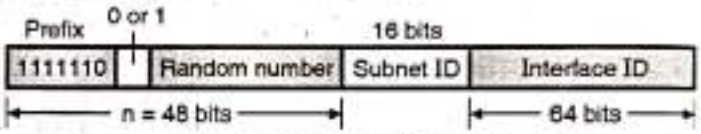
- The compatible and mapped addresses have been designed in such a way that the checksum can be calculated by either using the embedded address or the complete address because the extra zeros and ones are in multiples of 16. Hence they do not affect the checksum calculation in any way.
- So the value of checksum remains same even if the packet address is changed from IPv6 to IPv4.

5.34 Global Unicast Block :

- This block is the main block which is used for facilitating the unicast communication between the hosts in the Internet.
- It is used in Internet to provide the **hierarchical addressing.**

5.34.1 Unique Local Unicast Block :

- When we discussed the private addresses for IPv4, it was seen that some blocks in the IPv4 address space were reserved for private addressing.
- In IPv6 they have reserved two large blocks for the private addressing. One block is reserved at the site level and the other one is reserved at the link level.
- The format of the unique local unicast block is as shown in Fig. 5.34.1.



(G-2141) **Fig. 5.34.1 : Unique local unicast block**

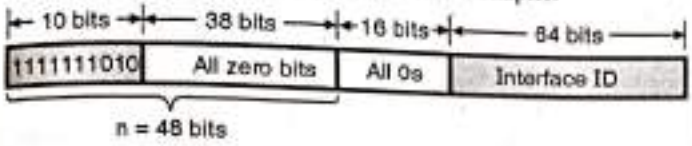
- We will discuss the first type i.e. the one which is reserved at the site in this section and the other one in the next section.
- Refer Fig. 5.34.1 which shows that it is possible to privately create a subblock in **unique local unicast block** and used by a site.
- We cannot expect a packet which is carrying this type of address as its destination address to be routed.
- The block identifier for this type of address is 1111 110 as shown in Fig. 5.34.1. The last (8th) bit can be 0 or 1 which is used for defining how the address is selected (locally or by an authority).
- The site selects the next 40 bits which is a randomly generated number. In this way the first 48 bits define a subblock which looks like a **global unicast address.**
- Due to this random number of 40 bits, the possibility of duplication of the address reduces to a very small value. This address and the global unicast address look very similar to each other.

5.34.2 Link Local Block :

- Link local block is the second block designed for private addresses. It is possible to use a subblock in this block as a private address in a network.
- The format of the link local address is as shown in Fig. 5.34.2. The first 8 bit block consists of the block identifier which is 1111111010 for this type of address.

Scanned by CamScanner

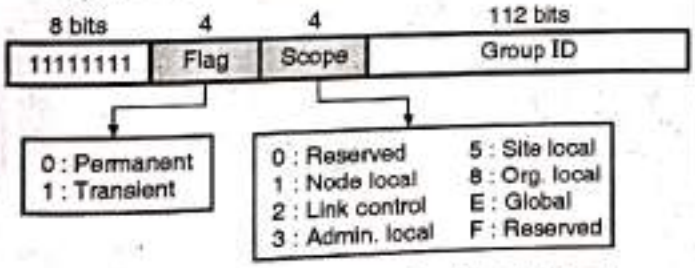
- The next 54 bits are set to zero and we can change the last 64 bits (interface ID) to define the interface for each computer.
- Even this address is very similar to the global unicast address, which has been discussed later on in this chapter.



(G-2142) **Fig. 5.34.2 : Link local address**

5.34.3 Multicast Block :

- While discussing the multicast addresses for IPv4 we have stated that multicast addresses are those which are used to define a group of hosts.
- A large block of addresses has been assigned for multicasting in IPv6.
- The prefix for all these addresses is 11111111, as shown in the format of the multicast address (Fig. 5.34.3).
- The second field in this address is a 4 bit **flag field.** It is used for defining the group address as either permanent or transient.
- The Internet authorities define **permanent group address** and it can be accessed at all the times.
- On the other hand, the transient group address is used only temporarily, for example when systems are engaged in teleconference, they can use a transient group address.
- The third field is the 4 bit **scope** field the contents of which define the scope of group address. Depending on its contents, various scopes are defined as shown in Fig. 5.34.3.



(G-2143) **Fig. 5.34.3 : Format of multicast address**

5.35 Global Unicast Address :

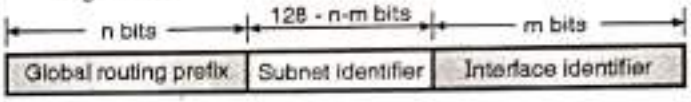
- This block is present in the address space. It is used by two hosts in the Internet for the unicast (one to one) communication between them. This block of addresses in IPv6 is called as **global unicast address block.**
- The CIDR notation used for this block is 2000::/3 which indicates that the 3 leftmost bits are same (101) for all the addresses in this blocks.
- The number of addresses in this block is 2^{125} which is a huge number and sufficient for many more years to come.

5.35.1 Three Levels of Hierarchy :

Any address in this block is divided into three parts as follows :

1. Global routing prefix.
2. Subnet identifier.
3. Internet identifier.

- The format of global unicast address is as shown in Fig. 5.35.1.



(G-2144) **Fig. 5.35.1 : Global unicast address**

- The recommended values for the lengths of the three blocks shown in Fig. 5.35.1 are as follows :

Block Name	Length
Global routing prefix	n = 48 bits
Subnet identifier	128 – n – m = 16 bits
Interface identifier	m = 64 bits

- The three parts in the global unicast address are as follows :

5.35.2 Global Routing Prefix :

- As shown in Fig. 5.35.1, the first block of 48 bits in the global unicast address is called as global routing prefix.
- The packet is routed through the Internet to the organization site using these 48 bits. The first three bits in this block are fixed (001). Therefore the remaining 45 bits can be used to define upto 2^{45} sites.
- A packet is routed to its destination site through the Internet by the global routers on the basis of the value of n.

Subnet Identifier :

- As shown in Fig. 5.35.1, the second block of 16 bits in the global unicast address is called as the subnet identifier.
- It is used for defining a subnet in the organization. This means that there can be 2^{16} = 65,535 subnets in an organization.

Interface Identifier :

- The last 64 bits in the global unicast address define the interface identifier (Fig. 5.35.1).
- The interface identifier is very similar to the **hostid** which we defined for IPv4.
- There is no specific relation between the **hostid** and the physical address in IPv4.
- But in IPv6 this is possible. The length of the physical address is less then 64 bits. Hence it can be embedded fully or partially in the interface identifier. This will eliminate the need of address mapping process completely.

Scanned by CamScanner

5.35.3 Autoconfiguration :

- Autoconfiguration of hosts is one of the most interesting features of IPv6 addressing.
- In IPv4 the network manager originally configures the hosts and routers. Then we can allocate an IPv4 address to a host that joins the network using the DHCP protocol.
- In IPv6 we can either use DHCP protocol for allocating the IPv6 address to host or host can configure itself.
- The process of self configuration of a host when it joins the IPv6 network is as explained below.

1. The **link local address** is first created by the host for itself. This is done by following the stepwise procedure given below :
   (a) Take the 10 bit link local prefix (1111 1110 10).
   (b) Add 54 zeros to it.
   (c) Add 64 bit interface identifier which any host can generate from its interface card.

   After this we get the 128 bit link local address.
2. The host then checks for the uniqueness of this link local address. The 64 bit interface identifier also should be unique. To ensure this a neighbour solicitation message is sent by the host. Then it waits for the **neighbour advertisement message.** The process of autoconfiguration fails if any host in the subnet is using the same link local address. Then the host should use DHCP protocol to configure itself.
3. If the link local address is found to be unique, the host will store this address as its link local address for private communication. But it still requires a global unicast address. Therefore the **router solicitation message** is sent out by the host to a local router. If there is a router running on this network, then the host will receive the **router advertisement message.** This message contains the global unicast prefix and subnet prefix. The host adds these two pieces of information to its interface identifier and generates its **global unicast address.** However if it is not possible of the router to help the host with the configuration, then the router informs the host via the router advertisement message. In such a situation, the host needs to use some other means for its configuration.

5.36 Renumbering :

- In the IPv6 addressing, the facility of renumbering the address prefix (value of n) is given which allows sites to changes the service provider.
- The service provider gives a prefix number to each site to which it is connected. Therefore the site has to change the prefix number if it has to change the service provider.
- A router to which the site is connected can advertise a new prefix. The site is allowed to use its old prefix for sometime before it is finally disabled. This implies that a site uses two prefixes during the transition period.
- However the problem in using this renumbering mechanism is that it needs support of DNS.
- To overcome this problem, a new DNS protocol called **New Generation DNS** is being studied because it can support the renumbering mechanism.

5.36.1 Migrating to IPv6 (Compatibility to IPv4) :

1. It was IPv4's success that made an upgrade necessary, which means that there is a large number of IPv4 users that to be upgraded to IPv6. Keeping the transition orderly was a major objective of the entire IPng program. The cutover date when IPv6 would be turned on and IPv4 turned off has not been decided.
2. The simple strategy for upgrading involves deployment of IPv6 protocol stack in parallel with IPv4. In other words, hosts that upgrade to IPv6 will continue to simultaneously exist as IPv4 hosts.
3. An experimental IPv6 backbone, or 6 bone, has been set up to handle IPv6 Internet traffic in parallel with the regular Internet. Such hosts will continue to have 32-bit IPv4 addresses but will add 128-bit IPv6 addresses. By 1999, hundreds of networks were linked to the 6 bone.
4. The transition can be achieved through two approaches: protocol tunneling or IPv4/IPv6 dual stack.

5.36.2 Comparison between IPv4 and IPv6 :

MU : Dec. 14

University Questions

Q. 1 Compare the network layer protocols IPv4 and IPv6 **(Dec. 14, 10 Marks)**

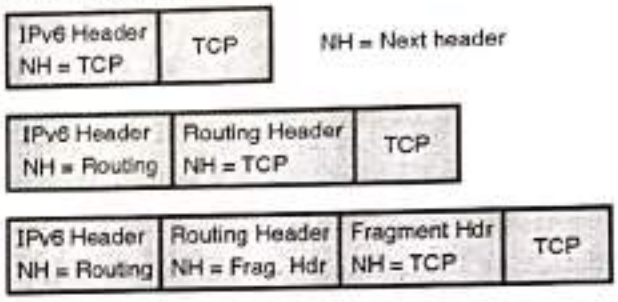
IPv4	IPv6
In IPv4 there are only 2^{32} possible ways to represent the address (about 4 billion possible addresses)	In IPv6 there are 2^{128} possible way (about 3.4×10^{38} possible addresses)
The IPv4 address is written by dotted-decimal notation, e.g. 121.2.8.12	IPv6 is written in hexadecimal and 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.

Scanned by CamScanner

IPv4	IPv6
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.
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.

5.36.3 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. 5.36.1).
- 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 :



(L-895) **Fig. 5.36.1 : 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 preceeding ones.
- Each extension header has a length equal to a multiple of 64 bits (8 bytes). A full implementation of IPv6 must include support for the following extension headers :
- When more than one extension header is used in the same packet, it is recommended that those headers appear in the following order :
  1. IPv6 header
  2. Hop-by-Hop Options header
  3. Destination Options header
  4. Routing header
  5. Fragment header
  6. Authentication header
  7. Encapsulating Security Payload header
  8. Destination Options header
  9. Upper-layer header

1. Fragmentation :

- The fragmentation in IPv6 is conceptually same as that discussed for IPv4, but the fragmentation in IPv6 takes place at a different place than that in IPv4.

Scanned by CamScanner

- In IPv4 the fragmentation is done by the source or router, but in IPv6 the fragmentation may be carried out only by the original source.

2. Authentication and Privacy :

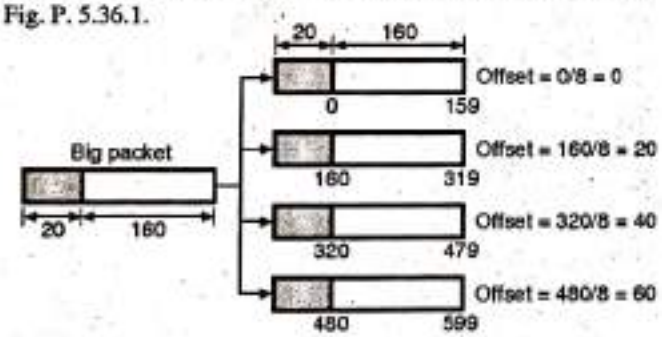
- IPv6 provides authentication and privacy using options in the extension header.

5.36.4 Solved Examples :

Ex. 5.36.1 : 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.

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. 5.36.1.



(G-1503) **Fig. P. 5.36.1 : Fragmentation**

Ex. 5.36.2 : 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.

Soln. :

Given : IP address : 220.125.5.192/26

Step 1 : Subnet mask :

- This is class C network. So default mask is given by,

255 · 255 · 255 · 0

(G-1504) **Fig. P. 5.36.2 : Subnet mask**

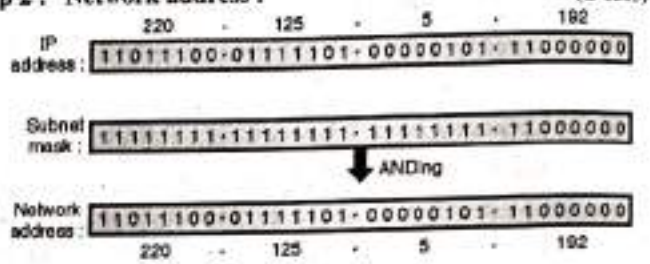
- The subnet mask is given by,

255.255.255.192

- Total number of hosts connected in each network are 64.

Step 2 : Network address :

(G-1505)



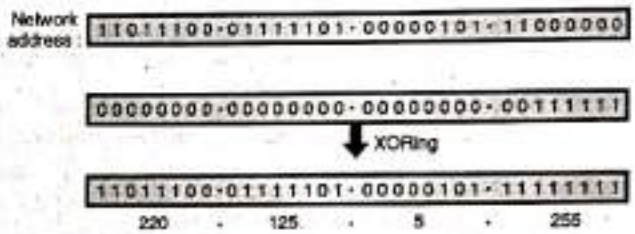
- Network address is,

220.125.5.192

Step 3 : Broadcast address :

To find broadcast address, take the inverted subnet mask and perform XOR with the network address.

(G-1506)



- The broadcast address is,

220.125.5.255

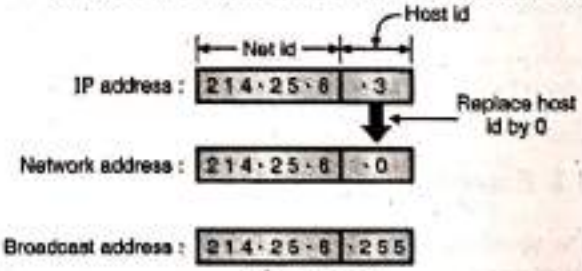
Ex. 5.36.3 : Identify class, subnet mask, network address and broadcast address of following IP addresses :

1. 214.25.6.3 2. 191.5.8.9
3. 5.6.45.4 4. 230.45.89.63

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. 5.36.3.



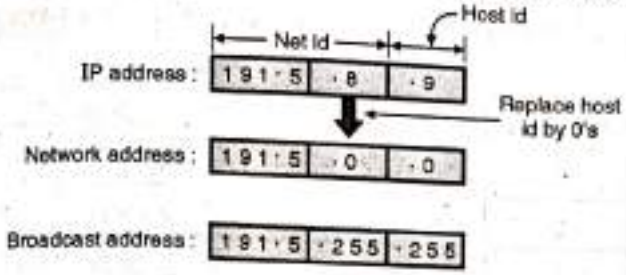
(G-1507) **Fig. P. 5.36.3**

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.

Scanned by CamScanner

– The net id and host id are as shown in Fig. P. 5.36.3(a).



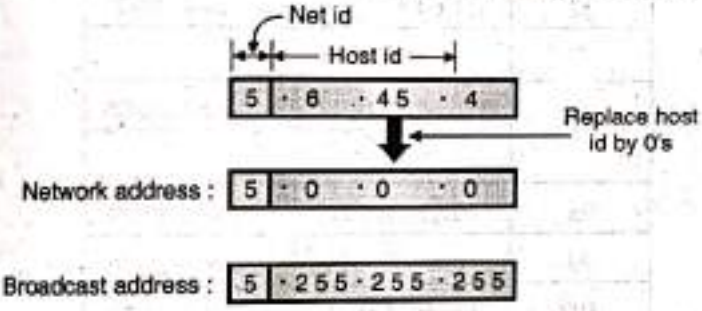
(G-1508) **Fig. P. 5.36.3(a)**

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. 5.36.3(b).



(G-1509) **Fig. P. 5.36.3(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. 5.36.3(c).

230	Multicast address

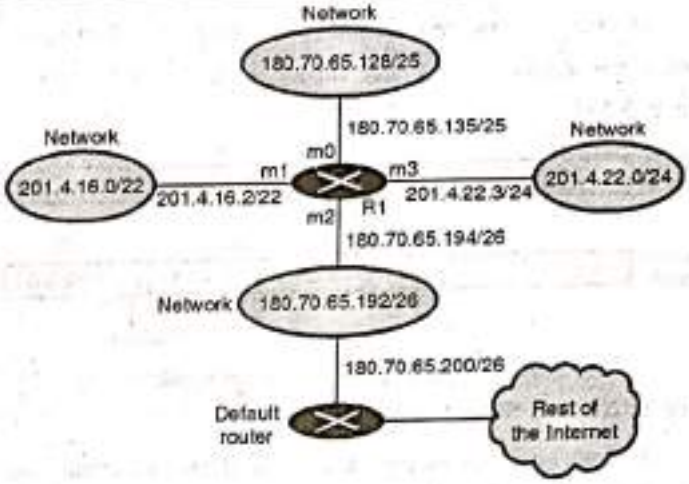
Fig. P. 5.36.3(c)

Ex. 5.36.4 : A router is networking four different networks with network addresses 180.70.65.192/26, 180.70.65.128/25, 201.4.22.0/24, 01.4.16.0/22 and default router on 180.70.65.200 make a routing table for this router and explain the forwarding process for packet with destination IP 18.24.32.78.

Soln. :

Step 1 : Draw the configuration :

The configuration is as shown in Fig. P. 5.36.4.



(G-1510) **Fig. P. 5.36.4 : The given configuration**

Step 2 : Make the routing table :

The routing table is as shown in Table P. 5.36.4.

Table P. 5.36.4 : 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. 5.36.5 : 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 ?

Soln. :

Given : A class C network, 3 subnets.

To find : 1. Network mask
2. Number of hosts per subnet

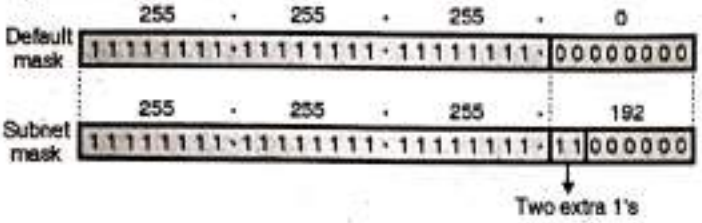
Step 1 : Subnet mask :

The default mask for a class C network is

255 · 255 · 255 · 0

Scanned by CamScanner

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. 5.36.5.



(G-1512) **Fig. P. 5.36.5 : Subnet mask**

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. 5.36.6 : 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.

$$\log 2^8 = \log 2^3$$
$$= 3 \log 2^2$$
$$= 3 \times 1$$
$$= 3$$

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	120.60.4.255/29
⋮	⋮	⋮
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

Numbers of granted address= 1024

Number of allocated address= 800

Number of available address

= Number of granted address – Number of allocated address.

$= 1024 - 800 = 224$

Ex. 5.36.7 : 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. :

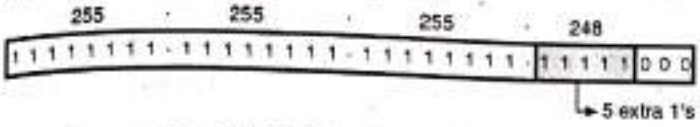
Step 1 : Subnet mask :

This is a class C network. So the default mask is given by,

255.255.255.0

Scanned by CamScanner

As we need 32 subnets we need 5 extra 1's. So the subnet mask will be as follows in the binary form.



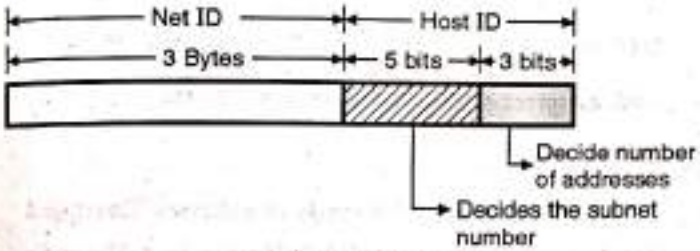
(G-1513) **Fig. P. 5.36.7(a) : Subnet mask**

The subnet mask is therefore given by,

255.255.255.248

Step 2 : Number of addresses in each subnet :

The structure of a class C address is as shown in Fig. P. 5.36.7(b).



(G-1514) **Fig. P. 5.36.7(b)**

As seen from Fig. P. 5.36.7(b), we have only 3 bits to decide the number of addresses in each subnet.

$\therefore$ No. of addresses per subnet $= 2^3 = 8$

Step 3 : First and the last address in subnet 1 :

First address in subet-1 = 211.17.180.0

Last address in subet-1 = 211.17.180.7

Step 4 : First and the last address in subnet 31 :

First address in subet-32 = 211.17.180.248

Last address in subet-32 = 211.17.180.255

Ex. 5.36.8 : 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. :

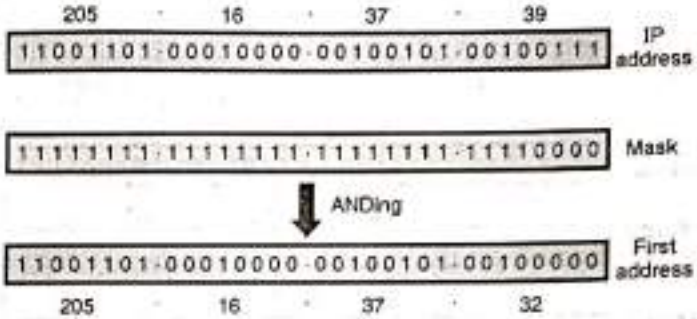
Given IP address is 205.16.37.39/28.

1. **To find address mask :**

Address mask is /28 which can be represented as

11111111.11111111.11111111.11110000

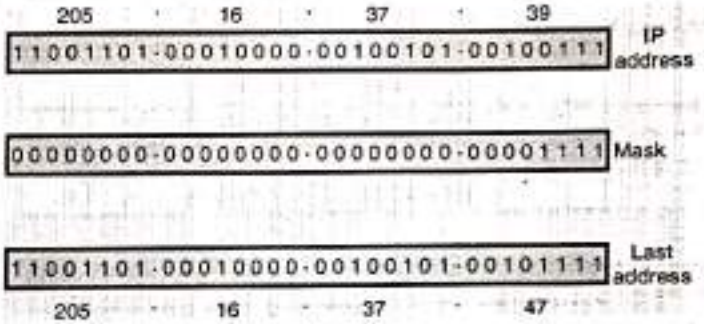
2. **To find first address of block AND the given address with mask :**



(G-1515) **Fig. P. 5.36.8**

First address of block is 205.16.37.32. **...Ans.**

3. **To find last address of the block OR the given address with mask :**



(G-1516) **Fig. P. 5.36.8(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 $2^4 = 16$

Ex. 5.36.9 : Calculate the following for a network address 192. 168. 1. 0/27

(a) Number of valid subnets

(b) Number of actual hosts per subnet

(c) Network and broadcast address for each subnet.

Soln. :

Given : IP address 192.168.1. 0 /27 (Class C)

Step 1 : To find subnet mask :

Address mask is /27 which can be represented as,

11111111 · 11111111 · 11111111 · 11100000

$\therefore$ New subnet mask = 255.255.255.224

Step 2 : To find number of subnets and number of hosts :

The number of subnets are determined by the number of extra is.

$\therefore$ Number of extra 1's = 3

$\therefore$ Number of subnets $= 2^3 = 8$ **...Ans.**

Scanned by CamScanner

The value of n is 27 which means that number of host address is

$$2^{32-n} = 2^{32-27} = 2^5 = 32 \quad \text{...Ans.}$$

Step 3 : Find network address : (G-1744)

	192	168	1	0
IP address :	11000000	10101000	00000001	00000000
	255	255	255	224
Subnet mask :	11111111	11111111	11111111	11100000
	ANDing			
Network address :	11000000	10101000	00000001	11100000
	192	168	1	0

Network address is : 192.168.1.0 ...Ans.

Step 4 : Find broadcast address :

To find broadcast address, take inverted subnet mask and perform XOR with network address. (G-1745)

	192	168	1	0
Network address :	11000000	10101000	00000001	00000000
Inverted subnet mask :	00000000	00000000	00000000	00011111
	XORing			
Broadcast address :	11000000	10101000	00000001	00011111
	192	168	1	31

The broadcast address is : 192.168.1.31 ...Ans.

Ex. 5.36.10 : An ISP is granted a block of addresses starting with 150.80.0.0/16.

The ISP wants to distribute these blocks to 2600 customers as follows :

a. The first group has 200 medium-size businesses ; each needs 128

b. The second group has 400 small businesses ; each needs 16

c. The third group has 2000 households ; each needs 4 addresses. Design the subblocks and give the slash notation for each subblock. Find out how many addresses are still available after these allocations ? **May 16, 10 Marks**

Soln. :

Granted address : 150.80.0.0/16

As n = 16 the total number of available addresses is $2^{32-n} = 2^{16} = 65536$.

The three groups are as follows :

Group 1 :

- For this group each business needs 128 addresses. This means that 7 bits ($\log_2 128 = 7$) are required to define each host. The prefix length is then $32 - 7 = 25$ i.e. $n_1 = 25$.
- The addresses in group-1 are

1st business : 150.80.0.0/25 to 150.80.0.127/25

2nd business : 150.80.0.128/25 to 150.80.0.255/25

.

.

.

200th business : 150.80.99.128/25 to 150.80.99.255/25

Total addresses in group-1 = 200 × 128 = 25600

Group 2 :

- For this group each business needs 16 addresses. Therefore 4 bits ($\log_2 16 = 4$) are required to define each host. The prefix length is then $32 - 4 = 28$. i.e. $n_2 = 28$.
- The addresses in group-2 are

1st business : 150.80.100.0/28 to 150.80.100.15/28

2nd business : 150.80.100.16/28 to 150.80.100.31/28

.

.

.

400th business : 150.80.124.240/28 to 150.80.124.255/28

- Total addresses in group-2 = 400 × 16 = 6400

Group 3 :

- For this group each household needs 4 addresses. Therefore only 2 bits ($\log_2 4 = 2$) are required to define each host.

The prefix length is then $32 - 2 = 30$ i.e. $n_3 = 30$

The addresses of group-3 are

1st household : 150.80.125.0/30 to 150.80.125.3/30

2000th household : 150.80.156.60/30 to 150.80.156.63/30

Total addresses in group-3 = 2000 × 4 = 8000

Number of granted address to ISP = 65, 536

Number of allocated addresses by

ISP = 25600 + 6400 + 8000 = 40,000

Number of available addresses = 65, 536 – 40,000 = 25,536.

Scanned by CamScanner

Ex. 5.36.11 : An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows :

1. The first group has 64 customers ; each needs 256 addresses.
2. The second group has 128 customers ; each needs 128 addresses.
3. The third group has 128 customers ; each needs 64 addresses. Design the sub blocks and find out how many addresses are still available after these allocations. **Dec. 16, 10 Marks**

Soln. :

Group 1 :

Each customer in this group needs 256 addresses i.e. suffix length is 8 ($2^8 = 256$).

∴ Prefix length = 32 – 8 = 24. The addresses are as follows :

Customer	Starting address	Ending address
1.	190.100.0.0/24	190.100.0.255/24
2.	190.100.1.0/24	190.100.1.255/24
3.	190.100.2.0/24	190.100.2.255/24
.		
.		
.		
64	190.100.63.0/24	190.100.63.255/24

Total : 64 × 256 = 16384

Group 2 :

Each customer in this group needs 128 addresses i.e. suffix length is 7 ($2^7 = 128$).

∴ Prefix length = 32 – 7 = 25. The addresses are as follows :

Customer	Starting address	Ending address
1	190.100.64.0/25	190.100.64.127/25
2.	190.100.64.128/25	190.100.64.255/25
.		
.		
.		
128	190.100.127.128/25	190.100.127.255/25

Total : 128 × 128 = 16384

Group 3 :

Each customer in this group needs 64 addresses i.e. suffix length is 6. ($2^6 = 64$).

∴ Prefix length = 32 – 6 = 26. The addresses are as follows :

Customer	Starting address	Ending address
1	190.100.128.0/26	190.100.128.63/26
2.	190.100.128.64/26	190.100.128.127/26
.		
.		
.		
128	190.100.159.192/26	190.100.159.255/26

Total = 128 × 64 = 8192

Number of granted addresses to the ISP = 65536

Number of allocated addresses by the ISP = 40960

Number of available addresses = 65536 – 40960

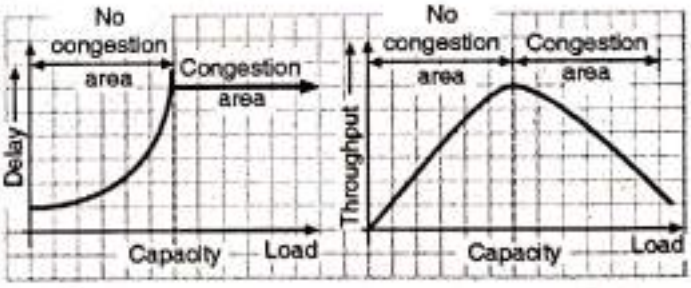
= 24576

5.37 Network Layer Congestion :

- The Internet model does not explicitly deal with the congestion at the network layer. However this study of network layer congestion is very important because it helps us to understand the congestion at the transport layer better.
- It also helps us to find remedies on congestion. The two important network performance issues that are related to the congestion at network layer are :

  1. Throughput and 2. Delay.

- The variation of these performance parameters with respect to load has been shown in Fig. 5.37.1(a) and (b) respectively.



(a) Variation of delay with load **(b) Variation of throughput with load**

(G-2231) **Fig. 5.37.1 : Packet delay and throughput as function of load**

1. Variation of packet delay with load :

- Consider Fig. 5.37.1(a) which shows that packet delay is very small when the load is much less than the capacity of the network. This small delay is only due to the propagation delay and processing delay both of which have very small values.

Scanned by CamScanner

- However as the load increases and reaches close to the network capacity the packet delay increases sharply due to the significant increase in the queuing delay.
- If the load is increased beyond the network capacity, the delay will become infinite, and congestion will result.

2. Variation of throughput with load :

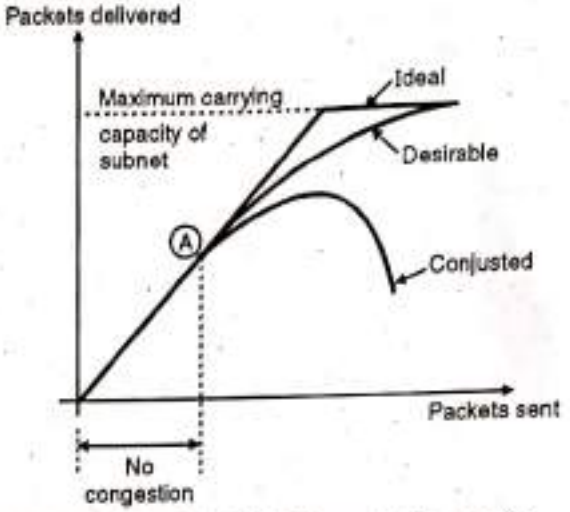
- Now refer Fig. 5.37.1(b) which shows that the throughput increases with increase in load as long as the load is less than the network capacity.
- It is expected that for any load beyond the capacity, the throughput should remain constant. Instead it decreases sharply as the load exceeds the capacity of the network.
- This sharp reduction in throughput results due to discarding of packets by the routers.
- As the load is higher than the capacity, the queues at the routers overflow and some packets must be discarded.
- But packet discarding does not reduce the number of packets present in the network because every discarded packet is retransmitted by its source due to the time out mechanism.
- Therefore increasing the load beyond the capacity results in the congestion of network.

5.37.1 Congestion : MU : Dec. 14

University Questions

Q. 1 Why there is a need for congestion control ? What are the different mechanisms ? Explain them. **(Dec. 14, 10 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. 5.37.1(c) explains the concept of congestion graphically.
- Upto point A in Fig. 5.37.1(c), the number of packets sent into the subnet by the host is within the capacity of the network. So all these packets are delivered. In short the number of packets delivered is proportional to number of packets sent and no congestion takes place.
- But after point A, the traffic increases too far. The routers cannot cope with the increased traffic and they begin to lose packets. The congestion begins here.
- As the traffic increases further, the performance degrades more and more packets are lost and congestion worsens.
- At very high traffic, the performance collapses completely and almost all packets are lost. This is the worst possible congestion.



(G-473) **Fig. 5.37.1(c) : Concept of congestion**

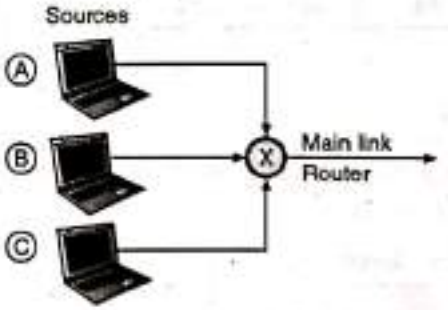
5.37.2 Need of Congestion Control :

- It is not possible to completely avoid the congestion but it is necessary to avoid it otherwise control it.
- Congestion will result in long queues, which results in buffer overflow and loss of packets.
- So congestion control is necessary to ensure that the user gets the negotiated QoS (Quality of Service).

5.37.3 Causes of Congestion :

Some of the causes of congestion are as follows :

1. If suddenly a flow of packets start coming on three or four senders which all needing the same output line. Then a queue will become long. If the memory capacity is not sufficient to hold all these packets, some of them will be lost. This is shown in Fig. 5.37.2(a). This leads to congestion.



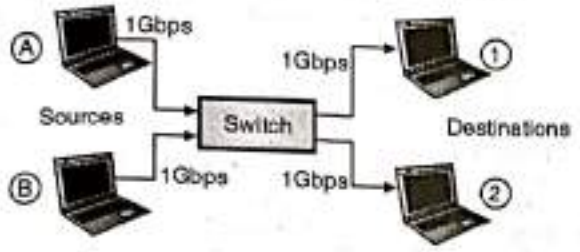
(G-2232) **Fig. 5.37.2(a)**

Note that increasing the memory to infinity also does not solve the problem, in fact it worsens.

2. Congestion is caused by slow and low bandwidth links. The problem will be solved when high speed links become available. It is not always the case, sometimes increases in link bandwidth can aggravate the congestion problem because higher speed links may make the network more unbalanced. For the configuration shown in Fig. 5.37.2(b), if both the sources begin to send to destination 1 at their maximum rate,

Scanned by CamScanner

congestion will occur at the switch. Higher speed links can make the congestion condition in the switch worse.



(G-2233) **Fig. 5.37.2(b) : Network with high speed links**

3. Congestion is caused by slow processors. The problem will be solved when processor speed is improved.

   Faster processors will transmit more data in unit time. If several nodes begin to transmit to one destination simultaneously at their maximum rate, the destination will be overwhelmed soon.

4. Congestion can make itself worse. If a router does not have any free buffers it should ignore (discard) new packets arriving at it. But when a packet is discarded, the sender may retransmit it many times because it is not receiving the acknowledgement of the packet.

   This multiple transmission of packets will force the congestion to take place at the sending end.

5.37.4 Difference between Congestion Control and Flow Control : MU : Dec. 08

University Questions

Q. 1 Compare congestion control and flow control. **(Dec. 08, 10 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.

5.37.5 Principle of Congestion Control :

MU : Dec. 05, Dec. 15, May 16, Dec. 16, Dec. 17, New Syll. : Dec. 18

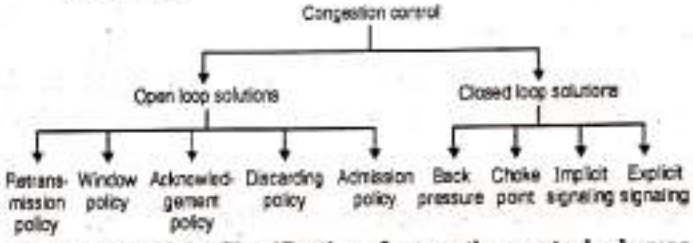
University Questions

Q. 1 Write short notes on : Congestion control. **(Dec. 05, 8 Marks)**

Q. 2 Compare open loop congestion control, closed loop congestion control. **(May 16, Dec. 16, 10 Marks)**

Q. 3 What is congestion control ? Explain various congestion prevention policies. **(Dec. 15, Dec. 17, 10 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. 5.37.3 shows the classification of congestion control schemes and various policies used in open loop and closed loop groups.



(G-476) **Fig. 5.37.3 : 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.

Scanned by CamScanner

Open loop versus closed loop :

- Open loop approaches do not need end-to-end feedback, one of the examples of this type are prior-reservation and hop-to-hop flow control.
- In closed-loop approaches, the source can adjust its cell rate on the basis of the feedback information received from the network.
- Some people feel that closed loop congestion control schemes are too slow in 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.

5.37.6 Congestion Prevention Policies :

MU : May 12, Dec. 12, Dec. 15, May 17, Dec. 17

University Questions

Q. 1 List the design features to be taken care of as congestion prevention policies in the different layers of network. **(May 12, 10 Marks)**

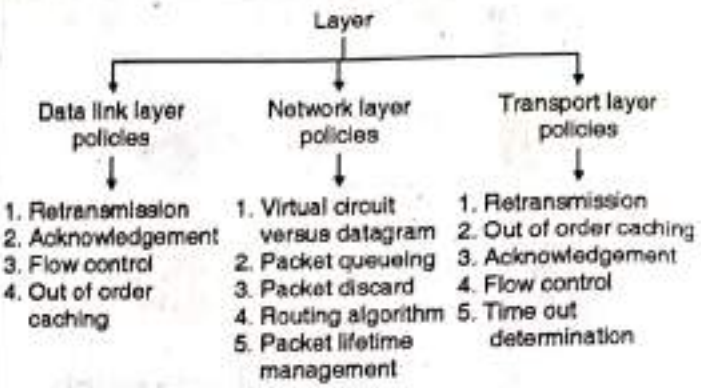
Q. 2 What are the congestion prevention policies ? Explain the congestion control in virtual circuit and datagram subnets. **(Dec. 12, 10 Marks)**

Q. 3 What is traffic shaping ? Explain leaky bucket algorithm and compare it with token bucket algorithm. **(Dec. 15, 10 Marks)**

Q. 4 What is congestion control ? Explain various congestion prevention policies. **(Dec. 15, Dec. 17, 10 Marks)**

Q. 5 What are congestion prevention policies ? Explain congestion control in virtual circuit and datagram subnets. **(May 17, 10 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. 5.37.4 lists various policies corresponding to different layers for avoiding congestion.



(G-477) **Fig. 5.37.4 : 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.

Scanned by CamScanner

2. **Packet queuing and service :**
   - This policy is related to whether the routers have one queue per input line and one queue per output line or both.
   - This policy is also related to the order in which the packets are processed e.g. round robin or priority based etc.

3. **Discard policy :**
   - This policy lays a rule which tells the routers about which packet is to be discarded.
   - A good discard policy can prevent congestion and a bad one will worsen the situation.

4. **Routing algorithms :**

   The routing algorithms can spread the traffic over all the lines. By doing so it is ensured that none of the lines are overloaded. This will certainly avoid congestion.

5. **Package lifetime management :**
   - This policy decides the maximum time for which a packet may live before being discarded.
   - This time should be of adequate value so that congestion can be avoided.

Policies related to transport layer :

- The policies at the transport layer are same as those at the data link layer.
- But at transport layer determining the time out interval is more difficult.
- If it is too short then extra packets are sent unnecessarily whereas if it is too long, congestion will reduce at the cost of increased response time (network will become slow).

Traffic shaping :

- One of the important reason behind congestion is the bursty nature of the traffic. If the traffic has a uniform data rate then congestion would not happen every now and then. But due to bursty traffic it can happen regularly.
- Traffic shaping is an open loop control. It prevents the congestion by making the packet transmission rate to be more predictable (bursty traffic is unpredictable).
- Thus traffic shaping will regulate the average rate or the burstiness of data transmission.
- Monitoring a traffic flow is called as **traffic policing**.
- Check if a packet stream (connection) is as per its descriptor, and if it is not as per its descriptor, then give penalty !
- In order to achieve this the network may want to monitor the traffic flow during the connection period. The process of monitoring and enforcing the traffic flow is called traffic policing.
- The types of penalties enforced are as follows :
  1. Drop packets that violate the descriptor.
  2. Give low priority to the packets violating the descriptor.

5.37.7 Congestion Control in Virtual Circuit Subnets : MU : May 12, Dec. 12, May 17

University Questions

Q. 1 Compare virtual circuits and datagram subnets and show their diagrammatic representation during congestion control. **(May 12, 10 Marks)**

Q. 2 What are the congestion prevention policies ? Explain the congestion control in virtual circuit and datagram subnets. **(Dec. 12, 10 Marks)**

Q. 3 What are congestion prevention policies ? Explain congestion control in virtual circuit and datagram subnets. **(May 17, 10 Marks)**

- All the congestion control techniques discussed till now were open loop techniques.
- Now let us discuss a dynamic technique called **admission control.**

Admission control principle :

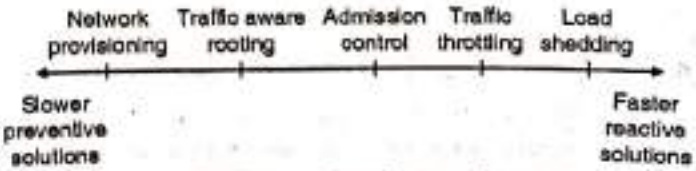
- This technique is used to keep the congestion which has already begun to a manageable level and does not allow it to worsen any further.
- Its principle is as follows : Once congestion has been detected, do not set up any more virtual circuits until the congestion is cleared.
- The advantage of this technique is that it is a simple and easy to carry out control.

Alternative approach :

- An alternative approach to admission control allows the virtual circuits to set up even when a congestion has taken place.
- But carefully route all the new virtual circuits around the area where congestion is already present.

5.37.8 Approaches to Congestion Control :

- The two basic solutions to the problem of congestion are :
  1. Increase the resources 2. Decrease the load
- These solutions are applied on different time scales in order to either prevent congestion or handle it if it has occurred.



(G-1522) **Fig. 5.37.5 : Time scales of approaches to congestion control**

Scanned by CamScanner

1. **Network provisioning :**
   - The fundamental way of avoiding congestion is to build a network that is properly matched to the traffic that it is going to carry.
   - If the network uses a low bandwidth link along which a heavy traffic is directed, then congestion is most certain to take place.
   - We can add resources dynamically when there is congestion. For example, we can turn on additional routers and use spare (back up) lines whenever congestion has taken place.
   - Another example is purchasing bandwidth on open market as and when congestion occurs. But you can't do it instantly. It takes a long time.
   - This is called as **Network Provisioning.** It is a slow preventive solution and happens on a time scale of months.
2. **Traffic aware routing :**
   - If we can not increase the capacity of a network then we should think of utilizing the existing capacity in the best possible why.
   - Routers can be tailored to suite traffic patterns that change during the day as network users wake and sleep in different time zones.
   - The traffic can be routed over those paths which have less traffic at that time. This is known as traffic aware routing.
3. **Admission control :**
   - Sometimes it is not possible to increase capacity. Then the only possible way to fight congestion is to **decrease the load.**
   - As stated earlier, in the virtual circuit networks, new connections are not allowed once congestion has been detected.
   - This is a feedback (closed loop) control approach. When the congestion is predicted, the network can deliver feedback to those sources who are responsible for congestion.
   - Then these sources would be requested to **reduce** their outputs.
   - There are two difficulties faced in this approach :
     1. It is difficult detect the of beginning of congestion.
     2. It is also difficult to inform the sources to slow down accordingly.
   - The **leaky bucket** and **token bucket** methods are examples of admission control.
4. **Traffic throttling (Congestion avoidance) :**
   - In the Internet and many other computer networks, senders adjust their transmission rates and send only that much traffic which a network can readily deliver without causing congestion.
   - This is done so as to operates the network just before the beginning point of congestion.
   - When congestion is about to happen the senders should be told to **reduce** their transmission and slow down. This technique is an example of **congestion avoidance** principle.
   - The first step in traffic throttling is to **detect** the beginning point of congestion and the second step is to tell the senders to slow down.
   - Note that traffic throttling approach can be used in both datagram **subnets** as well as **virtual circuit subnets.**
   - The onset of congestion can be detected if the routers are made to monitor the following parameters :
     1. Utilization of output links.
     2. Buffering of queued packets inside the router.
     3. Number of packets lost due to inadequate buffering.
   - Generally the second parameter is most useful in practice.
   - The second task for the routers is that they should deliver timely feedback to the senders. Different schemes use different feedback mechanisms. Some of them are as follows :
     1. Choke packets.
     2. Explicit Congestion Notification (ECN).
     3. Hop by Hop back pressure.
5. **Load shedding :**
   - When all other solutions fail to contain congestion, the network has no option but to discard packets that can not be delivered.
   - A good policy for selecting which packets to discard can help preventing the congestion collapse.

5.37.9 Congestion Control in Datagram Subnets :

MU : Dec. 04, May 12, Dec. 12, Dec. 13, Dec. 14, May 17

University Questions

Q. 1 Give one approach of congestion control in datagram subnets. **(Dec. 04, 10 Marks)**

Q. 2 Compare virtual circuits and datagram subnets and show their diagrammatic representation during congestion control. **(May 12, 10 Marks)**

Q. 3 What are the congestion prevention policies ? Explain the congestion control in virtual circuit and datagram subnets. **(Dec. 12, 10 Marks)**

Q. 4 Explain the various methods for congestion control used in datagram subnets. **(Dec. 13, 10 Marks)**

Scanned by CamScanner

Q. 5 Why there is a need for congestion control ? What are the different mechanisms ? Explain them.

(Dec. 14, 10 Marks)

Q. 6 What are congestion prevention policies ? Explain congestion control in virtual circuit and datagram subnets.

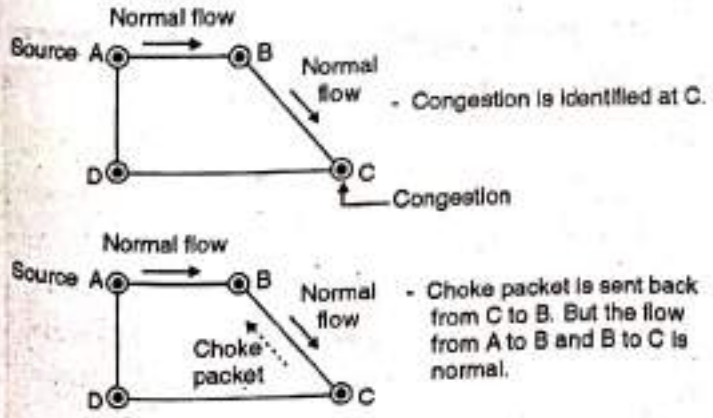
(May 17, 10 Marks)

- Let us now discuss some congestion control approaches which can be used in the datagram subnets (and also in virtual circuit subnets).
- The techniques are :

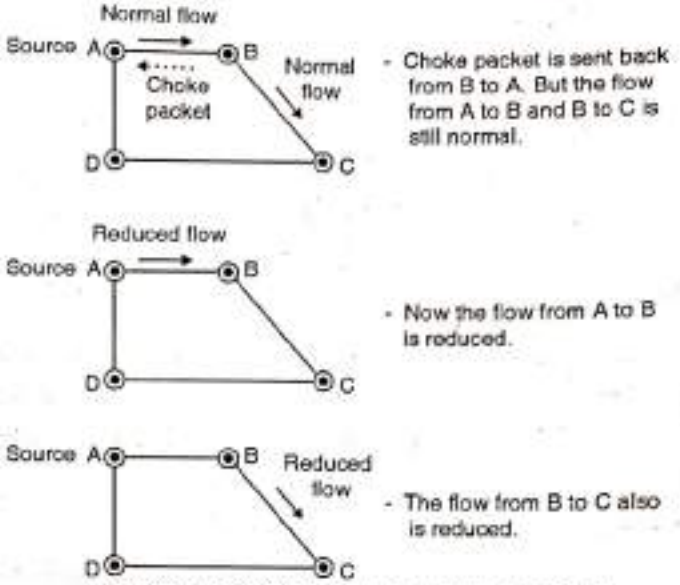
  1. Choke packets 2. Load shedding 3. Jitter control.

1. Choke packets :

- This approach can be used in virtual circuits as well as in the datagram subnets.
- In this technique each router associates a real variable with each of its output lines. This real variable say "u" has a value between 0 and 1 and it indicates the how much is utilization of that line in percentage (60 %, 70 % etc.).
- If the value of "u" goes above the threshold then that output line will enter into a "warning" state. The router will check each newly arriving packet to see if its output line is in the "warning state".
- If it is in the warning state then the router will send back a **choke packet** signal to the sending host.
- The sender host will not generate any more data packets. This will reduce the congestion.
- Different congestion control algorithm have been proposed, depending on the value of thresholds.
- Depending on the threshold value, the choke packets can contain a mild warning, a stern warning or an ultimatum.
- Another algorithm may use the queue lengths or buffer utilization instead of using the line utilization as a deciding factor.
- The general concept of choke packet mechanism is demonstrated in Fig. 5.37.6(a).



(G-478) **Fig. 5.37.6(a)(Contd...)**

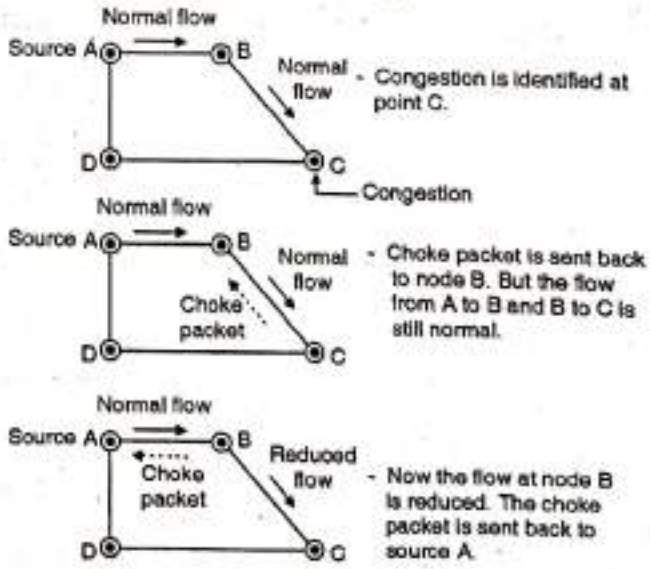


(G-478) **Fig. 5.37.6(a) : Choke packet mechanism**

- Fig. 5.37.6(a) shows that, the choke packets have to travel over the entire network, from the point of congestion to the appropriate source (i.e. from C to A).
- Then the action of reducing the flow will take place. The whole process is therefore very much time consuming.

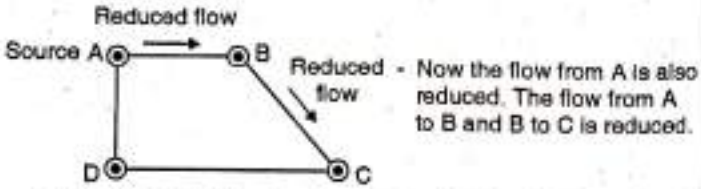
Hop-by-Hop choke packet technique :

- The problem associated with the general choke packet mechanism can be overcome by using another technique called as hop-by-hop choke packet technique.
- This is demonstrated in Fig. 5.37.6(b). In this approach, the choke packets are used at each hop between the destination and source.
- Each node receiving the choke packet will reduce its output flow. This will have a more effective and fast control over the overall transmission rate.
- Fig. 5.37.6(b) shows how the transmission rate is reduced at every hop in response to the choke packets.



(G-479) **Fig. 5.37.6(b)(Contd...)**

Scanned by CamScanner



(G-479) **Fig. 5.37.6(b) : Concept of hop-by-hop choke packet mechanism**

Disadvantage :

The problem with choke packet technique is that the action to be taken by the source host on receiving a choke packet is not compulsory. The host may reduce its transmission rate or ignore the choke packets.

Weighted fair queuing :

- The disadvantage of choke packet technique can be overcome with the help of the weighted queuing technique.
- The queuing algorithm was proposed first in 1987. In this algorithm it is proposed that the routers have a number of queues for each output line, with one queue for each source.

2. Load shedding :

- Admission control, choke packets, fair queuing are the techniques suitable for light congestion.
- But if these techniques cannot eliminate the congestion, then the load shedding technique is to be used.
- The principle of load shedding states that when the routers are flooded with the packets that they cannot handle, they should simply throw the packets away.
- A router which is flooding with packets due to congestion can discard any packet at random. But there are better ways of doing this.
- The policy for dropping a packet depends on the type of packet.
- For file transfer an old packet is more important than a new packet. In contrast for multimedia a new packet is more important than an old one. Accordingly a policy is formulated for discarding the packets.
- An intelligent discard policy can be decided depending on the applications.
- It is not possible to implement such an intelligent discard policy without the, co-operation from the sender. The applications should mark their packets as per priority to indicate how important they are.
- If this is done then when the packets are to be discarded the routers can first drop packets having lower priority (i.e. the packets which are least important).
- Then the routers will discard the packets from next lower class and so on.
- One or more header bits are required to put the priority of a packet.
- In every ATM cell, 1 bit is reserved in the header for marking the priority. Every ATM cell is labeled either as a low priority or high priority.

3. Jitter Control : **MU : Dec. 13**

University Questions

Q. 1 Explain the various methods for congestion control used in datagram subnets. **(Dec. 13, 10 Marks)**

Definition :

- The delay introduced by the data communication networks is not constant. It varies packet to packet. The jitter measures the variability in packet delays and it is measured in terms of the difference of the minimum delay and maximum value of delay.
- Jitter is defined as the variation in delay for the packets belonging to the same flow.
- The real time audio and video cannot tolerate jitter on the other hand the jitter does not matter if the packets are carrying any data information contained in a file.
- For the audio and video transmission if the packets take 20 msec to 30 msec (delay) to reach the destination, it does not matter, provided that the delay remains constant.
- The quality of sound or video will be hampered if the delays associated with different packets have different values.

Jitter control :

- When a packet arrives at a router, the router will check to see whether the packet is behind or ahead and by what time.
- This information is stored in the packet and updated at every hop.
- If the packet is ahead of the schedule (early) then the router will hold it for a slightly longer time and if the packet is behind the schedule (late), then the router will try to send it out as quickly as possible.
- This will help in keeping the average delay per packet constant and will avoid time jitter.

5.38 Quality of Service (QoS) :

MU : May 10, Dec. 10, May 11, May 13, Dec. 13

University Questions

Q. 1 Write short notes on : Quality of Service (QoS) of Internetworking. **(May 10, May 11, 5 Marks)**

Q. 2 Discuss the quality of service requirements for audio on demand. **(Dec. 10, 5 Marks)**

Q. 3 Explain the different factors associated with quality of service in Internetwork. **(May 13, 10 Marks)**

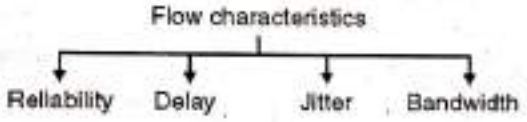
Q. 4 Write short notes on : QoS requirements. **(Dec. 13, 10 Marks)**

Scanned by CamScanner

The long form of QoS is quality of service and it is an internetworking issue. We can informally define quality of service as something flow seeks to attain.

Flow characteristics :

- There are four important characteristics of data flow : reliability, delay, jitter and bandwidth.
- These characteristics are shown in Fig. 5.38.1.



(G-480) **Fig. 5.38.1 : 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.

5.38.1 Techniques for Achieving Good QoS :

- Some of the techniques useful in achieving good QoS are as follows :
  1. Buffering
  2. Traffic shaping
  3. Leaky bucket algorithm
  4. Token bucket algorithm
  5. Resource reservation
  6. Admission control
  7. Proportional routing
  8. Packet scheduling.

5.38.2 Traffic Shaping :

MU : Dec. 15, New Syll. : Dec. 18

University Questions

Q. 1 What is traffic shaping ? Explain leaky bucket algorithm and compare it with token bucket algorithm. **(Dec. 15, 10 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 :
  1. Drop packets that violate the rules.
  2. Give low priority to them.
- **Traffic shaping** is defined as a mechanism to control the amount and rate of the traffic sent to the network.
- The two popularly used traffic shaping techniques are :
  1. Leaky bucket
  2. Token bucket.

5.38.3 Leaky Bucket Algorithm :

MU : Dec. 06, May 09, May 10, Dec. 15, New Syll. : Dec. 18

University Questions

Q. 1 Explain leaky bucket algorithm in detail. Also explain advantages and disadvantages of same compared with token bucket algorithm. **(Dec. 06, May 09, 10 Marks)**

Q. 2 Explain the working of leaky bucket algorithm. Why leaky bucket algorithm is used in Computer Network. **(May 10, 10 Marks)**

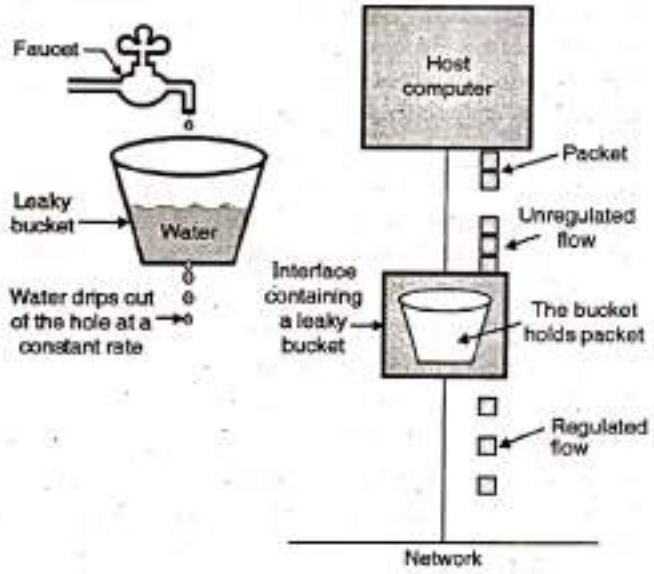
Q. 3 What is traffic shaping ? Explain leaky bucket algorithm and compare it with token bucket algorithm. **(Dec. 15, 10 Marks)**

- 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.

Scanned by CamScanner

- 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. 5.38.2 the data flow at the input of the bucket is unregulated but that at the bucket output is a regulated one.

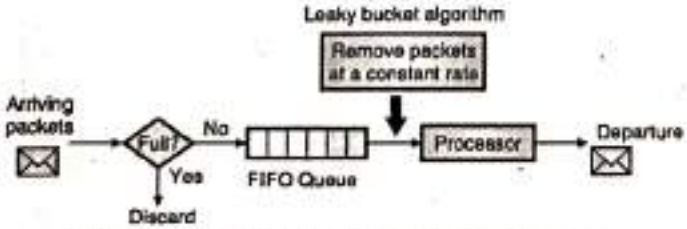


(a) (b)

(G-481) **Fig. 5.38.2 : Leaky bucket algorithm**

Leaky bucket implementation :

- Fig. 5.38.3 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. 5.38.3 can be discussed under two different operating conditions, namely :
  1. For packets of fixed size.
  2. For packets of variable size.



(G-482) **Fig. 5.38.3 : 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. 5.38.3 will allow the removal of a fixed number of packets from the queue corresponding to every tick of the clock.

2. **Packets of variable size :**

   If the packets at the input of the process are of different size, then the fixed output rate will not correspond to the number of packets leaving the process but it will correspond to the number of bits leaving the process.

Algorithm :

The algorithm for variable length packets is as follows :

1. Initialize a counter to a number "n" at the tick of the clock.
2. If "n" is greater than the packet size, then send the packet and decrement the counter by the packet size.
3. Repeat step 2 until "n" becomes smaller than the packet size.
4. Reset the counter and go back to step 1.

Note : Thus a leaky bucket algorithm shapes the bursty traffic to convert it into a fixed rate traffic. It does so by averaging the data rate. It drops the packets if the bucket (buffer) is full.

5.38.4 Token Bucket Algorithm :

MU : Dec. 10, May 15, Dec. 15, Dec. 17

University Questions

Q. 1 How does the token bucket algorithm works ? **(Dec. 10, 5 Marks)**

Q. 2 How does the Token Bucket Algorithm works ? **(May 15, 4 Marks)**

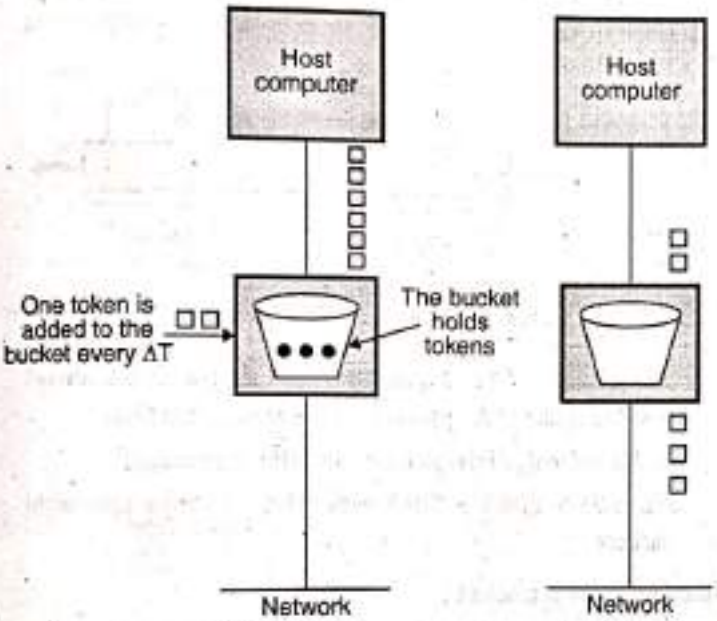
Q. 3 What is traffic shaping ? Explain leaky bucket algorithm and compare it with token bucket algorithm. **(Dec. 15, 10 Marks)**

Q. 4 How does the token Bucket algorithm work ? **(Dec. 17, 5 Marks)**

- This algorithm is similar to the leaky bucket but it is possible to vary output rates. This is useful when larger burst of traffic is received.

Scanned by CamScanner

- It enforces a long-term average transmission rate while permitting bounded bursts. In this approach, a token bucket is used to which manages the queue regulator that ultimately controls the rate of packet flow into the network.
- A token generator continuously produces tokens at a rate of R tokens per second and puts them into a token bucket with a depth of D tokens as shown in Fig. 5.38.4. If the token bucket gets full then the extra tokens are discarded.



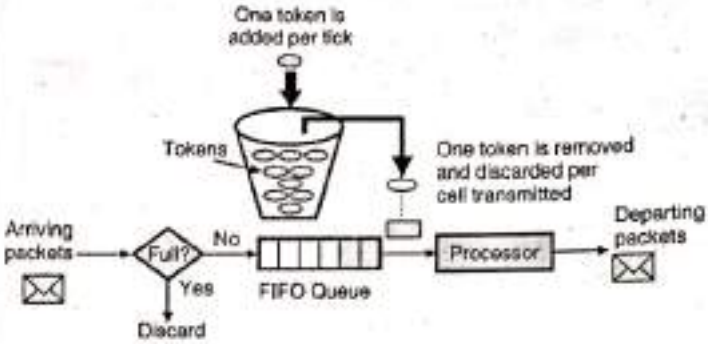
(a) Before (b) After

(G-483) **Fig. 5.38.4 : Token bucket algorithm**

- Token bucket algorithm is a variant of leaky bucket algorithm discussed earlier. Here the bucket is filled with tokens.
- A packet which grabs and distroies 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. 5.38.5 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-484) **Fig. 5.38.5 : Implementation of token bucket**

Note : The token bucket allows the bursty traffic at maximum possible rate.

Token bucket performance :

Let, s = Burst length (seconds),

c = Bucket capacity (bytes),

ρ = Token arrival rate (bytes/second),

and m = Maximum source rate (bytes/second)

What is the duration of a maximum-rate burst through a token bucket ?

1. Maximum bytes sent from the token bucket during a burst is, $c + \rho \cdot s$
2. Maximum bytes the source can send during a burst is, $m \cdot s$
3. Setting the two equal and solving for s,

$$s = \frac{c}{m - \rho}$$

Ex. 5.38.1 : 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 ?

Soln. :

Given : C = Bucket capacity = 8 M bits

m = Maximum output rate = 6 Mbps

ρ = Token arrival rate = 1 Mbps

To find : S = Time for which maximum output is obtained.

$$S = \frac{c}{m - \rho}$$

$$\therefore \quad S = \frac{8 \text{ M bits}}{6 \text{ Mbps} - 1 \text{ Mbps}}$$

$$= \frac{8}{5} = 1.6 \text{ sec}$$

So the computer can transmit at the full 6 Mbps for 1.6 seconds.

Scanned by CamScanner

5.38.5 Comparison of Token Bucket and Leaky Bucket :

MU : Dec. 15, New Syll. : Dec. 18

University Questions

Q. 1 What is traffic shaping ? Explain leaky bucket algorithm and compare it with token bucket algorithm. **(Dec. 15, 10 Marks)**

Table : 5.38.1 : Comparison of Token Bucket and Leaky Bucket

Sr. No.	Leaky Bucket	Token Bucket
1.	Smooth out traffic by passing packets only when there is a token. Does not permit burstiness.	Token bucket smooths traffic too but permits bustiness.
2.	Leaky bucket discards packets for which no tokens are available. (No concept of queue)	Token bucket discards token when bucket is full, but never discards packets (infinite queue)
3.	Application : Traffic shaping or traffic policing.	Application : Network traffic shaping or rate limiting

5.38.6 Combination of Token Bucket and Leaky Bucket :

- The token bucket and leaky bucket techniques can be combined to obtain the following advantages :
  1. To credit an idle host 2. To regulate the traffic
- The token bucket is used first followed by the leaky bucket technique. The rate of leaky bucket needs to be higher than the rate of tokens dropped in the bucket.

5.38.7 Resource Reservation :

- The data flow is dependent on the following resources :
  1. Buffer 2. Bandwidth 3. CPU time
- The QoS can be improved by reserving these resources. The QoS model called integrated services operates on the principle of resource reservation, for improvement in QoS.

5.38.8 Admission Control :

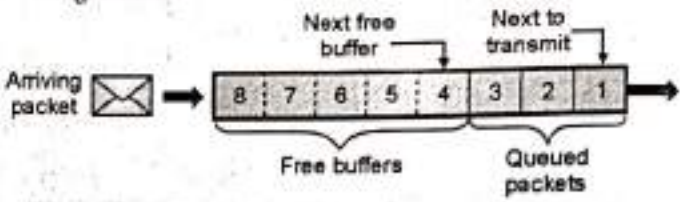
- Admission control technique is used by a router or a switch. They use this mechanism to accept or reject the data flow based on predefined parameters called flow specifications.
- Before accepting a flow for processing, a router checks the flow specifications and finds out if it is possible to take up and handle this new data flow.
- It does this by comparing its bandwidth, buffer size, CPU speed etc. with the flow specifications.

5.38.9 Queuing Disciplines :

- Each router must implement some queuing discipline which decides about how the packets are buffered when they are waiting to get transmitted.
- There are two algorithms commonly used in packet switching networks namely :
  1. First In First Out (FIFO) 2. Fair Queuing (FQ)

5.38.10 FIFO Queuing :

- The FIFO queuing is also called as First Come First Served (FCFS) Queuing. Its idea is simple and illustrated in Fig. 5.38.6.

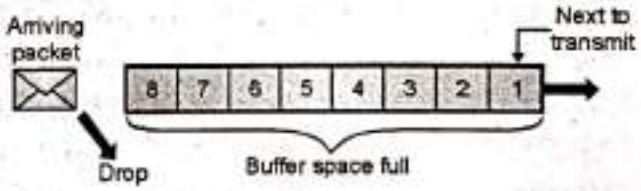


(G-485) **Fig. 5.38.6 : FIFO queuing**

- The principle of FIFO queuing is, that the packet that arrives first at a router is the packet which is transmitted first.
- In this sense it is First In First Out (FIFO) queuing.
- Fig. 5.38.6 shows a FIFO with "slots" to store upto eight packets.

Discarding of a packet :

- The buffer space at any router is limited. So if a packet arrives when the queue (buffer space) is full, then the router discards that packet as shown in Fig. 5.38.7.



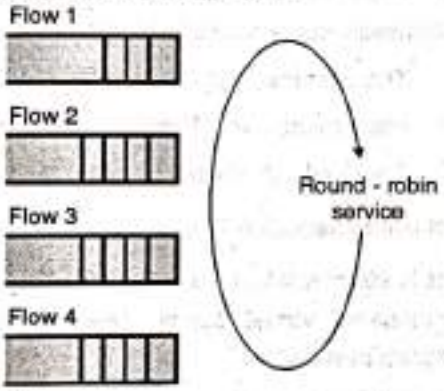
(G-486) **Fig. 5.38.7 : Dropping of a packet**

- The packet is dropped (discarded) irrespective of which flow the packet belongs to or what is its priority level etc.
- This is sometimes called as "tail drop" because packets which arrive at the tail end of the FIFO are dropped.
- FIFO with tail drop, is the simplest queuing algorithm and so it is the most widely used one.
- A simple types of the basic FIFO queuing is priority queuing.
- In this each packet is marked with a priority.
- The router then implements multiple FIFO queues, one for each priority class.
- The router will always transmit out packets of highest priority queues if that queue is non-empty, then it moves to the next priority queue.

Scanned by CamScanner

5.38.11 Fair Queuing :

- The disadvantage of FIFO queuing is that there is absolutely no discrimination among the packets being received from different sources. All are treated equally.
- Because the entire congestion control mechanism is implemented at the sources and the FIFO queuing does not have any facility of policing the source behaviour to this mechanism, it is possible that a bad behaved source may occupy large fraction of the network capacity.
- Fair Queuing (FQ) is an algorithm which is proposed to solve this problem. It maintains a separate queue for each flow which is being currently handled by the router.
- The router then entertains these queues in the round robin manner as shown in Fig. 5.38.8.
- When a sender sends packets too fast, then its queue is filled up. When a queue reaches a particular length, additional packets from that flow are dropped.



(G-487) **Fig. 5.38.8 : Concept of fair Queuing (FQ) at the router**

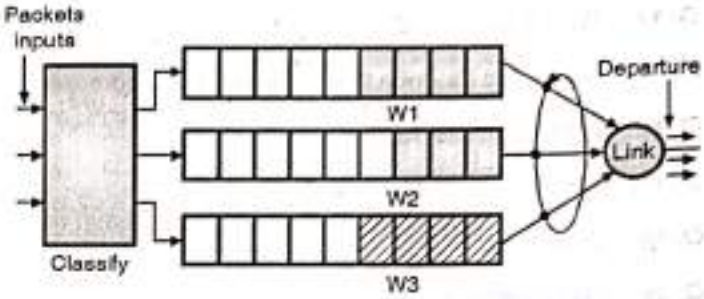
- This ensures that any source can not arbitrarily increase its share of the network's capacity.
- The main problem with FQ is that the packets being processed at a router are not of same length.
- Ideally a bit by bit round robin is expected i.e. one bit from flow-1 is transmitted, then one bit from flow-2 and so on. But practically it is not possible.
- The FQ mechanism therefore simulates this behaviour by first determining when a given packet would finish being transmitted if it were being sent using bit by bit round robin, and then using this finishing time to sequence the packets for transmission.

Disadvantages of fair queuing algorithm :

- The problem with this algorithm is that it gives all the hosts the same priority.
- To overcome this problem, the modified algorithm called weighted fair queuing is used.

5.38.12 Weighted Fair Queuing :

- The disadvantage of choke packet technique can be overcome with the help of the Weighted Fair Queuing (WFQ) technique.
- This queuing algorithm was proposed first in 1987. In this algorithm it is proposed that the routers have a number of queues for each output line, with one queue for each source.
- Refer Fig. 5.38.9 to understand weighted fair queuing.



(G-488) **Fig. 5.38.9 : Weighted fair queuing (WFQ)**

- The incoming packets are classified into different classes (1, 2, 3 etc) and stored in separate queues (W1, W2, W3 etc.) specifically assigned to them.
- Similar to the round robin technique the WFQ scheduler, will output the packets from W1, W2, and W3 in a sequential manner.
- If a queue is empty the WFQ scheduler will move immediately to the next queue. It will always keep the link busy. No empty slots are present on the link.

Difference between round robin and WFQ :

In round robin the service given to each class is same but in WFQ, each class may receive a different amount of service in any interval of time, depending on the weightage of that class.

Review Questions

Q. 1 Explain the connection oriented and connectionless services.

Q. 2 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.

Q. 3 What is fragmentation ?

Q. 4 Write short notes on : Hierarchical routing.

Q. 5 Write short notes on : Multicast routing.

Q. 6 Name different protocols in the network layer.

Q. 7 Write a note on IP.

Q. 8 Explain fragmentation in IP.

Q. 9 What is the name of a packet in IP ?

Q. 10 Explain the IP header.

Scanned by CamScanner

Q. 11 What is MTU and how is fragmentation related to it ?

Q. 12 Compare IPv4 and IPv6.

Q. 13 State limitations of IPv4.

Q. 14 Write a note on ICMP.

Q. 15 Name and describe three types of IPv6 addresses.

Q. 16 What is unicast routing ?

Q. 17 What is multicast routing ?

Q. 18 Explain IGMP.

Q. 19 Write a note on mobile IP.

Q. 20 What is fragmentation ? Explain how is it supported in IPv4 and IPv6.

Q. 21 Explain the addressing scheme in IPv4 and IPv6. When IPv6 protocol is introduced, does the ARP protocol have to be changed ? Explain.

Q. 22 What is fragmentation ? Explain how it is supported in IPv4 and IPv6.

Q. 23 Given an IP address, how will you extract its net id and host id.

Q. 24 What is subnetting in IP network, explain with suitable examples.

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 is the first fragment ? Explain your answer.

Q. 27 Write short note on : Network layer congestion.

Q. 28 State the difference between multiple unicasting and multicasting.

Q. 29 Explain the connection oriented and connectionless services.

Q. 30 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 ?

Q. 31 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 ?

Q. 32 Why leaky bucket algorithm should allow only 1 packet tick independent of how large the packet is ?

Q. 33 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 ?

Q. 34 What is firewall ? What is difference between packet filtering firewall and proxy server gateways ?

Q. 35 What is fragmentation ?

Q. 36 Write a short note on leaky bucket algorithm.

Q. 37 Write a short note on Congestion control.

Q. 38 Enlist and discuss various design layer issues.

Q. 39 A message is broken up into three pieces. Discuss the transmission of packets using :

1. The datagram approach to packet switching.
2. Permanent virtual circuit.
3. Switched virtual circuit.

Q. 40 What is fragmentation ?

Q. 41 What is fragmentation ? Is fragmentation needed in concatenated virtual circuit internets, or only in datagram system ?

Q. 42 Write short notes on Hierarchical routing.

Q. 43 Give an efficient algorithm for finding the shortest paths between all pairs of nodes in a tree. What is the complexity of the algorithm ?

Q. 44 Write short notes on Tunneling.

Q. 45 What is the difference between flow control and congestion control ?

Q. 46 What is the difference between end to end delay and packet Jitter ? What are the causes of packet Jitter ?

Q. 47 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 ?

Q. 48 What is transparent and non transparent fragmentation ? Is fragmentation needed in concatenated virtual circuit internets or only in datagram systems ?

Scanned by CamScanner

Q. 49 Write short note on congestion prevention policies.

Q. 50 Write short note on multicast routing.

Q. 51 What is fragmentation ?

Q. 52 Discuss the various causes of congestion in subnet.

Q. 53 Write a short note on leaky bucket algorithm.

Q. 54 Give an argument why the leaky bucket algorithm should allow just one packet per tick, independent of how large the packet is.

Q. 55 Write short note on Jitter control.

Q. 56 Whether the network layer should provide a connection oriented service or connectionless service ? Explain with suitable example.

Q. 57 Write short note on Network design issues.

Q. 58 What is the difference between congestion control and flow control ?

Q. 59 Name different protocols in the network layer.

Q. 60 Explain the purpose of ARP.

Q. 61 Why is ARP request broadcast but ARP reply unicast ?

Q. 62 Write a note on IP.

Q. 63 Explain fragmentation in IP.

Q. 64 What is the name of a packet in IP ?

Q. 65 Explain the IP header.

Q. 66 What is MTU and how is fragmentation related to it ?

Q. 67 Compare IPv4 and IPv6.

Q. 68 State limitations of IPv4.

Q. 69 Write a note on ICMP.

Q. 70 Name and describe three types of IPv6 addresses.

Q. 71 What is unicast routing ?

Q. 72 Write a note on RIP.

Q. 73 What is multicast routing ?

Q. 74 Explain IGMP.

Q. 75 Write a note on mobile IP.

Q. 76 What is fragmentation ? Explain how is it supported in IPv4 and IPv6.

Q. 77 Explain the addressing scheme in IPv4 and IPv6. When IPv6 protocol is introduced, does the ARP protocol have to be changed ? Explain.

Q. 78 What is fragmentation ? Explain how it is supported in IPv4 and IPv6.

Q. 79 Given an IP address, how will you extract its net id and host id.

Q. 80 What is PING utility ? How many ways are there to implement PING ? Explain steps.

Q. 81 What is subnetting in IP network, explain with suitable examples.

Q. 82 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. 83 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. 84 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 is the first fragment ? Explain your answer.

Q. 85 Write short note on Jitter control.

Q. 86 Whether the network layer should provide a connection oriented service or connectionless service ? Explain with suitable example.

Q. 87 Write short note on Network design issues.

Q. 88 What is the difference between congestion control and flow control ?

5.39 University Questions and Answers :

Q. 1 Explain the following with examples : MAC address, IP address, Latency. **(Dec. 2012, 10 Marks)**

Ans. :

For MAC address, IP address, refer sections 5.23.1 and 5.9.1.

Latency (Delay) :

- The latency or delay defines how long it takes for an entire message to reach its destination from the instant at which the first bit is sent out from the source.

Scanned by CamScanner

- Latency is made of four components.
  1. Processing delay
  2. Queueing delay
  3. Transmission delay
  4. Propagation delay.
- The sum of all these delays amounts to the total nodal delay.

∴ Latency = Propagation delay + Transmission delay + Queueing time + Processing delay

Q. 2 Explain IPv4 header format in detail. If value at HLEN field is 1101 find the size of option and padding field ? **(Dec. 2015, 10 Marks)**

Ans. :

Please refer Section 5.13.4 for IPv4 header format.

Total length of the IP header = HLEN contents × 4 bytes

= 13 × 4 = 52 bytes.

Number of bytes corresponding to all the fields except the option + padding is 20 bytes.

∴ Size of option + padding field = 52 – 20 = 32 bytes ...Ans.

5.40 University Questions and Answers (New Syllabus) :

Dec. 2018 [Total Marks : 68]

Q. 1 Explain with examples the classification of IPv4 addresses. **(Section 5.9.1)** **(4 Marks)**

Q. 2 Explain the need of subnet mask in subnetting. **(Section 5.9.10)** **(4 Marks)**

Q. 3 What is IPv4 protocol ? Explain the IPv4 header format with diagram.

(Sections 5.13.2 and 5.13.4) **(10 Marks)**

Q. 4 What is traffic shaping ? Explain leaky bucket algorithm and compare it with token bucket algorithm.

(Sections 5.38.2, 5.38.3 and 5.38.5) **(10 Marks)**

Q. 5 What is ICMP protocol ? Explain the ICMP header format with diagram.

(Sections 5.26 and 5.26.3) **(10 Marks)**

Q. 6 Compare open loop congestion control and closed loop congestion control.

(Section 5.37.5) **(10 Marks)**

Q. 7 Write a short note on the following :

(a) Distance Vector Routing

(Section 5.21.1) **(10 Marks)**

(b) ARP / RARP

(Sections 5.24 and 5.25.1) **(10 Marks)**

❑❑❑

Scanned by CamScanner

CHAPTER 6

Module 5

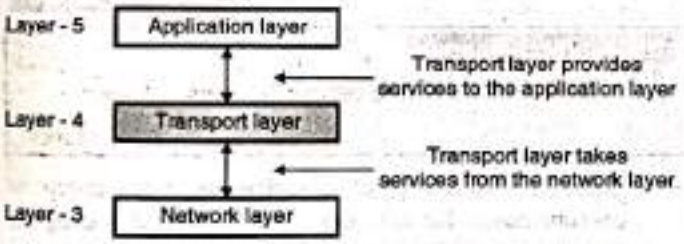
Transport Layer

Syllabus :

The transport service : Transport service primitives, Berkeley sockets, Connection management (Handshakes), UDP, TCP, TCP state transition, TCP timers, TCP flow contraol (sliding window), TCP congestion control : Slow start.

6.1 Introduction :

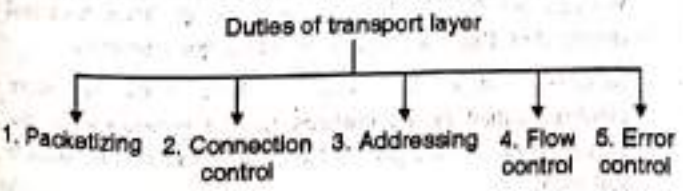
- The transport layer is the core of the Internet model. The application layer programs interact with each other using the services of the transport layer.
- Transport layer provides services to the application layer and takes services from the network layer.
- Fig. 6.1.1 shows the position of the transport 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-592) **Fig. 6.1.1 : Position of transport layer**

6.2 Transport Layer Duties and Functionalities :

- 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.



(G-1407) **Fig. 6.2.1 : Duties of transport layer**

1. Packetizing :

- The transport layer creates packets with the help of encapsulation on the messages received from the application layer. Packetizing is a process of dividing a long message into smaller ones.
- These packets are then encapsulated into the data field of the transport layer packet. The headers containing source and destination address are then added.
- The length of the message which is to be divided can vary from several lines (e-mail) to several pages.
- But the size of the message can become a problem. The message size can be larger than the maximum size that can be handled by the lower layer protocols.
- Hence the messages must be divided into smaller sections. Each small section is then encapsulated into a separate packet.
- Then a header is added to each packet to allow the transport layer to perform its other functions.

2. Connection control :

- Transport layer protocols are divided into two categories :

  1. Connection oriented. 2. Connectionless.

Connection oriented delivery :

- A connection oriented transport layer protocol establishes a connection i.e. virtual path between sender and receiver.
- This is a virtual connection. The packet may travel out of order. The packets are numbered consecutively and communication is bi directional.

Connectionless delivery :

A connectionless transport protocol will treat each packet independently. There is no connection between them. Each packet can take its own different route.

3. Addressing :

The client needs the address of the remote computer it wants to communicate with. Such a remote computer has a unique address so that it can be distinguished from all the other computers.

Scanned by CamScanner

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.

6.3 Transport Layer Services :

MU : Dec. 05, May 07

University Questions

Q. 1 Discuss the services offered by transport layer. **(Dec. 05, May 07, 8 Marks)**

- In this section we are going to discuss the services provided by the transport layer.

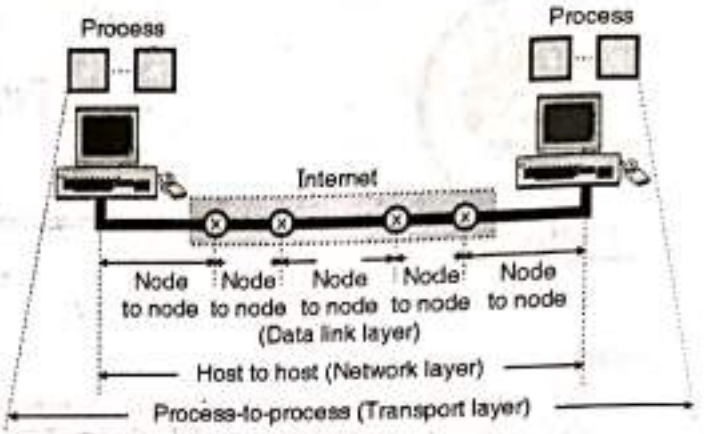
6.3.1 Process-to-Process Communication :

MU : Dec. 05, May 07

University Questions

Q. 1 Discuss the services offered by transport layer. **(Dec. 05, May 07, 8 Marks)**

- 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. 6.3.1 demonstrates the three processes.



(G-594) **Fig. 6.3.1 : Types of data deliveries**

- There is a difference between host-to-host communication and process to process communication that we need to understand clearly.
- The host to host (computer to computer) communication is handled by the network layer. But this communication only ensures that the message is delivered to the destination computer. But this is not enough.
- It is necessary to handover this message to the correct process. The transport layer will take care of this.

6.3.2 Addressing : Port Number :

MU : Dec. 05, May 07

University Questions

Q. 1 Discuss the services offered by transport layer. **(Dec. 05, May 07, 8 Marks)**

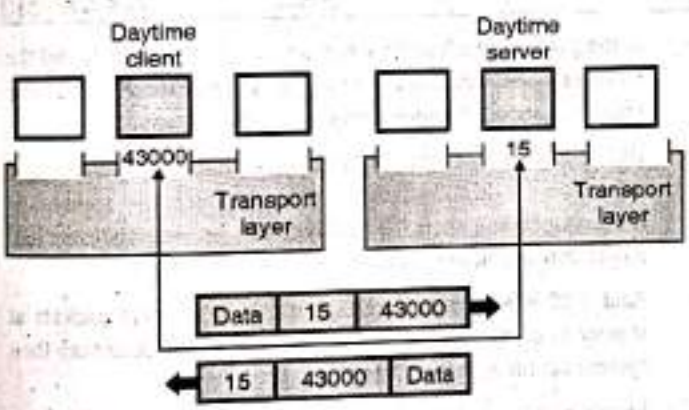
- There are several ways of achieving the process-to-process communication, but the most common method is using the client-server paradigm.
- **Client** is defined as the process on the local host. It needs services from another process called **server** which is on the other (remote) host.
- Both client and server have the same name. Some of the important terms related to the client-server paradigm are :

  1. Local host 2. Remote host
  3. Local process 4. Remote process

- We can use the IP addresses to define the local host and remote host. But this is not enough to define a process.
- In order to define a process, we have to use one more identifier called **Port Numbers.** In TCP/protocol suite, the port numbers are integers and they are numbered between 0 and 65,535.
- At the data link layer we need a MAC address, at the network layer we need to use an IP address. A datagram uses the destination IP address to deliver the datagram and uses the source IP address for the destination's reply.

Scanned by CamScanner

- At the transport layer a transport layer address called a **port number** is required to be used to choose among multiple processes running on the destination host.
- The destination port number is required to make the packet delivery and the source port number is needed to return back the reply.
- In the Internet model, the port numbers are 16 bit integers. Hence the number of possible port numbers will be $2^{16} = 65,535$ and the port numbers range from 0 to 65,535.
- The client program identifies itself with a port number which is chosen randomly. This number is called as **ephemeral port number.** Ephemeral means short lived. It is used because life of a client is generally short.
- The server process should also identify itself with a port number but this port number can not be chosen randomly.
- The Internet uses universal port numbers for servers and these numbers are called as **well known port numbers.**
- Every client process knows the well known port numbers of the pre identified server process.
- For example, a Day time client process can use an ephemeral (temporary) port number 43000 for identifying itself, the Day time server process must use the well known (permanent) port number 15. This is illustrated in Fig. 6.3.2.



(G-595) **Fig. 6.3.2 : Concept of port numbers**

What is difference between IP Addresses and Port Numbers ?

- The IP addresses and port numbers have altogether different roles in selecting the final destination of data.
- The destination IP address is used for defining a particular host among the millions of hosts in the world.
- After a particular host is selected, the port number is used for identifying one of the processes on this selected host.

IANA Ranges :

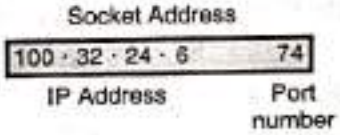
- The port numbers are divided into three ranges by IANA (International Assigned Number Authority).
- The ranges are as follows :

1. Well known ports
2. Registered ports
3. Dynamic or private ports.

1. **Well known ports :** The ports from 0 to 1023 are known as well known ports. They are assigned as well as controlled by IANA.
2. **Registered ports :** The ports from 1024 to 49,151 are neither controlled nor assigned by IANA. We can only register them with IANA to avoid duplication.
3. **Dynamic or private ports :** The ports from 49,152 to 63,535 are known as dynamic ports and they are neither controlled nor registered. They can be used by any process. Dynamic ports are also known as private ports and dynamic port are called as ephemeral ports.

Socket Address :

- Process to process delivery (transport layer communication) has to use two addresses, one is IP address and the other is port number at each end to make a connection. Hence a process to process delivery uses the combination of these two.
- The combination of IP address and port number is as shown in Fig. 6.3.3 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. 6.3.3 : 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.
- If we want to use the transport layer services in the Internet, then we have to use a pair of socket addresses namely the clients socket address and the server's socket address.

6.3.3 Encapsulation and Decapsulation :

MU : Dec. 05, May 07

University Questions

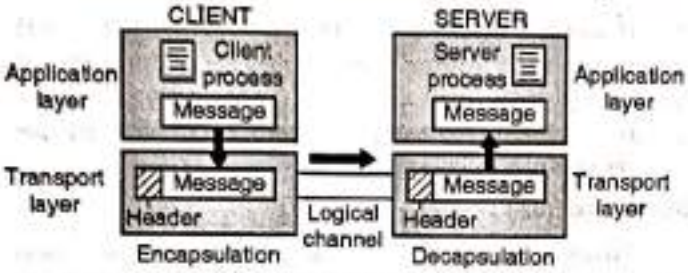
Q. 1 Discuss the services offered by transport layer. **(Dec. 05, May 07, 8 Marks)**

- The transport layer carries out the **Encapsulation** of the message at the sending end and then **Decapsulation** at the receiving end when two computers communicate. This process has been illustrated in Fig. 6.3.4.

Scanned by CamScanner

Encapsulation :

- At the sending end the process that has a message to send, will pass it to the transport layer alongwith a pair of socket addresses and some additional information.
- The transport layer adds its own header to this data. This packet at the transport layer in the Internet is known by different names such as **user datagram, segment or packet.**



(G-2012) **Fig. 6.3.4 : Encapsulation and decapsulation**

Decapsulation :

- When the segment or datagram arrives at the receiving end, the header is isolated and destroyed, and the message is delivered to the process running at the application layer as shown in Fig. 6.3.4.
- The socket address of the sender process is then handed over to the destination process.

6.3.4 Multiplexing and Demultiplexing :

MU : Dec. 03, Dec. 05, May 07

University Questions

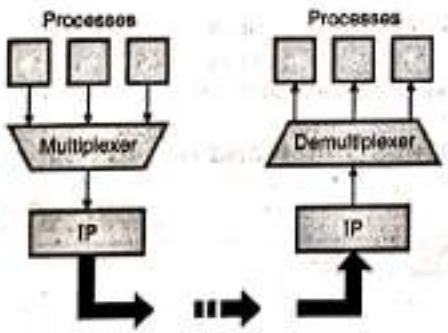
Q. 1 How are the port numbers used by TCP/UDP in demultiplexing incoming segments ?

(Dec. 03, 10 Marks)

Q. 2 Discuss the services offered by transport layer.

(Dec. 05, May 07, 8 Marks)

- The addressing mechanism allows multiplexing and demultiplexing taking place at the transport layer as shown in Fig. 6.3.5.



(G-597) **Fig. 6.3.5 : Multiplexing and demultiplexing**

Multiplexing :

- At the sending end, there are several processes that are interested in sending packets. But there is only one transport layer protocol (UDP or TCP). Thus it is a many processes-one transport layer protocol situation.
- Such a many-to-one relationship requires multiplexing.
- The protocol first accepts messages from different processes. These messages are separated from each other by their port numbers. Each process has a unique port number assigned to it.
- Then the transport layer adds header and passes the packet to the network layer as shown in Fig. 6.3.5.

Demultiplexing :

- At the receiving end, the relationship is one as to many. So we need a demultiplexer.
- First the transport layer receives datagrams from the network layer.
- The transport layer then checks for errors and drops the header to obtain the messages and delivers them to appropriate process based on the port number.

6.3.5 Flow Control :

MU : Dec. 05, May 07

University Questions

Q. 1 Discuss the services offered by transport layer.

(Dec. 05, May 07, 8 Marks)

- If the packets produced by the sender are at a rate X and the receiver is receiving them at a rate Y, then for X = Y, there will be a perfect balance observed in the system.
- But if X is higher than Y (source is producing packets at a rate which is higher than the rate at which the receiver is accepting them), then the receiver can be overwhelmed and has to **discard** some packets.
- And if X is less than Y (i.e. source is producing packets at slower rate than the rate of acceptance at the receiver) then system becomes **less efficient.**
- Flow control is related to the situation in which X > Y because it is very important to prevent data loss (due to discarding of packets) at the receiver site.

Pushing and pulling for flow control :

- There are two different ways of delivering the packets produced by the sender to the receiver. They are pushing or pulling.

1. Pushing :

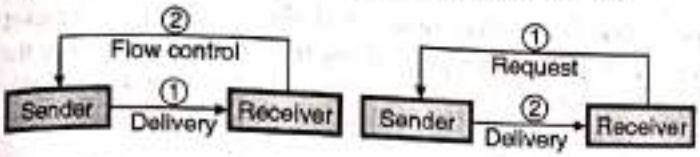
If the sender is sending the packets soon as they are produced, without receiving any prior request from the receiver then this type of deliver is called as **pushing.** Fig. 6.3.6(a) illustrates this concept.

2. Pulling :

If the sender sends the produced packets only when they are

Scanned by CamScanner

requested by the receiver then the delivery is called as **pulling.** Fig. 6.3.6(b) illustrates the principle of pulling.



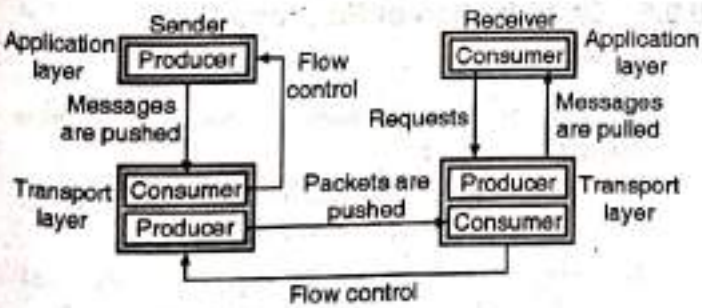
(a) Concept of pushing **(b) Concept of pulling**

(G-2013) **Fig. 6.3.6**

- In case of **pushing** type delivery, if the packets are being sent at a higher rate than that of receiving, then the receiver will be **overwhelmed,** and some received packets will have to be discarded.
- In order to avoid discarding of packets, the **flow control** will have to be exercised. For this the receiver has to warn the sender to stop the delivery when it is overwhelmed and it has to inform the sender again to start delivery when it (receiver) is ready, to receive the packets.
- In case of **pulling type delivery,** the receiver is actually pulling the packets from the sender. It requests for the packets when it is ready. Therefore the flow control is not required in this case.

6.3.6 Flow Control at Transport Layer :

- The concept of flow control at transport layer has been illustrated in Fig. 6.3.7. It shows the communication taking place between a sender and a receiver.
- As shown in Fig. 6.3.7, there are four entities involved in this communication. They are as follows :
  1. Sender process.
  2. Sender transport layer.
  3. Receiver process.
  4. Receiver transport layer.



(G-2014) **Fig. 6.3.7 : Flow control at transport layer**

- We will discuss the flow control by considering the sending and receiving ends separately.

Sending end :

- The first entity on the sending end is the **sender process,** at the application layer. It works only as a **producer** which produces chunk of messages and pushes them to the transport layer on the sending end, as shown in Fig. 6.3.7.
- The second entity on the sending end is the **sender transport layer.** It has two different roles to play.
- First it acts as a **customer** and consumes all the messages produced and pushed by the producer. Then it encapsulates those messages into packets and pushes them to the receiver transport layer as shown in Fig. 6.3.7. Here it acts as a **producer.**

Receiving end :

- The first entity on the receiving end is the **receiver transport layer.** It also has two different roles to play.
- It acts as a **consumer** for the packets pushed by the senders transport layer and it also acts as the **producer.** It has decapsulate the messages and deliver them to the application layer as shown in Fig. 6.3.7.
- However the delivery of decapsulated messages to the application layer is a **pulling type delivery.** That means the transport layer waits till the application layer process requests for the decapsulated messages.

Flow control :

- As shown in Fig. 6.3.7, the flow control is needed for atleast two cases. First is from transport layer of sender to the application layer of sender.
- And secondly form the transport layer of receiver to the transport layer of sender.

Buffers :

- It is possible to implement the flow control in many different ways. One of the ways of implementation is to use two **buffers** one each at the sending and receiving transport layers.
- A **buffer** is nothing but a set of memory locations which can temporarily hold (store) packets.
- It is possible to exercise flow control communication by sending signals from the consumer to producer.
- The **flow control** at the **sending end** takes place as follows : As soon as the buffer at the transport layer becomes full it sends the stop message to its application layer in order to stop the chunk of messages that are being pushed into the buffer.
- The second flow control takes place at the receiver transport layer as follows : As soon as the buffer at receiver transport layer becomes full, it will inform the sender transport layer to stop pushing the packets.
- Whenever the buffer becomes partially empty, it again informs the sender transport layer to start sending the packets again.

Scanned by CamScanner

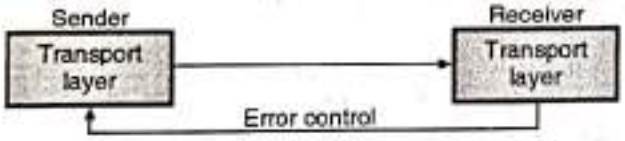
6.3.7 Error Control :

Need of error control :

- In the Internet, the network layer protocol IP has the responsibility to carry the packets from the transport layer at the sending end to the transport layer at the receiving end.
- But IP is unreliable. Therefore transport layer should be made reliable, in order to ensure reliability at the application layer.
- We can make the transport layer reliable by adding the **error control service** to the transport layer.

Duties of error control mechanism :

- Following are the important responsibilities of the error control mechanism introduced at the transport layer :
  1. To find and discard the corrupted packets.
  2. To keep the track of lost and discarded packets and to resend them.
  3. Identify the duplicate packets and discard them.
  4. To buffer out of order packets until the missing packets arrive.
- In the error control process, only the sending and receiving transport layers are involved. That means it is assumed that the chunk of messages exchanged between the application layers and transport layers are error free.
- The concept of error control at the transport layer level is demonstrated in Fig. 6.3.8.
- The receiving transport layer manages the error control by communicating with the sending transport layer about the problem.



(G-2015) **Fig. 6.3.8 : Concept of error control at the transport layer**

Sequence numbers :

- In order to exercise the error control at the transport layer following two requirements should be satisfied :
  1. The sending transport layer should know about the packet which is to be resent.
  2. The receiving transport layer should know about the packets which are duplicate or the ones that have arrived out of order.
- The requirements can be satisfied only if each packet has a unique **sequence number.**
- If a packet is either corrupted or lost the receiving transport layer will somehow inform the sending transport layer about the sequence number of those packets and request it to resend those packets.
- Due to the unique sequence number assigned to each packet it is possible for the receiving transport layer to identify the duplicate packets received. The out of order packets can also be recognized by observing gaps in the sequence numbers of the received packets.
- Packet numbers are given sequentially. But the length of the sequence number cannot be too long because the sequence number is to be included in the header of the packets.
- If the header of a packet allows "m" bits per sequence number, then the range of sequence number will be from 0 to $2^m - 1$. For example if m = 3 then the range of sequence numbers will be from 0 to 7.
- Thus sequence numbers are modulo 2^m.

Acknowledgement :

- The receiver side can send an acknowledgement (ACK) signal corresponding to each packet or each group of packets which arrived safe and sound.
- The question is what happens if a received packet is corrupted ? The answer is that the receiver simply discards the corrupted packet and does not send any ACK signal for it.
- The sender can detect a lost packet with the help of a timer. A timer is started at the sending end as soon as a packet is sent. If the ACK does not arrive before the expiry of the timer, then the sender treats the packet to be either lost or corrupted and resends it.
- The receiver silently discards the duplicate packets. It will either discard the out of order packets or stored until the missing packet is received.
- Note that every discarded packet is treated as a lost packet by the sender.

6.3.8 Combination of Flow and Error Control :

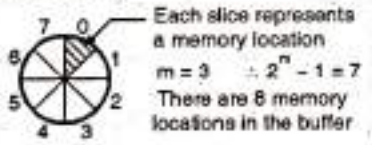
- Till now we have discussed the following important concepts :
  1. We need to use buffers at the sending and receiving ends for exercising the flow control.
  2. Also we have to use the sequence numbers and acknowledgements for exercising the error control.
- We can combine these two concepts together by using two numbered buffers one at the sender and the other at the receiver, in order to exercise a combination of flow and error control.
- At the sending end, when a packet, is prepared to be sent, the number of the next free location (x) in the buffer is used as the sequence number of that packet.

Scanned by CamScanner

- As soon as the packet is sent, its copy is stored at location (x) in the sending end buffer and the sender waits for the acknowledgement from the receiver.
- On reception of the acknowledgement of the sent packet, the copy of that packet is purged to make the memory location (x) free again.
- At the receiver, when a packet having a sequence number "y" arrives, it is stored at the memory location "y" in the receiver buffer until the receiver application layer is ready to receive it. The receiver will send the ACK message back to sender to inform it that packet "y" has arrived.

Sliding window :

- As the sequence numbers are modulo 2^m, we can use a circle as shown in Fig. 6.3.9 to represent the sequence number from 0 to 2^m-1.
- We can represent the buffer as a set of slices, called as the **sliding window** which will occupy a part of the circle at any time.
- In Fig. 6.3.9, we have assumed that m = 3. Therefore $2^m - 1 = 7$ and the sequence numbers are from 0 to 7. Hence the number of memory locations in a buffer will also be 8 i.e. 0 to 7.
- The sliding windows will correspond to the sender as well as receiver.
- On the sending side, when a packet is sent we will mark the corresponding slice. Therefore when marking of all the slices is done, it means the **sending buffer is full**, and it cannot accept any further messages from the application layer as shown in Fig. 6.3.9(d).



(a) Sliding window in the circular format

(b) Two packets have been sent

(c) Three packets have been sent

(d) Four packets have been sent. The window is full

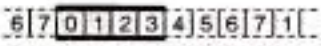
(e) Packet 0 has been acknowledged and the window slides

(G-2017) **Fig. 6.3.9**

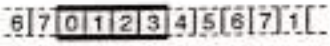
- When the acknowledgement for segment "0" arrives at the sending end, the corresponding segment (segment 0) is unmarked and window slides ahead by one slice as shown in Fig. 6.3.9(e). The size of the **sending window** is 4.
- Note that the sliding window is just an abstraction. In actual practice, computer variables are used to hold the sequence number of the next packet to be sent and the last packet sent.

Sliding window in the linear format :

- This is another way to diagrammatically represent a sliding window. It is as shown in Fig. 6.3.10.
- The principle of this type of sliding window is same as that of the circular representation. The linear format is the most preferred format. It needs less space on paper.
- Fig. 6.3.10(a), (b), (c) and (d) are the sliding windows presented in the linear format corresponding to Figs. 6.3.9(b), (c), (d) and (e) respectively in the circular presentation.

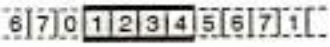


(a) Two packets have been sent



(b) Three packets have been sent

(c) Four packets have been sent. The window is full.



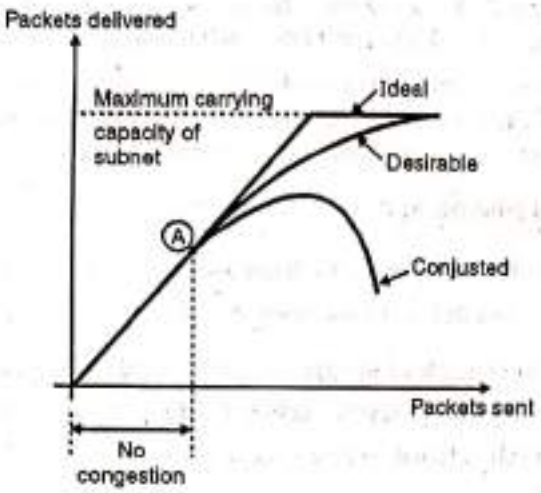
(d) Packet 0 has been acknowledged and the window slides

(G-2075)**Fig. 6.3.10 : Sliding windows presented in the linear format**

6.3.9 Congestion Control :

- An important issue in a packet switching network is congestion.
- If an extremely large number of packets are present in a part of a subnet, the performance degrades. This situation is called as congestion.
- Congestion in a network may occur when the load on the network i.e. the number of packets sent to the network is greater than the capacity of the network (i.e. the number of packets a network can handle).
- Fig. 6.3.11 explains the concept of congestion graphically.
- Upto point A in Fig. 6.3.11, the number of packets sent into the subnet by the host is within the capacity of the network. So all these packets are delivered. In short the number of packets delivered is proportional to number of packets sent and no congestion takes place.
- But after point A, the traffic increases too far. The routers cannot cope with the increased traffic and they begin to lose packets. The congestion begins here.
- As the traffic increases further, the performance degrades more and more packets are lost and congestion worsens.
- At very high traffic, the performance collapses completely and almost all packets are lost. This is the worst possible congestion.

Scanned by CamScanner



(G-473) **Fig. 6.3.11 : Concept of congestion**

Need of congestion control :

- We may define the **congestion control** as the mechanisms and techniques to control the congestion and keep the load below the capacity.
- It is not possible to completely avoid the congestion but it is necessary to avoid it otherwise control it.
- Congestion will result in long queues, which results in buffer overflow and loss of packets.
- So congestion control is necessary to ensure that the user gets the negotiated QoS (Quality of Service).

Causes of congestion :

- Congestion happens in any network due to waiting, and due to the abnormality in the flow.
- It also occurs due to the fact that routers and switches have queues at the buffers which store packet before and after their processing.

6.3.10 Connectionless and Connection Oriented Services :

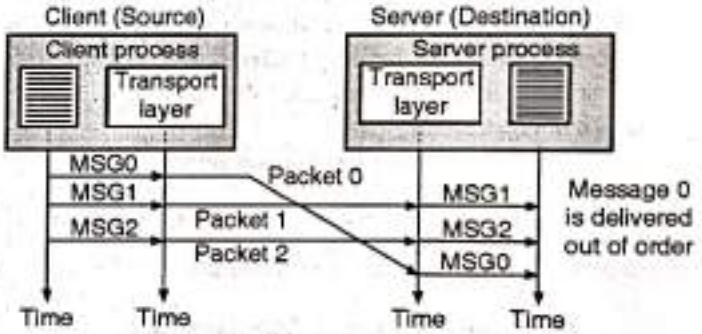
- A transport layer protocol is capable of providing two types of services :
  1. Connectionless services.
  2. Connection oriented services.
- The meaning of the words connectionless and connection oriented is different at the transport layer than that at the network layer.
- A connectionless service at the network layer means different datagrams of the same message following different paths.
- However at the transport layer, the meaning of connectionless service is independency between different packets.
- On the other hand a connection oriented service means the packets are interdependent.

Connectionless service :

- Refer Fig. 6.3.12 to understand the concept of connectionless service.
- The source process at the application layer first divides its message in chunks of data the size of which is acceptable to the transport layer.
- These data chunks are then delivered to the transport layer one by one. These chunks are treated as independent units by the transport layer.
- Every data chunk arriving from the application layer is encapsulated in a packet by the transport layer and sent to the destination transport layer as shown in Fig. 6.3.12.

Out of Order Delivery :

- In Fig. 6.3.12 we have considered three chunks of independent messages 0, 1 and 2. As the corresponding packets also are independent of each other and as they are free to follow their own path, these packets can arrive out of order at the destination as shown in Fig. 6.3.12.
- Naturally they are delivered to server process in an out of order manner.



(G-2018) **Fig. 6.3.12 : Concept of connectionless service**

- As seen in Fig. 6.3.12, at the sending end (client) the three chunks of messages 0, 1 and 2 are delivered to the transport layer in the order 0, 1, 2.
- But packet 0 travels a longer path and undergoes an extra delay. Therefore the packets are not delivered in order at the destination (server) transport layer.
- Therefore the message chunks delivered to the server process will also be out of order (1, 2, 0).
- If these chunks are of the same message then due to their out of order delivery the server will receive a strange message.

One packet is lost :

- The UDP packets are not numbered. So if one of the packets is lost, then the receiving transport layer will not have any

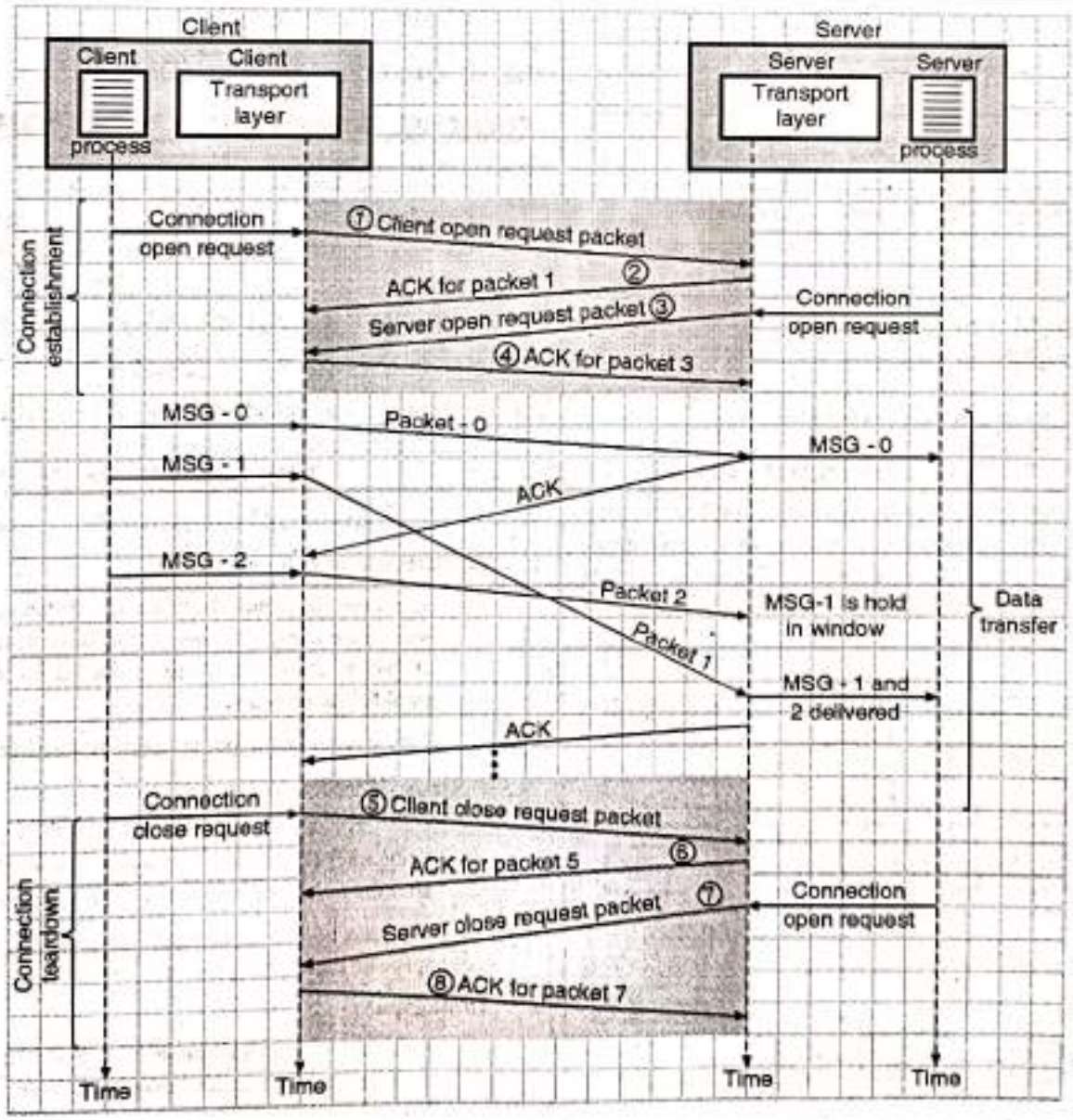
Scanned by CamScanner

idea about the lost packet. It will simply deliver the received chunks of messages to the server process.

- The above problems arise due to **lack of coordination** between the two transport layers. Due to this lack of co-ordination it is not possible to implement flow control, error control or congestion control in the connectionless service.

Connection oriented service :

- As we know, there are three stages involved in the connection oriented service. They are :
  1. Connection establishment.
  2. Exchange of data.
  3. Connection teardown.
- The connection oriented service is present at the network layer as well, but it is different from that at the transport layer.
- At the network layer, the meaning of connection oriented service involves the co-ordination between the hosts on either sides and all the routers between them.
- But at the transport layer, the meaning of connection oriented service is the end to end service that involves only the two hosts.
- Refer Fig. 6.3.13 to understand the concept of connection oriented service at the transport layer.
- In Fig. 6.3.13, all the three stages namely connection establishment, data exchange and connection teardown have been shown.
- It is important to note that it is possible to implement the flow control, error control and congestion control in the connection oriented service.



(G-2076) **Fig. 6.3.13 : Concept of connection oriented service**

Scanned by CamScanner

Comparison of Connection Oriented and Connectionless Services :

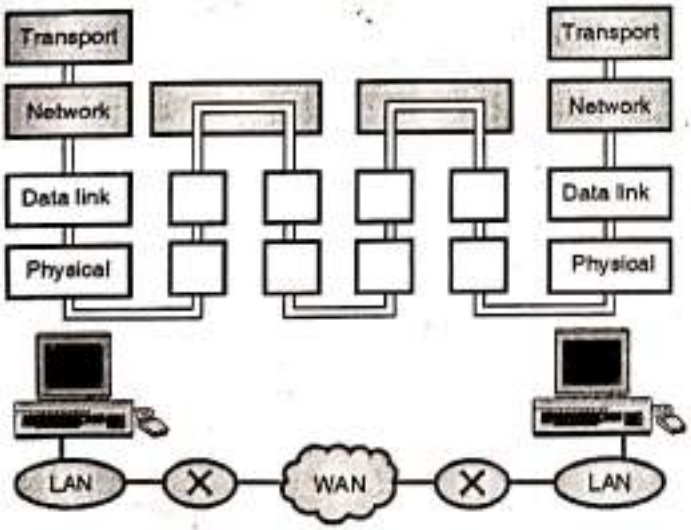
Sr. No.	Parameter	Connection oriented	Connectionless
1.	Reservation of resources	Necessary	Not necessary
2.	Utilization of resources	Less	Good
3.	State information	Lot of information required	Not much information is required to be stored
4.	Guarantee of service	Guaranteed	No guarantee
5.	Connection	Connection 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

6.3.11 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.



(G-598) **Fig. 6.3.14 : Error control**

- 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 eventhough 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.

  Note that the error is checked only upto the data link layer by the data link error control system.

6.3.12 Quality of Service (QoS) :

MU : Dec. 04, Dec. 06, May 09, May 15, May 16, Dec. 16

University Questions

Q. 1 Briefly explain the primary parameters that are the requirements to provide Quality of Service in networks. **(Dec. 04, 10 Marks)**

Q. 2 Write short notes on : QoS in transport layer. **(Dec. 06, May 09, 3 Marks)**

Q. 3 Discuss the quality of service parameters in computer network. **(May 15, May 16, Dec. 16, 10 Marks)**

- As mentioned earlier, the QoS parameters are as follows :

1. **Connection establishment delay :**
   - The time difference between the instant at which a request for transport connection is made and the instant at which it is confirmed is called as **connection establishment delay.**
   - This delay should be as short as possible to ensure better service.
2. **Connection establishment failure probability :**
   - Sometimes the connection may not get established even after the maximum connection establishment delay.
   - This can be due to network congestion, lack of table space or some other problems.
3. **Throughput :**
   - It is defined as the number of bytes of user data transferred per second, measured over some time interval.
   - Throughput is measured separately for each direction.

Scanned by CamScanner

4. **Transit delay :**

It is the time duration between a message being sent by the transport user from the source machine and its being received by the transport user at the destination machine.

5. **Residual error ratio :**

- It measures the number of lost or garbled messages as a percentage of the total messages sent.
- Ideally the value of this ratio should be zero and practically it should be as small as possible.

6. **Protection :**

This parameter provides a way to protect the transmitted data against reading or modifying it by some unauthorised parties.

7. **Priority :**

- Using this parameter the user can show that some of its connections are more important (have higher priority) than the other ones.
- This is important when congestions take place. Because the higher priority connections should get service before the low priority connections.

8. **Resilience :**

Due to internal problem or congestion the transport layer spontaneously terminates a connection. The resilience parameter gives the probability of such a termination.

6.4 Transport Service Primitives :

MU : Dec. 15, Dec. 17

University Questions

Q. 1 What are transport service primitives ? Discuss in brief. **(Dec. 15, 10 Marks)**

Q. 2 What are transport service primitives ? Explain. **(Dec. 17, 10 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

Sr. 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.
  1. The server executes a LISTEN primitive. This will make a system call to block the server until a client turns up.
  2. When a client wants to talk to the server it executes the CONNECT primitive.
  3. 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 :

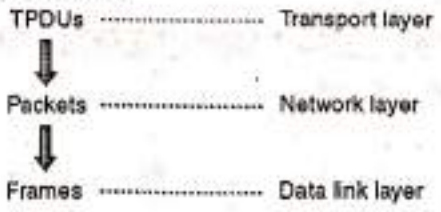
MU : Dec. 15, Dec. 17

University Questions

Q. 1 What are transport service primitives ? Discuss in brief. **(Dec. 15, 10 Marks)**

Q. 2 What are transport service primitives ? Explain. **(Dec. 17, 10 Marks)**

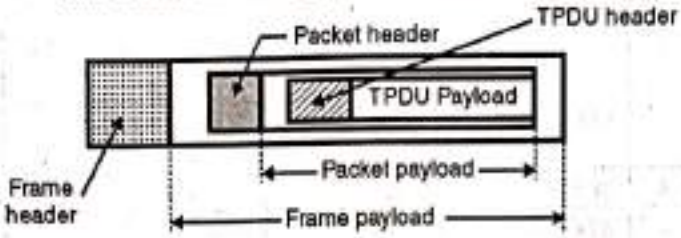
- The TPDUs which are exchanged by the transport layer are contained in the packets that are exchanged by the network layer.
- These packets are in turn contained in the frames which are exchanged by the data link layer.
- When a frame arrives, the data link layer processes the frame header and passes the contents of the frame payload field to the network entity.



(G-599(a)) **Fig. 6.4.1**

Scanned by CamScanner

- 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 :
  1. Asymmetric
  2. Symmetric

6.5 Sockets :

MU : Dec. 03, Dec. 06, Dec. 07, May 08, May 09

University Questions

Q. 1 Explain the difference of UDP and TCP socket of server side especially when the client initiates the connection or request to the server. **(Dec. 03, 10 Marks)**

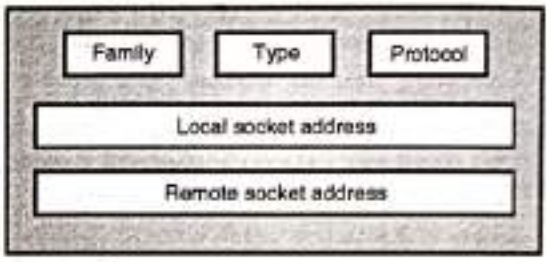
Q. 2 Explain the terms : Socket. **(Dec. 06, Dec. 07, May 09, 2 Marks)**

Q. 3 Explain with example : Socket. **(May 08, 10 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-601) **Fig. 6.5.1 : Socket structure**

- Various fields in the socket structure are as follows :
  1. **Family :** This field is used for defining the protocol group such as IPv4 or IPv6, UNIX domain protocol etc.
  2. **Type :** This field is used for defining the type of socket such as stream socket, packet socket or raw socket.
  3. **Protocol :** This field is usually set to zero for TCP and UDP.
  4. **Local socket address :** It is used for defining the local socket address. This address is a combination of local IP address and the port address of the local application program.
  5. **Remote socket address :** It is used for defining the remote socket address which is a combination of remote IP address and the port address of the remote application program.

6.5.1 Socket Types :

- 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.

Scanned by CamScanner

1. **Stream socket :**

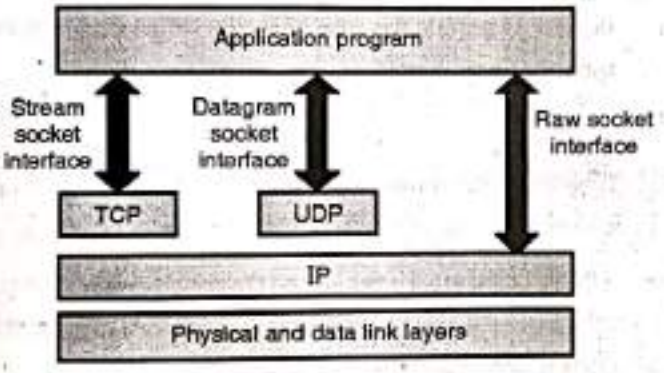
This is designed for the connection oriented protocol such as TCP. The TCP uses a pair of stream sockets one each on either ends for connecting one application program to the other across the Internet.

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-602) **Fig. 6.5.2 : Type of sockets**

6.5.2 Berkeley Sockets :

MU : Dec. 09, Dec. 11, May 13, Dec. 13, May 15

University Questions

Q. 1 Write short notes on : Berkeley socket.
(Dec. 09, Dec. 11, May 13, 6 Marks)

Q. 2 Show the usage of the different socket programming primitives used for establishing a connection between client and server.
(Dec. 13, 10 Marks)

Q. 3 Write short note on Berkeley Socket.
(May 15, 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.

Steps followed for Socket Programming :

- The steps followed for the socket programming are as follows :

Server side :

1. Server creates a socket and checks for errors using SOCKET.
2. Assign address to the newly created socket using BIND.
3. Use the LISTEN to allocate space for the queue which is used for the incoming calls.
4. Execute an ACCEPT for blocking the waiting incoming connections.

Scanned by CamScanner

Client side :

1. Create a socket using SOCKET.
2. Use CONNECT to initiate connection process.
3. Establish the connection.

6.5.3 Connectionless Iterative Server :

- 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.

6.5.4 Connection Oriented Concurrent Server :

- 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.

Scanned by CamScanner

(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 Transport Layer Protocols :

MU : Dec. 14

University Questions

Q. 1 Explain the different elements of transport protocols. **(Dec. 14, 10 Marks)**

- We have discussed a few transport layer services in the previous section. By combining a set of these services as per requirement, we can create a transport layer protocol.
- It is important to understand the behavior of these general protocols, before we discuss the transport layer protocols such as UDP and TCP.
- In this section we will discuss the following protocols :
  1. Simple protocol.
  2. Stop and wait protocol.
  3. Go back N (GBN) protocol.
  4. Selective repeat protocol.
  5. Bidirectional protocol. (Piggybacking).
- Initially we will discuss all these protocols as **simplex** i.e. **unidirectional** protocols and then we will see how to make them the **full duplex** i.e. **bidirectional** protocols.

6.6.1 Simplex Protocol :

- This is the simplest type of connectionless protocol which has the following characteristics :
  1. No flow control.
  2. No error control.
  3. The receiver does not get overwhelmed.
- Because the receiver does not get overwhelmed due to the incoming packets even at very high rate, the receiver can handle any packet immediately as soon as it is received.
- The principle of operation (or protocol layout) of the simple protocol has been illustrated in Fig. 6.6.1(a).

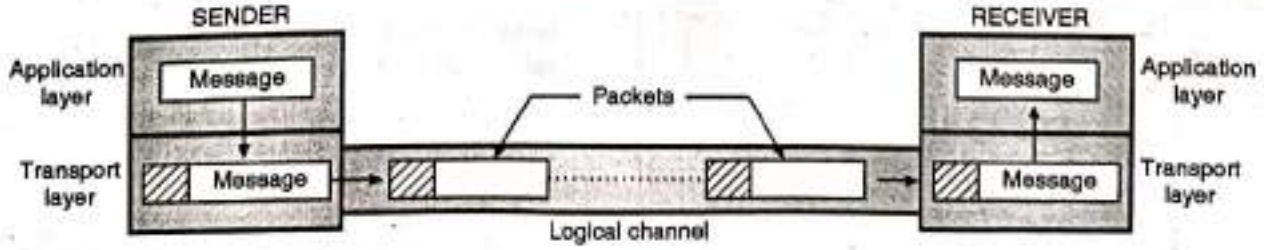
Operation :

At the sender :

- The application layer at the sender, sends its message to the transport layer.
- The sender transport layer receives the message and makes a packet out of it.
- This packet is then sent over the logical channel between the transport layers on the two ends.

At the receiver :

- The network layer at the receiver (not shown in Fig. 6.6.1(a)) delivers the received packet to the transport layer.
- The receiver transport layer extracts the message from the packet (decapsulation) and sends the message to the application layer.

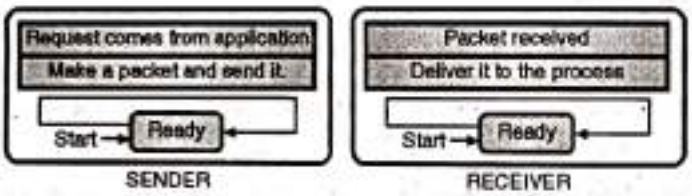


(G-2179) **Fig. 6.6.1(a) : Layout of the simple protocol**

Scanned by CamScanner

FSM :

- In this protocol, the sender should not send a packet as long as its application layer does not have a message to send.
- Whereas the receiving transport layer should not deliver a message to its application layer unless it receives a packet from the sender.
- These two requirements suggest, the sender and the receiver have only one state : **Ready state.**
- The sending machine remains in the **ready state** until a process in its application layer sends a request to send its message.
- As soon as the request comes, the sending machine will encapsulate the message and send it to the receiver.
- The receiving machine also remains in **ready state** until it receives a packet from the sender.
- On arrival of a packet, the receiver decapsulates it and delivers the extracted message to the application layer process.

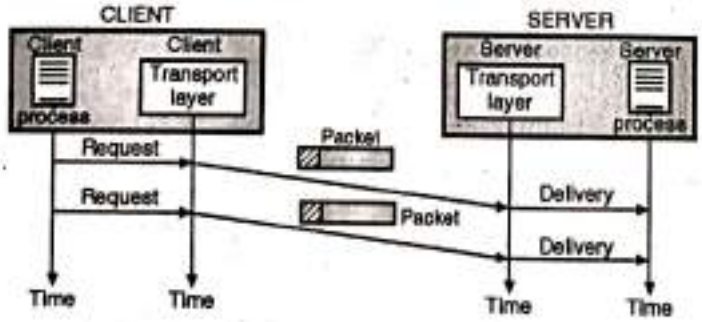


(G-2180) **Fig. 6.6.1(b) : FSM for the simple protocol**

- Note that the UDP protocol is a slight modification of this protocol. The FSM (Finite State Machine) for this protocol has been shown in Fig. 6.6.1(b) and its flow diagram is as shown in Fig. 6.6.1(c).

Flow Diagram :

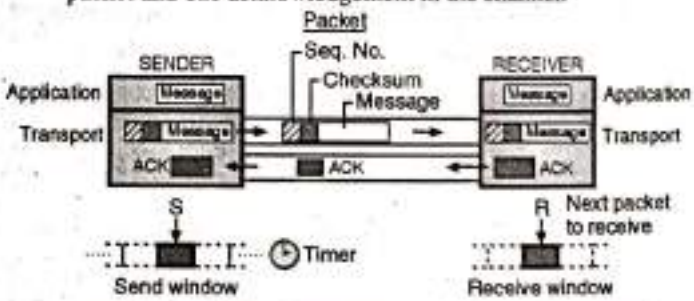
- The communication between the sender and receiver using the simple protocol has been shown in Fig. 6.6.1(c).
- The sender keeps sending the packets, without taking the receiver into consideration at all.



(G-2181) **Fig. 6.6.1(c) : Flow diagram for the simple protocol**

6.6.2 Stop and Wait Protocol :

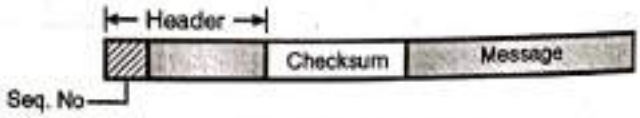
- The second transport layer protocol that we will discuss now is a **connection oriented** protocol called as **stop and wait protocol.**
- The operation of this protocol are as follows :
  1. It is a connection oriented protocol.
  2. It provides both flow and error control.
  3. Sender sends one packet at a time and waits for its acknowledgement from receiver before sending the next packet.
  4. A checksum is added to each data packet so as to detect a corrupted packet.
  5. At the receiver, the checksum in each packet is checked. If found incorrect, the receiver considers it as the corrupted packet and discards it silently. Such a packet is not acknowledged by the receiver.
  6. If the sender does not receive an acknowledgement for a packet within a predecided time, it understands that the packet is either corrupted or lost.
  7. The sender starts a timer everytime it sends out a packet. If it receives the acknowledgement for the packet before the expiry of the timer, it stops the timer, and sends the next packet. But if the timer expires before the arrival of acknowledgement, the sender resends the previous packet which was either corrupted or lost.
- Fig. 6.6.2(a) shows the principle of the stop and wait protocol. Note that at any given time there can be only one packet and one acknowledgement in the channel.



(G-2182) **Fig. 6.6.2(a) : Principle of stop and wait protocol**

Sequence number :

- In this protocol, sequence numbers and acknowledgement numbers are used for preventing duplicate packets.
- As shown in Fig. 6.6.2(b), an additional field is created in the packet header of each packet to hold its sequence number.



(G-2183) **Fig. 6.6.2(b) : Packet**

Scanned by CamScanner

- A very important consideration about the sequence number is the **range of sequence numbers.**
- In order to provide an unambiguous communication with the minimum packet size, we look for the smallest range of sequence numbers.
- Let x be the sequence number of a packet, then the next sequence number should be (x + 1). There is no need for (x + 2). We can show it using the following discussion.
- Suppose that a packet with the sequence number x has been sent by the sender. Then the following three things can possibly happen.

1. Everything is normal :

- The first possibility is that the packet reaches its destination safe and sound without getting corrupted or lost. The receiver sends the acknowledgement for it.
- The acknowledgement reaches the sender safe and sound.
- The sender sends the next packet having a sequence number of (x + 1).

2. Packet corrupted or lost :

- The second possibility is that the sent packet either gets corrupted or gets lost and does not reach the receiving end at all.
- The receiver discards the corrupted packet silently. In either case (corrupted or lost packet), the acknowledgement is not sent back.
- The sender waits for the timer to expire and resends the packet numbered x. The receiver sends back the acknowledgement for it.

3. The acknowledgement is corrupted or lost :

- The packet (numbered x) arrives safe and sound at the receiving end for which it sends an acknowledgement back to the sender.
- However the acknowledgement either get corrupted or gets lost on its way back. Therefore the sender resends the packet (numbered x) again after the expiry of the timer.
- Thus packet x has a duplicate now. The receiver will understand this fact because it was expecting packet numbered (x + 1) to arrive but instead it received the packet numbered x again.

Conclusions :

- From the above discussion we can conclude that sequence numbers x and x + 1 are required so that the receiver can distinguish between cases 1 and 3 discussed above. But it is not necessary to number the packet as (x + 2).
- In case 1, we can number the packet as x again because both the packets (x and x + 1) are acknowledged by the receiver and neither the sender nor the receiver has any ambiguity about it.
- Finally in the case 2 and 3, the new packet is (x + 1) and not (x + 2). Therefore we conclude that only two sequence numbers x and x + 1 are needed and x +2 is not needed.
- So let x = 0 then (x + 1) = 1. Thus there will be only two sequence numbers 0 and 1 and the packet sequence would be 0, 1, 0, 1, 0... and so on. Due to the presence of only two distinct sequence numbers, this is called as modulo-2 arithmetic.

Acknowledgement numbers :

- For both types of packets i.e. data packets and acknowledgements, the same sequence numbers should be suitable.
- For this to happen successfully the following convention is used.
- The acknowledgement number always indicates the sequence number of the **next packet** that the receiver is expecting to receive.
- For example, the packet with a sequence number 0 arrives at the receiver safe and sound. Then the corresponding ACK sent by the receiver will have a number 1 on it which means that the next expected packet to be received is packet 1.
- Similarly if packet 1 arrives safe and sound then ACK with acknowledgement 0 is sent back which means that packet – 0 is the next expected packet at the receiver.
- The **control variable** at the sender is called as the **sender (s)** and it points to the only slot present in the send window as shown in Fig. 6.6.2(a).
- Similarly the **control variable** at the receiving end called as the **Receiver (R)** and it points to the only slot present in the receive window as shown in Fig. 6.6.2(a).

FSMs of stop and wait protocol :

- This protocol is a connection oriented protocol. Therefore a connection between the two ends should be established before transferring the data.
- In other words both sender and receiver must be in the **established state** before the beginning of data exchange.

1. Sender FSM :

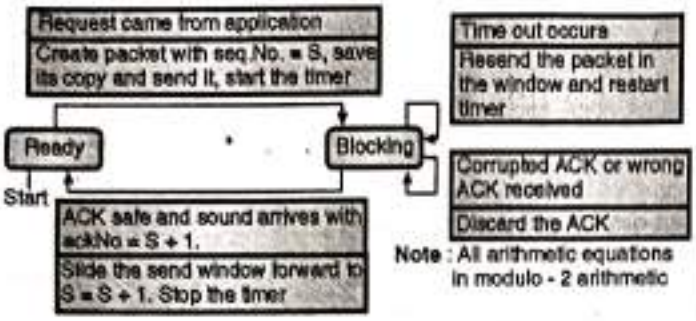
- The sender's FSM is shown in Fig. 6.6.2(c). Initially it is in the **ready** state. However it can move between the ready and blocking state.
- The initial value of variable "s" is set to 0.

1. Ready state :

- The sender, when in the ready state waits only for one event to happen, that is the request coming from application layer.
- As soon as such a request comes from the application layer, the sender makes a packet with the sequence number same as "s."

Scanned by CamScanner

– It stores a copy of this packet and sends the packet. The sender starts the timer and moves into its **blocking state.**



(G-2184) **Fig. 6.6.2(c) : Sender's FSM for stop and wait protocol**

2. Blocking state :

– When the sender is in the blocking state as shown in Fig. 6.6.2(c), the following three possible events can happen :

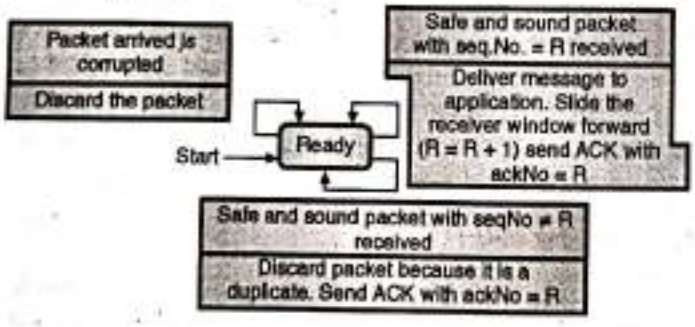
a. An error free ACK is received by the sender. It's ackNo is also correct i.e. (S + 1). The sender then stops the timer, slides the sending window to S = (S + 1) modulo - 2 and moves to the ready state.

b. The ACK received by the sender is either corrupted or a wrong ACK i.e. the one having the ackNo other than (S + 1). The sender discards the ACK.

c. In case if the timer expires (time out conditon), the sender resends the only outstanding packet with it. It then restarts the timer as shown in Fig. 6.6.2(c).

2. Receiver FSM :

– The receiver's FSM is shown in Fig. 6.6.2(d). Note that there is no blocking state in the receiver's FSM. There is only the ready state.



(G-2185) **Fig. 6.6.2(d) : FSM of receiver for stop and wait protocol**

– At the receiver also there is a possibility of following three events happening after the arrival of a packet.

a. A safe and sound packet (without corruption) is received with seq.No = R. Then the messages is extracted (decapsulation) and delivered to the application layer. The receive window slides forward to (R = R + 1) modulo - 2 and the receiver sends an ACK with ackNo = R.

b. A safe and sound packet (with any error) arrives, but its seq.No ≠ R. This shows that it is a duplicate packet. The receiver will discard this packet but sends an ACK with ackNo = R.

c. The received packet is corrupted. The receiver silently discards it. No ACK is sent back.

Efficiency of stop and wait protocol :

– The efficiency of the stop and wait protocol is very very low. This is because it sends a packet and simply waits for its ACK before sending the next packet.

– This is a gross underutilization of the communication channel especially if the channel is **thick and long.**

– A channel is thick if it has a large bandwidth and it is **long** if it has a long round trip time.

– The product of these two parameters is called as **bandwidth delay product.**

– A channel is equivalent to a pipe. If it is underutilized, then it will be called inefficient.

– The number of bits a sender can transmit through the channel can be measured from the value of bandwidth delay product.

– On all these accounts the stop and wait protocol proves to be extremely inefficient.

Pipelining :

– In networking and even other areas, a task is started before the ending of previous task. This is known as **pipelining.**

– In the stop and wait protocol, the senders sends a packet and waits for its acknowledgement before sending the next packet.

– This shows that there is no pipelining in the stop and wait protocol.

– But in the other protocols that we are going to discuss after the concept of pipelining will be used.

– Therefore it is possible for the sender to send several packets before it receives only acknowledgements for the previously sent packets.

– The process of pipelining improves the efficiency of the protocol.

6.6.3 Go Back-N Protocol (GBN) :

– The efficiency of transmission can be improved by transmitting multiple packets while the sender is waiting for acknowledgment.

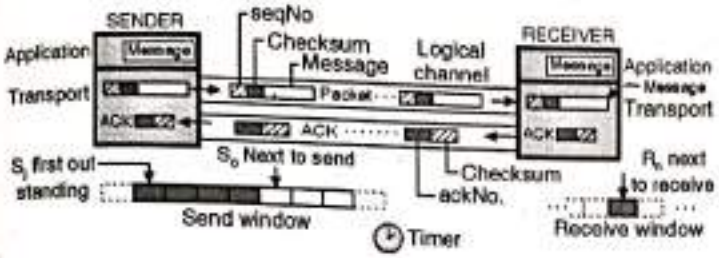
– That means we should allow more than one outstanding packets even when the sender is waiting for acknowledgement because this will keep the channel busy.

– A protocol which can achieve this goal is our next protocol called Go Back-N (GBN) protocol.

– The most important part in the operation of GBN protocol is that we can send several packets before receiving acknowledgement. But the receiver can buffer only one packet.

Scanned by CamScanner

- A copy of every sent packet is kept by the sender until it receives the acknowledgement of that packet.
- Fig. 6.6.3(a) shows the outline of GBN protocol which explains its principle of operation. Note the simultaneous presence of multiple packets and multiple acknowledgements in the channel at any given time.



(G-2186) **Fig. 6.6.3(a) : Principle of Go Back-N (GBN) protocol**

Sequence numbers :

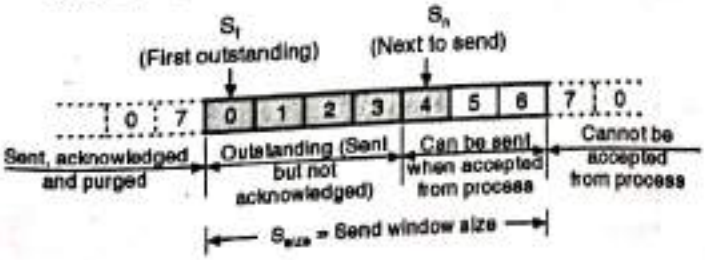
In GBN protocol, the sequence numbers are modulo 2^m, where **m** denotes the size of sequence number field in bits.

Acknowledge numbers :

- In the GBN protocol, the acknowledgement number is cumulative and it carries the sequence number of the next packet that is expected to be received at the receiver.
- If the ackNo = 6, its an indication that the receiver has received all the packets having sequence number upto 5 safe and sound. Hence the receiver is expecting the packet with seq.No = 6 to arrive next.

Send window :

- We can define the send window as an imaginary box, which covers the sequence numbers of the data packets that can be sent.
- The **maximum size** of the send window is $(2^m - 1)$ for the reasons discussed later on in the chapter.
- In each send window position (it can slide), some sequence numbers indicate the packets that have been already sent whereas the other sequence numbers indicate the data packet that are to be sent.
- In this chapter we assume that the send window size is fixed and has been set to its maximum possible value. But in some protocols the send window size is variable.
- The structure of a send window for the GBN protocol with m = 3 has been shown in Fig. 6.6.3(b). Note that the window size = $2^m - 1 = 2^3 - 1 = 7$.



(G-2187) **Fig. 6.6.3(b) : Format of the send window of GBN**

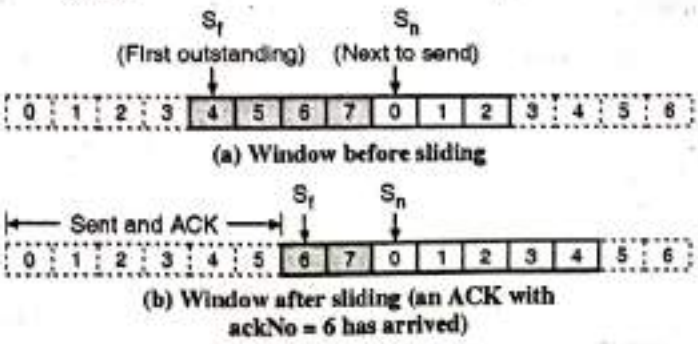
- At any given time, the send window divides the possible sequence numbers into four regions.
- As shown in Fig. 6.6.3(b), the first region corresponds to the portion to the left of the send window. It consists of the sequence numbers which belong to the packet which are already acknowledged. The sender does not keep any copy of these packets.
- The second region which is shaded in Fig. 6.6.3(b) contains the sequence numbers belonging to the packets that are already sent but not acknowledged by the receiver. That means the exact status of these packets is not known.
- These packets are called as **outstanding packets.**
- The third range, which is not shaded in Fig. 6.6.3(b), contains the sequence numbers belonging to the packets which the sender can send. But the corresponding data is yet to be received from the application layer.
- And finally the fourth range, which is at the right of the send window in Fig. 6.2.3(b), consists of the sequence numbers that cannot be used by the sender until the send window slides to the right hand side.

Size and location of send window :

- There are three variables that define the size and location of the send window at any given time. They are :
  1. S_f : Send window, the first outstanding packet.
  2. S_n : Send window ; the next packet to be sent.
  3. S_{size} : Send window, size.
- The sequence number of the first (oldest) outstanding packet is defined by the variable S_f.
- The sequence number, that will be assigned to the next packet to be sent is defined by the variable S_n.
- And finally the size of the send window which is fixed in GBN protocol is defined by the variable S_{size}.

Sliding of send window :

- A send window will slide right on the arrival of acknowledgements.
- Fig. 6.6.4 shows the send window before sliding and after the arrival of an acknowledgement with ackNo = 6. This means that all packets upto seq.No = 5 have reached safe and sound and the receiver is expecting the packet with seq.No = 6 to arrive.



(G-2188) **Fig. 6.6.4 : Sliding of send window**

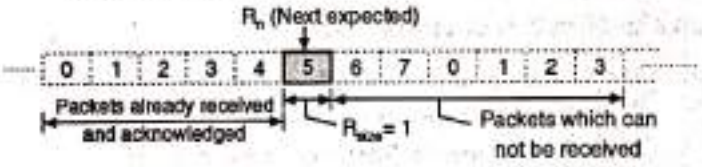
Scanned by CamScanner

Conclusion :

From all this discussion we conclude that the send window will slide by one or more slots when the sender receives an errorfree ACK whose ackNo is greater than or equal to S_f and less than S_n.

Receive window :

- The receive window has two tasks : First it has to ensure that correct data packets are received and second is to make sure that correct acknowledgements are sent.
- The size of receive window in the GBN protocol is always 1. Therefore, the receiver is always expecting a specific packet to arrive.
- That means the receiver will discard any packet which arrives out of order and the sender has to resend the discarded packet.
- The receive window for the GBN protocol is shown in Fig. 6.6.5. It has only one variable R_n. i.e. receive window, next packet expected.



(G-2189) **Fig. 6.6.5 : Structure of receive window of GBN**

- The sequence numbers to the left of the receive window correspond to the already received and acknowledged packets.
- The sequence numbers to the right of receive window correspond to the packets which cannot be received.
- The receiver discards any packet that belongs to these two ranges. It will only accept that packet whose sequence number exactly matches with the value of R_n.
- Like the sliding window, the receive window also slides but only by one slot at a time. On reception of a correct packet, the receive window slides to $R_n = (R_{n+1})$ modulo 2^m.
- If a corrupted packet is received, the receive window does not slide at all.

Timers :

- Ideally there should be one timer per packet, which is sent. In GBN protocol only one timer is used.
- The reason for this is that the timer for the first outgoing packet will always expire first. If so, then all the outstanding packets will be resent by the sender.

Resending the packets :

- As stated earlier, on the expiry of the only timer (also called as time out), all the outstanding packets will be resent.
- As an example, let us assume that the sender has already sent the packet having seq.No 6 (S_n = 7) but the time out takes place (that means the only timer in GBN has expired).
- If S_f = 3, then it is an indication that the packets 3, 4, 5 and 6 are all outstanding packets i.e. they are sent but not acknowledged.
- Hence, as soon as the timer expires, the sender will go back and resend all the outstanding packets i.e. packets 3, 4, 5 and 6.
- This is the reason behind the name of this protocol which Go Back N. The sender goes back by N slots and resends all the packets from there as soon as the timer expires.

Send window size :

- Now we are going to discuss, why in GBN protocol the size of send window should be less than 2^m.
- Let m = 2. Therefore the size of the send window will be 2^{m-1} = 3. With this send window size if all the acknowledgements are lost and the timer expires, then the sender resends all packets.
- As the receiver is expecting packet 3 and not 0, it will successfully identify the resent packet 0 as the duplicate and discard it.
- But if the send window size is 2^m = 4, and if all the acknowledgement are lost and the timer expires, then the sender will retransmit packet 0.
- But this time, the receiver also is expecting packet 0 to arrive (next cycle). Hence it won't treat the resent packet 0 as the duplicate packet and won't discard it.
- In fact the duplicate packet 0 is accepted as the legitimate packet 0 of the next cycle. This is an error.
- From this example we conclude that the size of send window in GBN protocol should be **less than 2^m.**

Comparison of GBN with stop and wait :

- The GBN and stop and wait protocols are somewhat similar to each other.
- The stop and wait protocol is actually a GBN protocol with only two sequence numbers (0 and 1) and send window size of 1.
- In stop and wait protocol, the modulo 2 arithmetic is used whereas in GBN protocol, modulo 2^m arithmetic is said to have been used.
- Thus stop and wait protocol is a GBN protocol with m = 1.

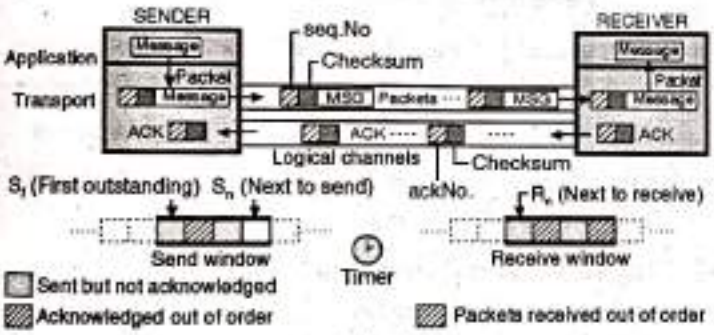
6.6.4 Selective Repeat Protocol :

- The process at the receiving end is simplified in the GBN protocol to a great extent. This is because R_n is the only variable which is to be tracked by the receiver ant the out of

Scanned by CamScanner

order received packets need not be buffered. They are to be simply discarded.

- But the problem with this protocol is its **inefficiency** if the underlying protocol tends to loose a lot of packets.
- This is because everytime with the loss of a packet the sender has to send all the outstanding packets.
- It is possible that some of these packets may have been received without any error but out of order.
- If the network congestion is already existing, then it will become worse due to these frequently resent packets. The worsened network congestion will result in the loss of more packets which leads to retransmission on of more packets and so on.
- This is called as an **avalanche effect** which may eventually cause total collapse of the network.
- In order to overcome these problems of the GBN protocol, a new protocol has been deviced which is called as the **Selective Repeat Protocol.**
- This new protocol, as the name suggests, resends only **selected packets**, that are actually corrupted or lost. It does not resend all the outstanding packets like the GBN protocol.
- This will reduce the number of resent packets and therefore reduces the possibility of network congestion.



(G-2190) **Fig. 6.6.6 : Outline of selective repeat protocol**

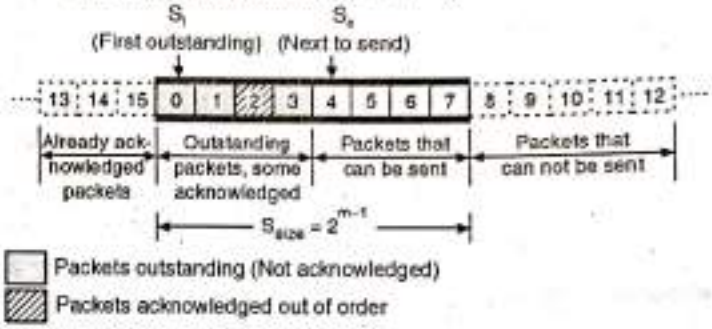
- The principle of selective repeat protocol has been illustrated in Fig. 6.6.6.

Windows :

- In the selective request protocol also there are two windows used : a send window and a receive window.
- However these windows are different from those in the GBN protocol. In this protocol the maximum size of send window is (2^{m-1}). This size is much smaller than that in the GBN protocol. Also the size of receive window is same as that of the send window.

Send and receive windows :

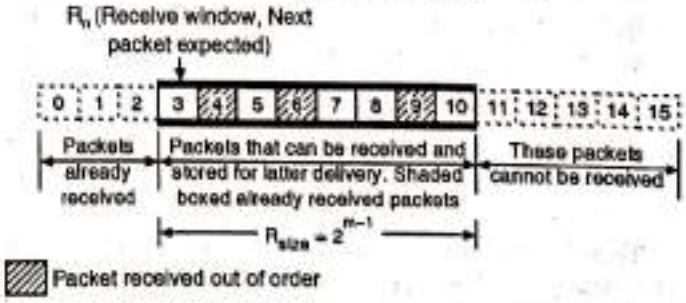
- If m = 4, then the maximum size of the send window is $2^{m-1} = 2^3 = 8$ (It is 15 in the GBN protocol). Fig. 6.6.6(a) shows the structure of the send window.
- Fig. 6.6.6(b) shows the structure of receive window in the selective repeat protocol. Note that it is totally different from that in the GBN protocol.
- The receive window here has the same size as that of the send window (Maximum size = 2^{m-1}).



(G-2191) **Fig. 6.6.6(a) : Send window for selective repeat protocol**

Principle :

- In the selective repeat protocol, the packets equal to the size of the receive window are allowed to arrive out of order.
- The receiver is allowed to keep them until it has a set of consecutive packets which can be delivered to the application layer.
- As the send and receive windows are of the same size, all the packets in the send window can arrive out of order at the receiver and the receiver is allowed to store them until it can deliver them to the application layer.
- However the selective repeat is a reliable protocol. Therefore the receiver is not expected to deliver packets out of order to the application layer.
- The structure of the receiver window for selective repeat protocol is as shown in Fig. 6.6.6(b). It shows that there are packets received out of order. These packets have to wait for the earlier transmitted packets to arrive before all of them are finally delivered to the application layer.



(G-2192) **Fig. 6.6.6(b) : Receive window for selective repeat protocol**

Scanned by CamScanner

Timer :

- Theoretically in SR protocol a timer is assigned to each outstanding packet in the send window. When a timer expires, only the corresponding packet is resent.
- This is totally different from the GBN protocol which has only one timer for a group of outstanding packets.
- But practically, almost all the transport layer protocols which are based on selective repeat principle use only one timer.

Acknowledgements :

- In GBN protocol, the ackNo is cumulative. It carries the number of the next expected packet to be received. It also confirms that all the previous packets have been received safe and sound.
- But in the SR protocol it is totally different. In SR the ackNo defines the sequence number of only one packet which is received safe and sound. It does not give any feedback about the other packets.

Window sizes :

- The maximum size of send and receive windows in the SR protocol is 2^{m-1} that means $2^m/2$ i.e. half of 2^m.
- If m = 2, all the acknowledgements are lost and if the time out takes place (i.e. timer expires) then sender retransmits packet 0.
- But the receiver window is expecting packet 2 and not packet 0. Hence the receiver will identify packet 0 as the duplicate packet and will discard it. (The sequence number 0 is not in the window).
- Now imagine that the window size is 3, all acknowledgements lost and the timer expires. Now the sender will resend packet 0.
- At this time the receiver is also expecting packet 0 of the next cycle to arrive (0 is the part of the window). Therefore the receiver cannot recognize that packet 0 is a duplicate packet. This is an error.
- That is why in S.R. protocol, the maximum size of the send and receive windows is 2^{m-1} or half of 2^m.

6.6.5 Bidirectional Protocols : Piggybacking :

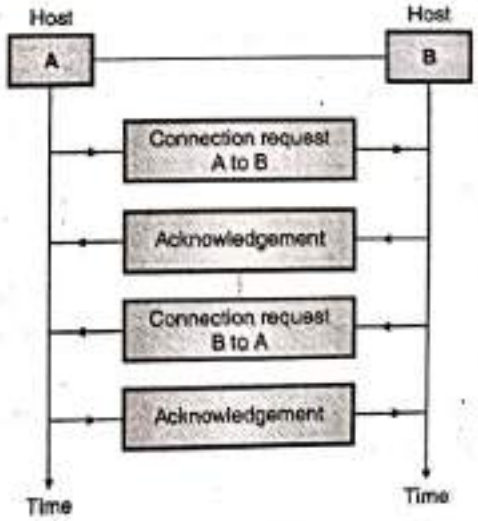
- Note that in all the protocols discussed so far the data packets flow in only one direction and acknowledgements travel in the opposite direction. Therefore all these four protocols are said to be **unidirectional protocols.**
- However in reality the data packets are travelling in both the directions, client to server and vice versa. The acknowledgements also are travelling in both the directions.
- Thus all the transport layer protocols in real life are bidirectional. We can improve the efficiency of these bidirectional protocols with a technique called **piggybacking.**
- In piggybacking, the data packet going from A to B can also carry acknowledgement for the data packet arrived from B to A.
- Similarly a data packet sent by B to A can carry acknowledgement for the data packet arrived from A to B.

6.7 Connection Management :

In a connection oriented service, a connection is established between source and destination. Then the data is transferred and at the end the connection is released.

6.7.1 Connection Establishment :

- Refer Fig. 6.7.1 to understand the connection establishment.
- Following steps are taken to establish a connection :
  1. Host A sends a connection request packet to host B. This contains the initialisation information about data from A to B.
  2. Host B sends the packet of acknowledgement to confirm that it has received the request from A.
  3. Host B sends a connection request to A along with the initialisation information about traffic from B to A.
  4. Host A sends a packet of acknowledgement to confirm that it has received the request from B. It is possible to merge the steps 2 and 3.
- Note that each connection request must have a sequence number which is helpful in recovering from the loss or duplication of the packets.
- For the same reason, each acknowledgement also should have an acknowledgement number.
- The first sequence number in each direction should be random for each connection established. This is to ensure that a sender can not create more than one connection which starts with the same sequence number (e.g. 2).



(G-604) **Fig. 6.7.1 : Establishing a connection**

Scanned by CamScanner

- This is important in recognizing the duplicate packets.
- Since a sequence number is required for each connection, the receiver has to keep the history of sequence numbers for each remote host for a specific amount of time but not indefinately.

Problems :

- Establishing a connection sounds easy. But actually it is a very tricky job. The problem occurs when the network can lose store and duplicate packets.
- The problems can be elaborated as follows :
  1. Due to congestion on a subnet, the acknowledgements do not get back in time from receiver to sender. So re-transmission of each packet takes place.
  2. If the subnet uses datagrams inside and every packet travels on a different route, then some of the packets might get stuck in a traffic jam and take a long time to arrive.
  3. The same connection getting re-established due to duplication of packet.
- So the crux of the problem is existence of delayed duplicate packets.

Remedy :

- The solution to this problem is to kill off the aged packets that are still wandering on the network.
- We should ensure that no packet lives longer than some predecided time.
- The packet lifetime can be restricted by using one of the following techniques :
  1. Restricted subnet design.
  2. Putting a hop counter in each packet.
  3. Time stamping each packet.

6.7.2 Three Way Handshake Technique :

MU : May 10, May 11, May 12, Dec. 13, May 15

University Questions

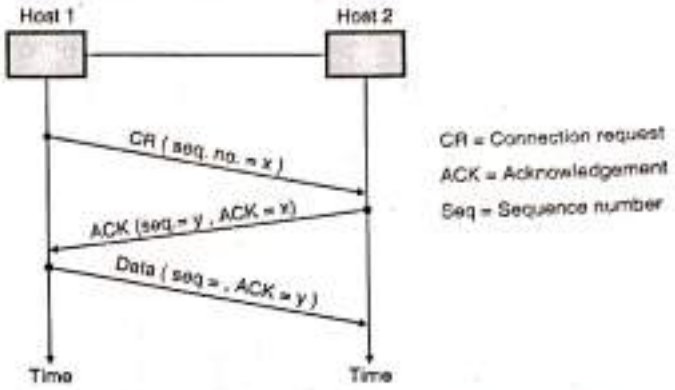
Q. 1 Explain three way handshake technique in TCP. **(May 10, May 11, 10 Marks)**

Q. 2 Explain the three protocol scenarios for establishing a connection using a 3-way handshake in TCP. **(May 12, 10 Marks)**

Q. 3 Show the different protocol scenarios for establishing a connection using 3-way handshake in the transport layer. **(Dec. 13, 10 Marks)**

Q. 4 Explain three way handshake technique in TCP. **(May 15, 10 Marks)**

- The delayed duplicate packet problem can be solved by using a technique called three way handshake.
- The principle of three way handshake is shown in Fig. 6.7.2(a).



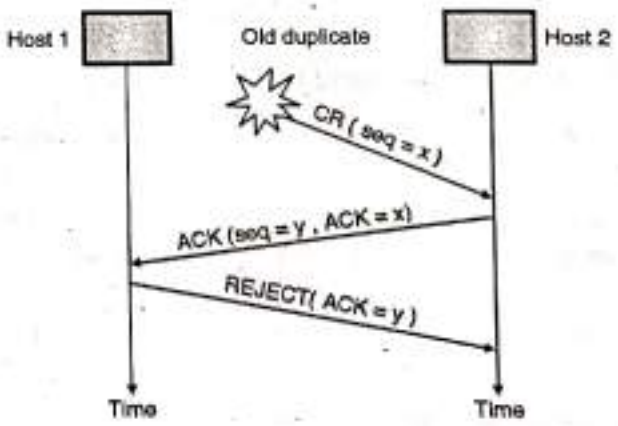
(G-605) **Fig. 6.7.2(a) : Three way handshake technique**

Normal operation :

1. Host 1 chooses a sequence number x and sends a TPDU containing the connection request (CR) TPDU to host 2.
2. Host 2 replies with a connection accepted TPDU to acknowledge x and to announce its own sequence number y.
3. Host 1 acknowledges host 2 and sends the first data TPDU to host 2.

Operation in the abnormal circumstances :

- Now let us see how the three way handshake works in presence of delayed duplicate control TPDUs.
- Refer Fig. 6.7.2(b). The first TPDU is a delayed duplicate CONNECTION REQUEST from an old connection. The HOST 1 does not know about it.



(G-606) **Fig. 6.7.2(b) : Response to an OLD duplicate**

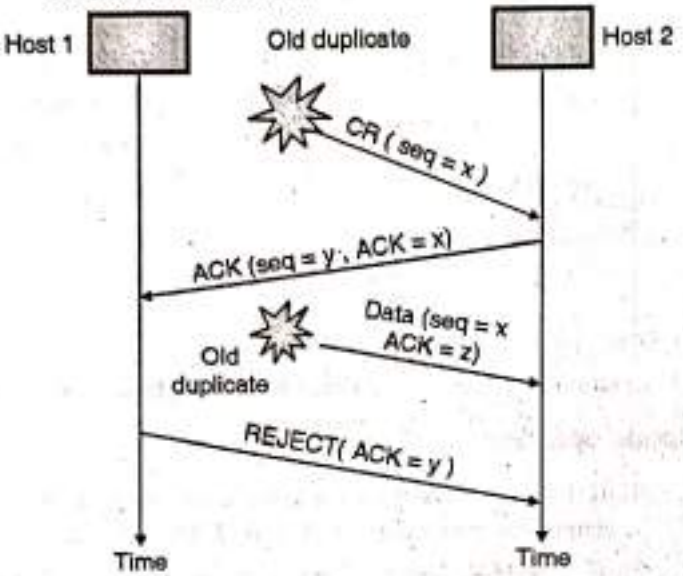
- Host 2 receives this TPDU and sends to host 1, a connection accepted TPDU.
- But host 1 is not trying to establish any connection so it sends a REJECT alongwith ACK = y.

Scanned by CamScanner

- So host 2 realizes that it was fooled by a delayed duplicate and abandons the connection.

Duplicate CR and duplicate ACK :

- This is another abnormal situation. Refer Fig. 6.7.2(c) to understand this situation.



(G-607) **Fig. 6.7.2(c) : Duplicate CR and duplicate ACK**

- This is the worst case in which delayed duplicates of both connection request (CR) and acknowledgement (ACK) are making rounds in the subnet.
- Host 2 gets a delayed duplicate CR and it replies to it by sending ACK. Note that host 2 has proposed a connection with a sequence number y.
- When the second delayed TPDU (duplicate) arrives at host 2 it understands that z has been acknowledged and not y. So it understands that this too is an OLD duplicate.

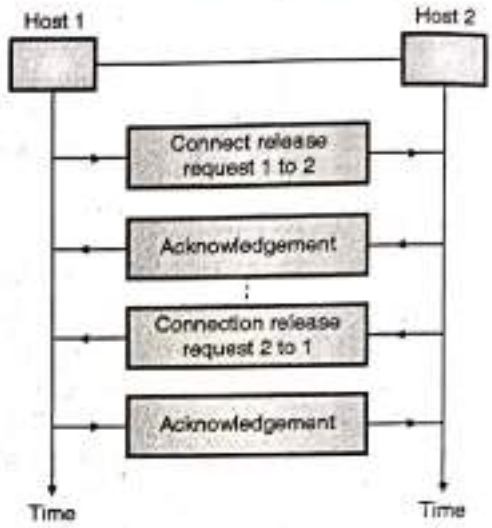
6.7.3 Connection Release :

- Any one of the two parties involved in data exchange can close the connection.
- But the problem is that, when connection is terminated from one end, the other party can continue to send data in the other direction.
- Hence, to ensure a proper connection release one has to follow the steps given below.

Procedure to release a connection :

Refer Fig. 6.7.3 to understand this procedure.

1. Host 1 sends a connection release request to host 2.
2. Host 2 sends an acknowledgement to confirm the release request of host 1.
3. After this the connection is closed in one direction (no data from host 1 to host 2) but host 2 can continue to send data to host 1.
4. When host 2 finishes sending his data, it sends a connection release request to host 1.
5. Host 1 acknowledges (confirms) the request made by host 2 and the connection is released from both ends.



(G-608) **Fig. 6.7.3 : Connection release**

- Releasing a connection is easier than establishing it. There are two styles of releasing a connection :

Types of connecting release :

1. Asymmetric release and
2. Symmetric release

1. Asymmetric release :

In asymmetric release, when one party stops communicating the connection is broken. It is an abrupt release and it may lead to loss of data.

2. Symmetric release :

- Symmetric release treats the connection as two separate unidirectional connections and in order to release the connection each side must release the connection on its side.
- Symmetric release is as shown in Fig. 6.7.3 and there is no loss of data with the symmetrical release.

6.8 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.

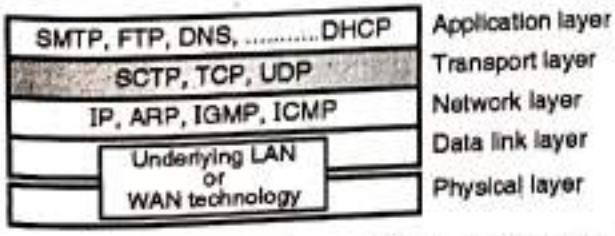
Scanned by CamScanner

6.9 User Datagram Protocol (UDP) :

- The User Datagram Protocol is a very simple protocol. It adds little to the basic functionality of IP. Like IP, it is an unreliable, connectionless protocol.
- You do not need to establish a connection with a host before exchanging data with it using UDP, and there is no mechanism for ensuring that data sent is received.
- A unit of data sent using UDP is called a Datagram. UDP adds four 16-bit header fields (8 bytes) to whatever data is sent.
- These fields are : a length field, a checksum field, and source and destination port numbers. "Port number", in this context, represents a software port, not a hardware port.
- The concept of port numbers is common to both UDP and TCP. The port numbers identify which protocol module sent (or is to receive) the data.
- Most protocols have standard ports that are generally used for this. For example, the Telnet protocol generally uses port 23. The Simple Mail Transfer. Protocol (SMTP) uses port 25. The use of standard port numbers makes it possible for clients to communicate with a server without first having to establish which port to use.
- The port number and the protocol field in the IP header duplicate each other to some extent, though the protocol field is not available to the higher-level protocols. IP uses the protocol field to determine whether data should be passed to the UDP or TCP module.
- UDP or TCP use the port number to determine which application-layer protocol should receive the data.
- Although UDP isn't reliable, it is still a preferred choice for many applications. It is used in real-time applications like Net audio and video where, if data is lost, it's better to do without it than send it again out of sequence. It is also used by protocols like the Simple Network Management Protocol (SNMP).

Relationship with other protocols :

- The relationship of UDP with the other protocols and layers of TCP/IP suite is as shown in Fig. 6.9.1. As shown, UDP is located between IP and application layer. It therefore works as an intermediary between application program and the network layer.



(G-2019) **Fig. 6.9.1 : Relation between UDP and other protocols**

6.9.1 Responsibilities of UDP :

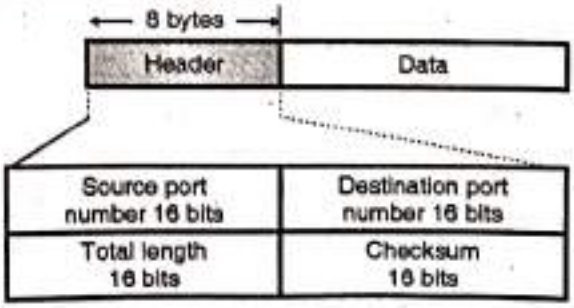
- Being a transport layer protocol, the UDP has the following responsibilities :
  1. To create a process to process communication, UDP uses port numbers to accomplish this.
  2. To provide control mechanisms at the transport layer, UDP does not provide flow control or acknowledgements. It provides error detection. The erroneous packet is discarded.
  3. UDP does not add anything to the services of IP except for providing process to process communication.

6.9.2 Advantages of UDP :

- UDP, despite all its simplicity and powerlessness is still used because it offers the following advantages :
  1. UDP has minimum overheads.
  2. UDP can be easily used if the sending process is not too bothered about reliability.
  3. UDP reduces interaction between sender and receiver.

6.9.3 User Datagram :

- User Datagram Protocol (UDP) provides a connectionless packet service that offers unreliable 'best effort' delivery. This means that the arrival of packets is not guaranteed, nor is the correct sequencing of delivered packets.
- Applications that do not require an acknowledgement of receipt of data, for example, audio or video broadcasting uses UDP.
- UDP is also used by applications that typically transmit small amounts of data at one time, for example, the Simple Network Management Protocol (SNMP).
- UDP provides a mechanism that application programs use to send data to other application programs. UDP provides protocol port numbers used to distinguish between multiple programs executing on a single device.
- That is, in addition to the data sent, each UDP message contains both a destination port number and a source port number. This makes it possible for the UDP software at the destination to deliver the message to the correct application program, and for the application program to send a reply.
- UDP packets are called as **user datagrams.** They have a fixed-size header of 8-bytes. The format of user datagram is as shown in Fig. 6.9.2.



(G-624) **Fig. 6.9.2 : User datagram format**

Scanned by CamScanner

- 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 Number :

- Source port is an optional field, when meaningful, it indicates the port of the sending process, and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.
- This is a 16 bit field. That means the port numbers can range from 0 to 65,535.
- If the source host is a client, means if a client is sending a request using UDP, then generally a **ephemeral (temporary)** port number is requested by the process and chosen by the UDP.
- If the source host is a server that means if a server is sending a response message, mostly the **well known port** number is used.

Destination Port Number :

- The destination port number also is a 16 bit number and this port number is used by the process running on the destination host.
- If the destination host is a server that means if a client is sending a request to it, then a **well known port** number is used in most cases.
- However if the destination host is a client than means if a server is sending its response to it, then the chosen port number is generally an **ephemeral port** number.

Length :

- It is also a 16 bit field which is used for defining the total length of the UDP datagram including header as well as data. Due to 16 bit length it can define a total length of the datagram upto 65,535 bytes.
- However practically the total length of a UDP datagram is much smaller than 65,535 bytes. This is because the UDP datagram is to be stored in an IP datagram which itself has a length of 65,535 bytes.
- The **length** field in the UDP datagram is actually not necessary, because this UDP datagram is actually encapsulated in an IP datagram and the IP datagram has its own length field.
- So without using the length field in UDP datagram, we can obtain the length of the UDP datagram as follows :

  UDP length = IP length – IP header length

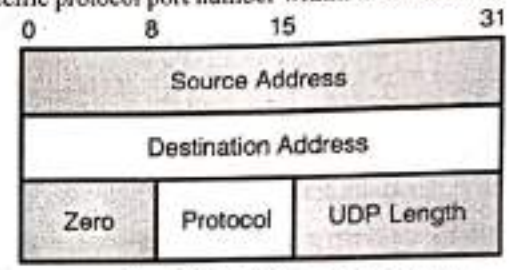
- Note that while delivering the UDP datagram to UDP layer, the IP software drops the IP header.

UDP Checksum :

This is used to verify the integrity (i.e. to detect errors) of the UDP header. The checksum is performed on a "pseudo header" consisting of information obtained from the IP header (source and destination address) as well as the UDP header.

6.9.4 UDP Pseudo Header :

- The purpose of using a pseudo-header is to verify that the UDP packet has reached its correct destination.
- The correct destination consists of a specific machine and a specific protocol port number within that machine.



(G-625) **Fig. 6.9.3 : UDP pseudo header**

- The UDP header itself specifies only the protocol port number. Thus, to verify the destination, UDP on the sending machine computes a checksum that covers the destination IP address as well as the UDP packet.
- At the ultimate destination, UDP software verifies the checksum using the destination IP address obtained from the header of the IP packet that carried the UDP message.
- If the checksum agrees, then it must be true that the packet has reached the intended destination host as well as the correct protocol port within that host.

User Interface :

- A user interface should allow the creation of new receive ports, receive operations on the receive ports that return the data octets and an indication of source port and source address, and an operation that allows a datagram to be sent, specifying the data, source and destination ports and addresses to be sent.

IP Interface :

- The UDP module must be able to determine the source and destination Internet addresses and the protocol field from the Internet header.
- One possible UDP/IP interface would return the whole Internet datagram including the entire Internet header in response to a receive operation. Such an interface would also allow the UDP to pass a full Internet datagram complete with header to the IP to send.
- The IP would verify certain fields for consistency and compute the Internet header checksum.

Scanned by CamScanner

Protocol Application :

- The major uses of this protocol are the Internet Name Server, and the Trivial File Transfer.

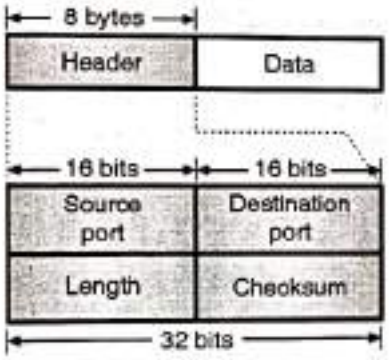
Protocol Number :

- This is protocol 17 (21 octal) when used in the Internet Protocol.

Ex. 6.9.1 : The dump of a UDP header in hexadecimal format is as follows :
B C 8 2 0 0 0 D 0 0 2 B 0 0 1 D
Obtain the following from it :
1. Source port number
2. Destination port number
3. Total length
4. Length of the data.
5. Packet direction.
6. Name of client process.

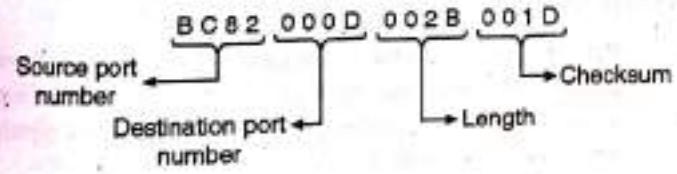
Soln. :

- The standard format of UDP header has been shown in Fig. P. 6.9.1.



(G-2020) **Fig. P. 6.9.1 : UDP header format**

- Therefore we can split the given UDP header in 4 equal parts as follows :



(G-2021)

1. Source port number = $(BC82)_{16}$ ...Ans.
2. Destination port number = $(000D)_{16}$ ...Ans.
3. Total length of UDP packet = $(002B)_{16} = (43)_{10}$ bytes ...Ans.
4. Length of data = Total length – Length of the header. = 43 – 8 = 35 bytes ...Ans.
5. Destination port number is $(000D)_{16} = (13)_{10}$
   - It is a well known port. Hence the direction of UDP packet travel is from client to server.
6. The client process can be obtained from Table 6.10.1 which shows that for well known port number 13, the corresponding client process is "Daytime".

6.10 UDP Services :

- In this section we are going to discuss the following important services provided by the UDP :
  1. Process to process communication.
  2. Connectionless services.
  3. Flow control.
  4. Error control.
  5. Checksum.
  6. Congestion control.
  7. Encapsulation and decapsulation.
  8. Queuing.
  9. Multiplexing and demultiplexing.

6.10.1 Process to Process Communication :

- We have already discussed the process to process communication in a general sense, earlier in this chapter.
- UDP also does it with the help of sockets which is a combination of IP address and port numbers. Table 6.10.1 shows different port numbers used by UDP.

Some of these ports can be used by UDP as well as TCP.

Table 6.10.1 : Well known ports used with UDP

Port	Protocol	Description
7	Echo	The received datagram is echoed back to sender.
9	Discard	Any received datagram is discarded.
11	Users	Active users.
13	Daytime	Return the day and the current time.
17	Quote	Return the quote of the day.
19	Chargen	To return a string of characters.
53	Nameserver	Domain Name Service (DNS).
67	BOOT PS	This is the server port to download the bootstrap information.
68	BOOT PC	This is the client port to download bootstrap information.
69	TFTP	Trivial File Transport Protocol.
111	RPC	Remote Procedure Call.
123	NTP	Network Time Protocol.
161	SNMP	Simple Network Management Protocol.
162	SNMP	Simple Network Management Protocol (Trap).

Scanned by CamScanner

6.10.2 Connectionless Services :

- As UDP is a connectionless, unreliable protocol, each user datagram sent using UDP is an independent datagram.
- Different user datagrams sent by the UDP have absolutely no relationship between them. This is true even for those datagrams which are originating from the same process and being sent to the same destination. The user datagrams **do not have any number.**
- Also the connection establishment and release are not at all required. So each datagram is free to travel any path.
- Only those processes which are sending very short messages can successfully use the UDP.

6.10.3 Flow and Error Control :

- Being a connectionless protocol, UDP is a simple, unreliable protocol. It does not provide any flow control, hence the receiver can overflow with incoming messages.
- UDP does not support any other error control mechanism, except for the checksum.
- There are no acknowledgements sent from destination to sender. Hence the sender does not know if the message has reached, lost or duplicated. If the receiver detects any error using the checksum, then that particular datagram is discarded.

6.10.4 Checksum :

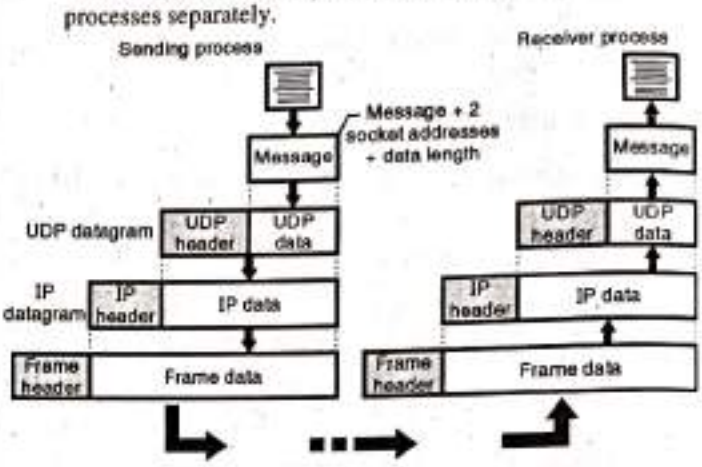
- The calculation of checksum for UDP is different than that for IP. In UDP the checksum is calculated by considering the following three sections :
  1. A pseudoheader
  2. The UDP header.
  3. The data coming from the application layer.
- The checksum in UDP is **optional.** That means the sender can make a decision of not calculating the checksum. If so, then the checksum field is filled with all zeros before sending the UDP packet.
- In case if the calculated checksum is all zeros (when the sender decides to send checksum) then an all 1 checksum is sent.
- This solution works without any problem because, a checksum will never have an all 1 value.

6.10.5 Congestion Control :

- UDP does not provide any congestion control. It assumes that the UDP packets being small, will not create any congestion.
- But this assumption may not always be correct.

6.10.6 Encapsulation and Decapsulation :

- The UDP encapsulates and decapsulates messages in an IP datagram in order to exchange the message between two communicating processes.
- This is as shown in Fig. 6.10.1. We will discuss the two processes separately.



(a) Encapsulation (b) Decapsulation

(G-2022) **Fig. 6.10.1**

Encapsulation :

- Refer Fig. 6.10.1(a). The message produced by a process is to be sent with the help of UDP. The process passes the message and two socket addresses alongwith the length of data to UDP.
- UDP receives this data and adds the UDP header to it as shown. This is called as UDP datagram which is passed to IP with the socket address.
- IP adds its own header to UDP datagram as shown. It enters value 17 into the protocol field. This is an indication that UDP is being used. The IP datagram is then passed on to the data link layer.
- The DLL adds its own header and possibly a trailer to create a frame and sends it to the physical layer.
- Finally the physical layer converts these bits into electrical or optical signals and sends them to the destination machine.

Decapsulation :

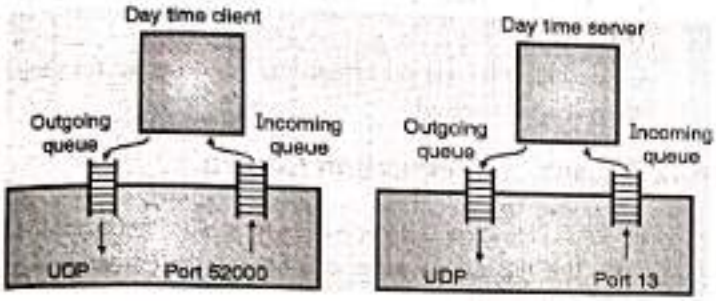
- Refer Fig. 6.10.1(b) for understanding of the decapsulation process. The encoded message arrives at the destination physical layer where it decodes the electrical/optical signals into bits and passes them to the DLL.
- The DLL checks the data using header and trailer. The header and trailer are discarded if no errors are found, and the datagram is passed to IP.
- The IP carries out its checking to find the errors and if none are found, the datagram is passed on to UDP, after dropping the IP header.
- The datagram from IP to UDP also contains the sender and receiver IP addresses. This entire user datagram is checked by the UDP with the help of checksum.
- If there is no error detected, then the UDP header is dropped and the application data plus senders socket address are handed over to the process.

Scanned by CamScanner

- The process can use this senders socket address if it wants to respond to the message received.

6.10.7 Queuing :

- The queues in UDP are related with ports as shown in Fig. 6.10.2.

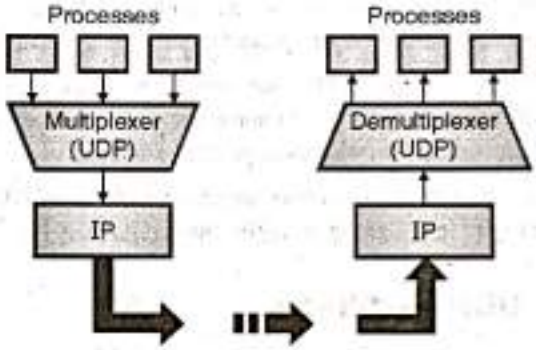


(G-626)**Fig. 6.10.2 : Queues in UDP**

- A process starts at the client site by requesting a port number from the operating system. In some implementations both incoming and outgoing queues are created in association with each process.
- Every process gets only one port number and hence it can create one outgoing and another incoming queue. The queues function only when the process is running. They are destroyed as soon as the process is terminated.
- The client process uses the source port number mentioned in the request to send message to its outgoing queue.
- UDP removes the queue messages one by one by adding the UDP header and delivers them to IP.
- If the outgoing queue overflows, then operating system tells that client process to wait before sending the next message.
- When the client receives a message, UDP checks if the incoming queue has been created or not. If the queue has been created, then the UDP sends the received datagram to the end of the queue.
- If the queue is not present then UDP will simply discard the user datagram. If the incoming queue overflows, then UDP discards the user datagram and arranges to send the port unavailable message to the server.
- The mechanism to create the server queue is different. The server creates the incoming and outgoing queues using its well known port as soon as it starts running. The queues exist as long as the server is running.
- When a message is received at the server, the UDP checks if the incoming queue has been created or not.
- If the queue is not present, the UDP discards the user datagram. If the queue is present then UDP sends the datagram at the end of the queue.
- If the incoming queue overflows, then UDP drops the user datagram and arranges to send the port unavailable message to the client.
- When the server wants to send a message to client it sends that message to the outgoing queue. These messages are then removed one by one after adding the UDP header. They are delivered to IP.
- If the outgoing queue overflows then the operating system will ask the server to wait before it sends the next message.

6.10.8 Multiplexing and Demultiplexing :

- We have discussed the general principle of multiplexing and demultiplexing in the transport layer.
- Now let us see how to apply the same principle to UDP. Imagine that a host is running a TCP/IP protocol suite and that there is only one UDP and a number of processes which would like to use the services of UDP.
- UDP handles such a situation by using the principle of multiplexing and demultiplexing as shown in Fig. 6.10.3.



(G-2023) **Fig. 6.10.3 : Multiplexing and demultiplexing**

Multiplexing :

- At the sending end, there are several processes that are interested in sending packets. But there is only one transport layer protocol (UDP or TCP). Thus it is a many processes-one transport layer protocol situation.
- Such a many-to-one relationship requires multiplexing.
- The UDP first accepts messages from different processes. These messages are separated from each other by their port numbers. Each process has a unique port number assigned to it.
- Then the UDP adds header and passes the packet to IP as shown in Fig. 6.10.3.

Demultiplexing :

- At the receiving end, the relationship is one as to many. So we need a demultiplexer.
- First the UDP layer receives datagrams from the IP.
- The UDP then checks for errors and drops the header to obtain the messages and delivers them to appropriate process based on the port number.

Scanned by CamScanner

6.10.9 Comparison of UDP and Generic Simple Protocol :

- In this section we will compare UDP with a simple connectionless transport layer protocol.
- The only difference between the two is that the UDP provides an **optional checksum.**
- If the checksum is added to the UDP packet then at the destination, the receiving UDP can check the packet for any error with the help of the checksum.
- If any error is detected, the receiving UDP will discard that packet, without sending any feedback to the sender.

6.11 UDP Applications :

- Despite being connectionless, unreliable, no flow control, no error control, UDP is still preferred for some applications.
- This is because UDP has some advantages too. An application designer has to sometimes compromise between advantages and drawbacks to get the optimum.
- Here we will discuss some important features of UDP that are useful in designing an application program.

6.12 UDP Features :

6.12.1 Connectionless Service :

- The feature of UDP is that it is a connectionless protocol and that each UDP packet is independent from the other packets, can be considered as an advantage or a disadvantage depending on the requirements of an application.
- In an application, if we want to send only short messages to server and receive short messages from the server. Then the above mentioned feature becomes an advantage.
- The feature of being connectionless is an advantage if request and respond each can fit in one single user datagram.
- The overhead (number packets to be exchanged) required to establish and close a connection is zero in case of UDP. This can be a very important advantage for some applications.
- Similarly the delay involved with the connectionless delivery is very short as compared to that with the connection oriented delivery. Hence the connectionless service provided by UDP is preferred for the applications in which delay is important

6.12.2 Lack of Error Control :

- UDP is an unreliable protocol which does not provide any error control. Now this is actually a disadvantage but it becomes an advantage for some applications as explained below.
- If TCP is used for reliable service and if a packet is lost, then TCP will resend it. So the receiver transport layer is unable to deliver that part of the message to the application immediately. Due to this an uneven delay is introduced between different parts of the messages which is undesirable for some delay sensitive applications.
- This delay is actually a side effect of the reliable operation of TCP.
- Some applications are not affected by this delay but for some others it is very crucial.

6.12.3 Lack of Congestion Control :

- We know that there is no provision for congestion control in UDP. But this disadvantage can become an advantage for some applications.
- A good side effect of lack of congestion control is that UDP does not create any additional traffic that is created by TCP for congestion control.
- Hence the UDP is preferred from some congestion prone networks.

6.12.4 Typical Applications of UDP :

1. UDP is suitable for the applications (processes) that have the following requirements :
   (a) A simple response to request is to be made.
   (b) Flow and error controls not essential.
   (c) Bulk data is not to be sent (like FTP).
2. UDP is used for RIP (Routing Information Protocol).
3. UDP is used for management processes such as SNMP.
4. UDP is suitable for the processes having inbuilt flow and error control mechanisms, such as TFTP.
5. UDP is suitable for the multicasting applications.
6. UDP is also used in the real time applications which do not tolerate the uneven delays.

6.13 Transmission Control Protocol (TCP) :

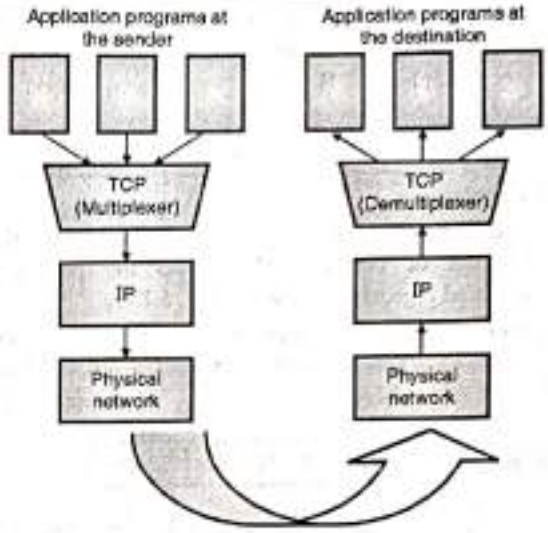
- The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model.
- Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.
- TCP is the layer 4 protocol in the TCP/IP suite and it is a very important and complicated protocol. TCP has been revised multiple times in last few decades.
- With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers.

Scanned by CamScanner

- 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.

6.13.1 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. 6.13.1.
- 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. 6.13.1.

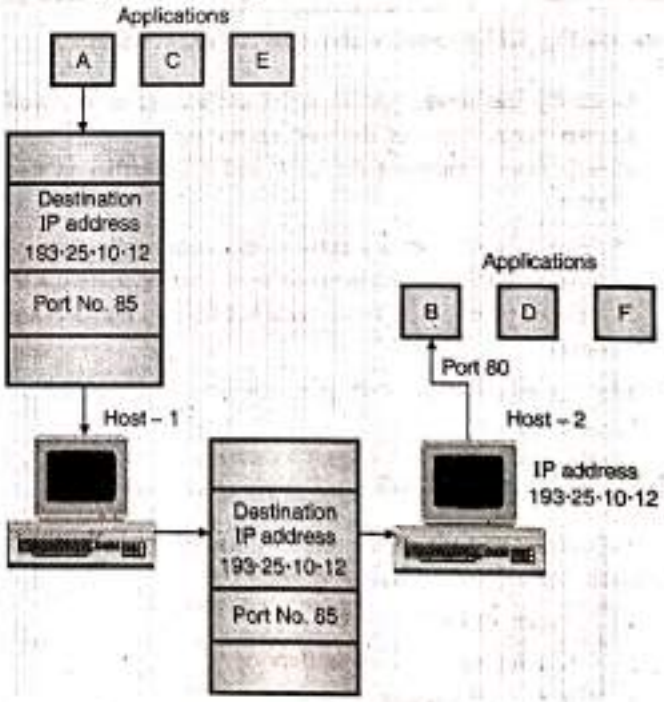


(G-1440) **Fig. 6.13.1 : Multiplexing and demultiplexing using TCP**

6.13.2 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. 6.13.2 and explained below.



(G-1437) **Fig. 6.13.2 : Use of port numbers**

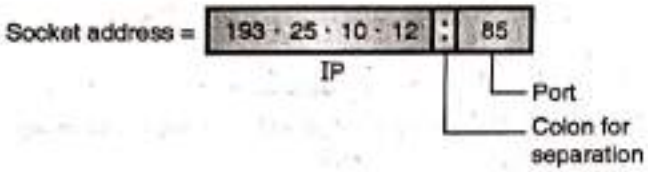
- Application A running on computer 1 provides the IP address of computer 2 and the port number corresponding to application B as shown in Fig. 6.13.2.

Scanned by CamScanner

- Computer 1 communicates with computer 2 using the IP address and computer 2 uses the port number to direct the message to application B.

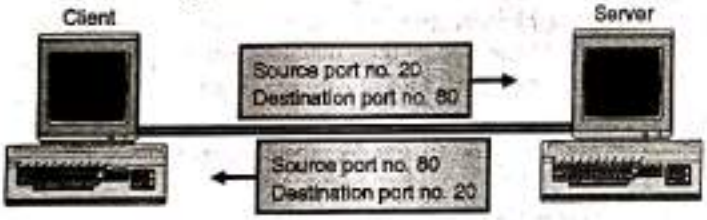
2. Sockets :

- A port is a 16 bit unique number used for identification of a single application.
- But socket address or simply socket would identify the combination of the IP address and the port number concatenated together as shown in Fig. 6.13.3.
- For example if the IP address = 193.25.10.12 and the port number is 85. Then this port of this computer will have the following socket address.



(G-1438) **Fig. 6.13.3**

- 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. 6.13.4.



(G-1436) **Fig. 6.13.4 : Source and destination port numbers**

- Generally the server port numbers are known as the **well known ports.** Some of the well known port numbers have already been mentioned for UDP and TCP earlier in this chapter.
- Multiple TCP connections between different applications or same applications on two hosts exist in practice. Here the IP addresses of the two hosts are same but the port numbers are different.
- The communication using port numbers is illustrated in Fig. 6.13.4.

6.14 TCP Services :

Following are some of the services offered by TCP to the processes at the application layer :

1. Stream delivery service
2. Sending and receiving buffers
3. Bytes and segments
4. Full duplex service
5. Connection oriented service
6. Reliable service.
7. Process to process communication.

6.14.1 Process to Process Communication :

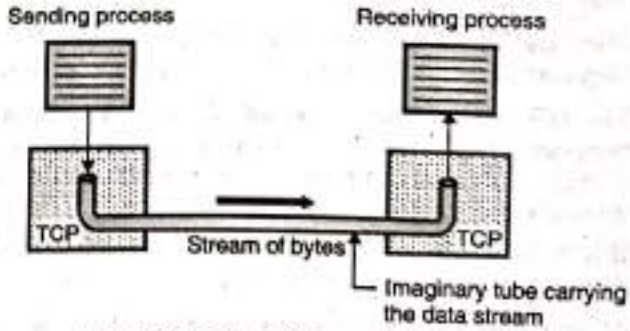
- The TCP uses port numbers a transport layer addresses. Table 6.14.1 shows some well known port numbers used by TCP.
- Note that if an application can use both UDP and TCP, the same port number is assigned to this application.

Table 6.14.1 : Well known ports used by TCP

Port	Protocol	Description
7	Echo	Sends received datagram back to sender
9	Discard	Discards any received packet
11	Users	Active users
13	Daytime	Sends the date and the time
17	Quote	Sends a quote of the day
19	Chargen	Sends a string character
20	FTP, Data	File Transfer protocol for data
21	FTP, Control	File Transfer protocol for control
23	TELNET	Terminal network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

6.14.2 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. 6.14.1.
- This is called as stream delivery service.



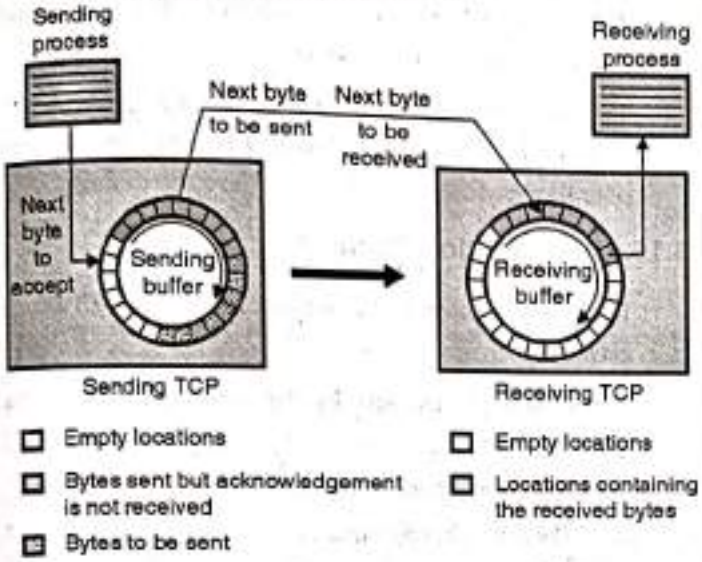
(G-621) **Fig. 6.14.1 : Stream delivery service**

6.14.3 Sending and Receiving Buffers :

- The sending and receiving processes may not produce and receive data at the same speed.

Scanned by CamScanner

- Hence TCP needs buffers for storage of data at both the ends. There are two types of buffers used in each direction :
  1. Sending buffer
  2. Receiving buffer.
- A buffer can be implemented by using a circular array of 1 byte locations as shown in Fig. 6.14.2.



(G-622)**Fig. 6.14.2 : Sending and receiving buffers**

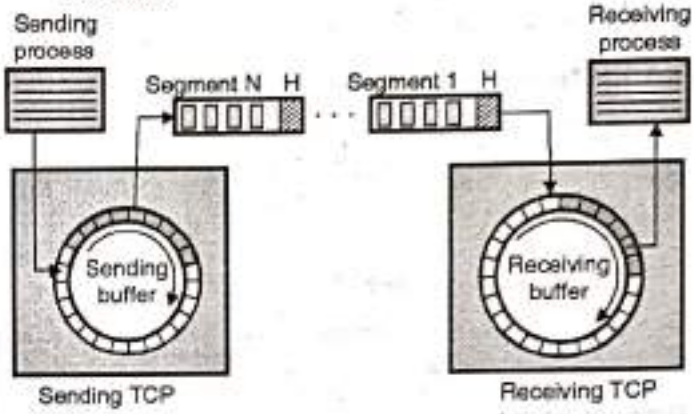
- Fig. 6.14.2 shows the direction of movement of data. The sending buffer has three types of locations :
  1. Empty locations
  2. Locations containing the bytes which have been sent but not acknowledged. These bytes are kept in the buffer till an acknowledgement is received.
  3. The locations containing the bytes to be sent by the sending TCP.

In practice, the TCP may be able to send only a part of data which is to be sent, due to slowness of the receiving process or congestion in the network.

- The buffer at the receiver is divided into two parts :
  1. The part containing empty locations.
  2. The part containing the received bytes which can be consumed by the sending process.

6.14.4 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. 6.14.3 shows the creation of segments from the bytes in the buffers.



(G-623)**Fig. 6.14.3**

- The segments are not of the same size. Each segment can carry hundreds of bytes.

6.14.5 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.

6.14.6 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.

Scanned by CamScanner

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 ultiples 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 :

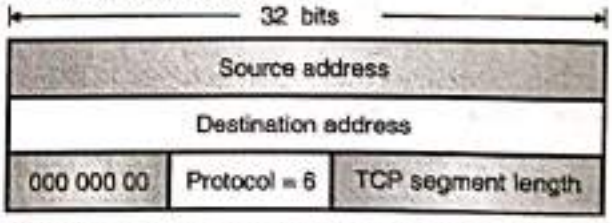
Because options may vary in size, it may be necessary to "pad" the TCP header with zeros so that the segment ends on a 32-bit word boundary as defined by the standard.

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.

6.16.3 Checksum :

- A checksum is provided to ensure extreme reliability. It checksums the header, the data and the conceptual pseudo header shown in Fig. 6.16.3.



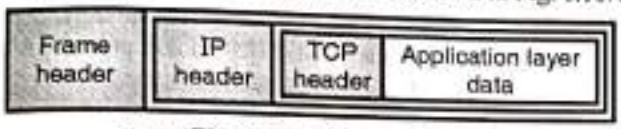
(G-612)**Fig. 6.16.3 : The pseudo header included in the TCP checksum**

- 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. 6.16.3.

Scanned by CamScanner

6.16.4 Encapsulation :

- The data coming from the application layer is encapsulated in a TCP segment. This TCP segment is then encapsulated in an IP datagram.
- The IP datagram is encapsulated in a frame at the data link layer. The process of encapsulation is shown in Fig. 6.16.4.



(G-2072) **Fig. 6.16.4 : Encapsulation**

6.17 A TCP Connection :

- TCP is a connection oriented protocol. Such a protocol would establish a virtual path between the sender and the receiver.
- Multiple segments corresponding to the message are then sent over this virtual connection.
- As TCP is using the same single path for the entire path, it can use the same path for acknowledgements and retransmission of damaged or lost packets.
- While discussing the relation between TCP and IP we have seen how TCP uses the services of IP.
- TCP operates at a higher level than IP and the TCP connection is virtual and not physical.
- Though IP delivers the individual segments to the destination, the entire control on the connection is exercised by TCP.
- If a segment is lost or damaged, the TCP makes a decision of its retransmission, and IP does not know anything about it.
- The **three phases** in the connection oriented TCP transmission are as follows :

  1. Connection establishment 2. Data transfer and
  3. Connection termination.

6.17.1 TCP Connection Establishment :

MU : Dec. 03

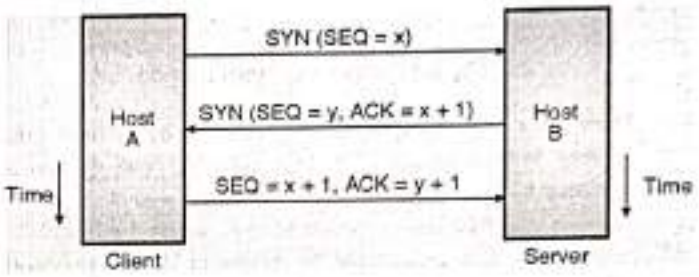
University Questions

Q. 1 Show how TCP connection setup protects against the situation in :

Draw the space time diagram for protocol message exchange and explain how the protocol works.

(Dec. 03, 10 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. 6.17.1(a).



(G-613) **Fig. 6.17.1(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.

6.17.2 Connection Termination Protocol [Connection Release] :

MU : Dec. 03

University Questions

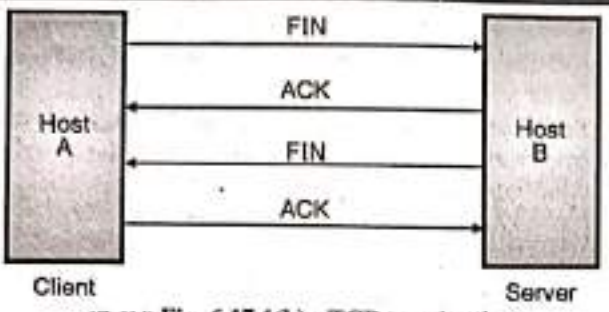
Q. 1 Show how TCP connection setup protects against the situation in :

Draw the space time diagram for protocol message exchange and explain how the protocol works.

(Dec. 03, 10 Marks)

- While it takes three segments to establish a connection, it takes four to terminate a connection.
- Since a TCP connection is full-duplex (that is, data flows in each direction independently of the other direction), the connection should be terminated in both the directions independently.
- The termination procedure in each direction is shown in Fig. 6.17.1(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.

Scanned by CamScanner



(G-614) **Fig. 6.17.1(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. 6.17.1(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.

6.17.3 TCP Connection Management :

MU : Dec. 03, Dec. 15, May 17, Dec. 17

University Questions

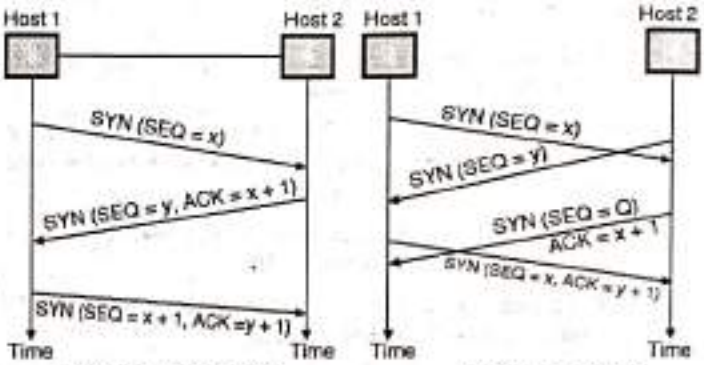
Q. 1 Show how TCP connection setup protects against the situation in :

Draw the space time diagram for protocol message exchange and explain how the protocol works. **(Dec. 03, 10 Marks)**

Q. 2 Write short notes on : TCP connection management **(Dec. 15, 10 Marks)**

Q. 3 Explain with the help of suitable diagram TCP connection management and release. **(May 17, Dec. 17, 10 Marks)**

- Connections are established in TCP by following the three-way handshake technique.
- To establish a connection, one side, say the server, passively waits. It executes the LISTEN and ACCEPT primitives, to specify either a particular other side or nobody in particular.
- The other side (client) executes a connect primitive, with the IP and the port specified. The other information is the maximum TCP segment size, possible other options and optionally some user data (e.g. a password).
- The CONNECT primitive sends a TCP segment with the SYN bit on and the ACK bit off and waits for a response.
- The sequence of TCP segments sent in the normal case is shown in Fig. 6.17.2(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.



(a) Normal operation **(b) Call collision**

(G-615) **Fig. 6.17.2 : TCP connection management**

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. 6.17.2(b).
- Under such circumstances only one connection is established. Both the connections can not be established simultaneously because connections are identified by their end points.
- If the first set up results in a connection which is identified by (x, y) and second connection is also set up, then only one table entry will be made i.e. for (x, y).
- For the initial sequence number a clock based scheme is used, with a clock pulse coming after every 4 μsec.
- 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.

6.17.4 TCP Connection Release :

MU : May 17, Dec. 17

University Questions

Q. 1 Explain with the help of suitable diagram TCP connection management and release. **(May 17, Dec. 17, 10 Marks)**

Scanned by CamScanner

- A TCP connection is actually a full duplex connection but to understand the connection release we will assume that it is a pair of simplex connections.
- We can then think that each simplex connection is getting terminated independently.
- Releasing a TCP connection is identical on both ends. Each side can send a TCP segment with the FIN bit set, meaning it has no more data to send.
- After receiving a FIN, the Acknowledge (ACK) signal is sent and that direction is shut down, but data may continue to flow indefinitely in the other direction.
- If the sender of FIN does not receive the ACK within 2 maximum packet lifetimes, it releases the connection. The receiver will eventually notice that it receives no more data and time-out as well.
- Normally four TCP segments are required to release a connection i.e. one FIN and one ACK in each direction.
- However the first ACK and second FIN can be combined in the same segment.

Connection reset :

- The connection reset in TCP can take place when TCP at one end done any one of the following :
  1. It may deny a connection request.
  2. It may abort the existing connection.
  3. It may terminate an idle i.e. non operating connection.
- TCP does all the three with the help of the RST (reset flag).

6.18 TCP State Transition Diagram :

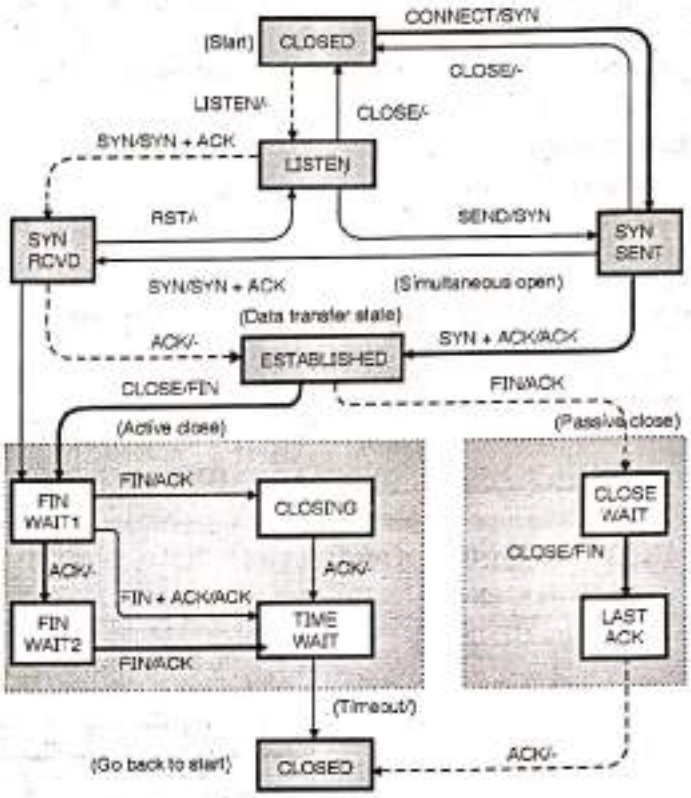
- The steps to be followed in TCP connection establishment and release can be represented using a finite state machine.
- The total eleven states in such a state machine are given in Table 6.18.1.

Table 6.18.1 : 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 6.18.1, 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. 6.18.1.



(G-696) **Fig. 6.18.1 : 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. 6.18.1. They have different meanings as stated below :-
  1. **Heavy solid lines :** These lines show a client actively connecting to a passive server.
  2. **Heavy dotted lines :** These lines are used for the server.
  3. **The light faced lines :** These are for unusual event sequences.
- Over each line in Fig. 6.18.1 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.

Scanned by CamScanner

- 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. 6.18.1, 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).

6.19 Windows in TCP : MU : Dec. 10

University Questions

Q. 1 Discuss the window management in TCP transmission policy with a neat diagram. **(Dec. 10, 5 Marks)**

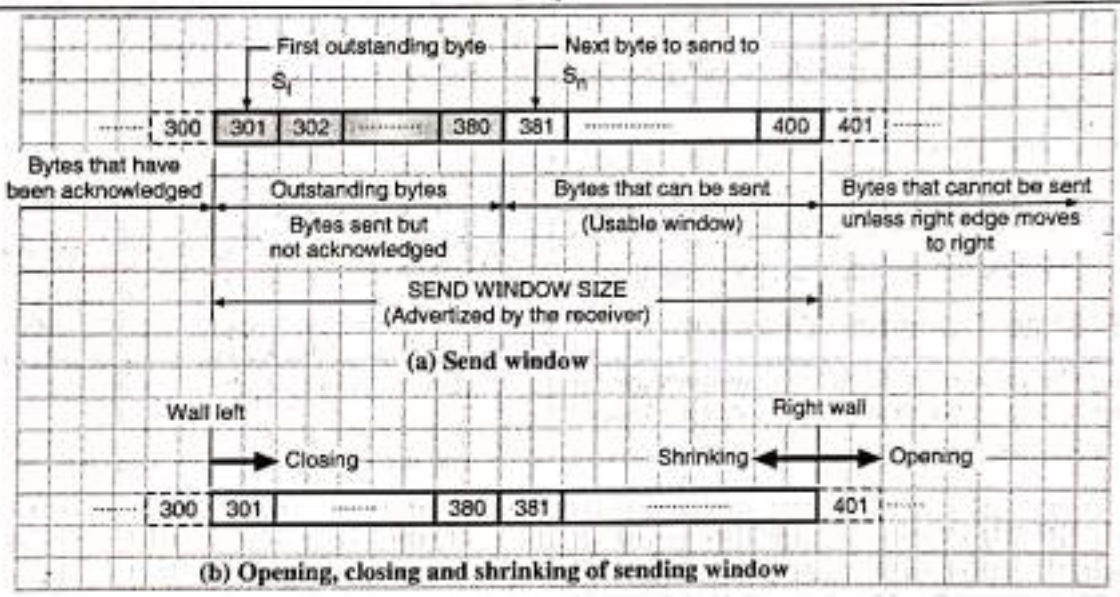
- In this section we will discuss the windows used in TCP. There are two types of windows used in TCP :
  1. Send window 2. Receive window
- Send window is for sending data and receive window is for receiving data. Therefore there will be four windows in all for a two way communication.
- However in order to make the discussion simple, we will assume that the communication takes place only in one direction (client to server or the other way round).

6.19.1 Send Window : MU : Dec. 10

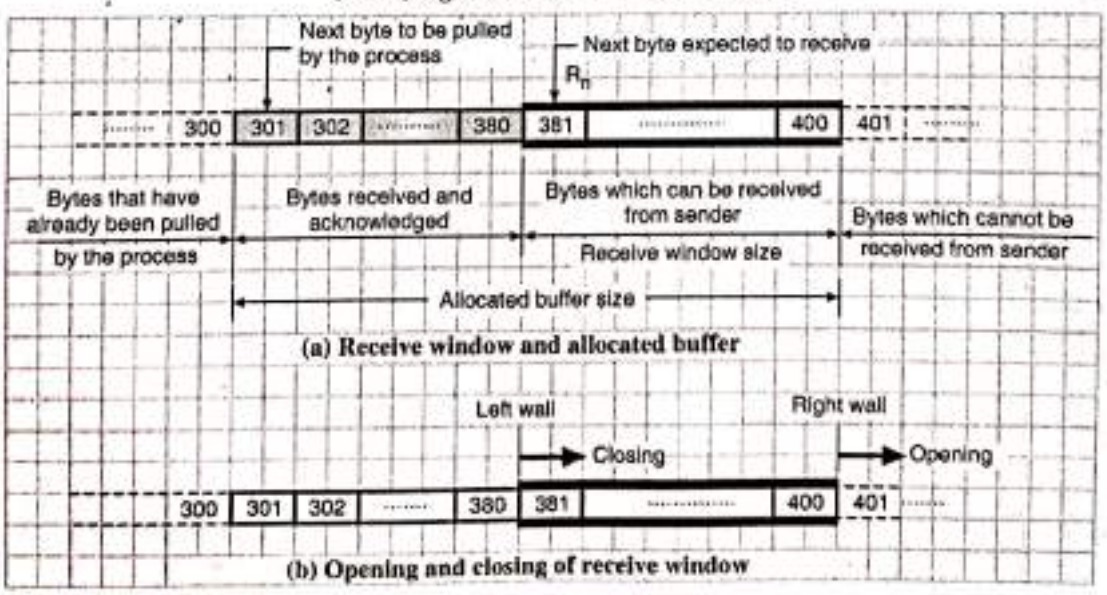
University Questions

Q. 1 Discuss the window management in TCP transmission policy with a neat diagram. **(Dec. 10, 5 Marks)**

- Fig. 6.19.1 illustrates an example of send window. In reality the send window can have a size of thousands of bytes however for simplifying the discussion a 100 byte send window has been considered in Fig. 6.19.1.



(G-1800) **Fig. 6.19.1 : Send window in TCP**



(G-1801) **Fig. 6.19.2 : Receive window in TCP**

Scanned by CamScanner

- The size of send window is dependent on the receiver (flow control) as well as on the congestion control.
- There are three operations that can take place in the send window, namely : open, close and shrink.
- The send window in TCP is similar to that in selective repeat request (SR) with the following differences :
  1. The SR send window numbers pockets but TCP send window numbers bytes. In TCP the transmission takes place in the form of segments but the controlling parameters of windows are expressed in bytes.
  2. Actually TCP is capable of storing data received from the process and send it later on. But we will assume that the sending TCP sends the segments of data as soon as it is received from the process.
  3. TCP uses only one timer as compared to several timers used by the SR protocol. This timer in TCP is used for error control.

6.19.2 Receive Window :

MU : Dec. 10

University Questions

Q. 1 Discuss the window management in TCP transmission policy with a neat diagram. **(Dec. 10, 5 Marks)**

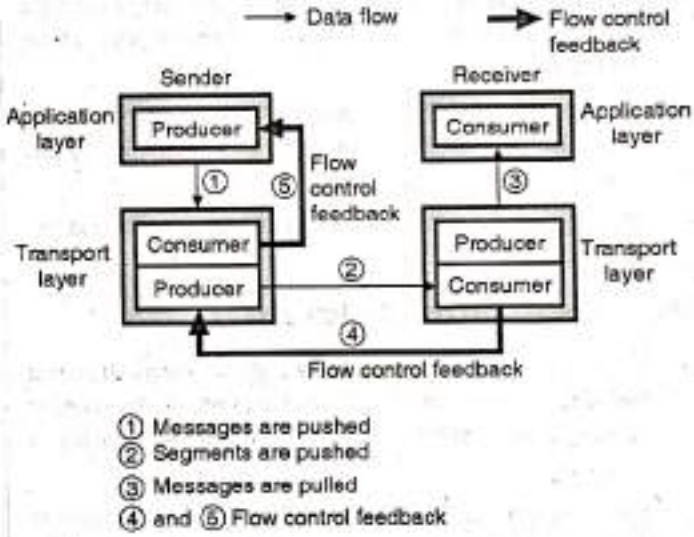
- The example of receive window has been shown in Fig. 6.19.2. In reality the receive window can have size of thousands of bytes however for simplification of discussion a 100 byte receive window has been shown in Fig. 6.19.2.
- The receive window in TCP is similar to that in selective repeat request (SR) with the following differences :
  1. The receiving process in TCP is allowed to pull data as per its own speed. That means in a part of allocated buffer there are bytes which have been received and acknowledged but waiting for the receiving process to pull them (see Fig. 6.19.2). The size of receive window is therefore always smaller than the allotted buffer size. The size of the receive window will decide the number of bytes a receiver can receive without causing the flow control problems. The receiver window size which is denoted by "rwnd" is expressed as follows :

rwnd = Buffer size – Number of acknowledged bytes to be pulled

  2. The acknowledgements in SR define the uncorrupted received packets only. This is selective acknowledgement. However in TCP the mechanism of acknowledgement is called as **cumulative acknowledgement** in which the next expected byte to be received (R_n = 381 in Fig. 6.19.2) is announced. The new version of TCP uses both selective and cumulative mechanisms for acknowledgements.

6.20 Flow Control :

- The flow control is a technique used for controlling the data rate of the sender so that the receiver is not overwhelmed.
- In TCP the flow control has been kept separate from the error control. So when the flow control is being discussed, we will temporarily ignore the error control. i.e. we assume that the data transmission is taking place over an errorfree channel.
- Refer Fig. 6.20.1 which shows the data transfer taking place in only one direction from the sender to receiver. We can apply the same principle to the bidirectional data transfer.
- Two different types of signals travel between the sending process and the receiving process in Fig. 6.20.1. They are data and flow control feedback signals.
- The data flow takes place from the sending process to the sending TCP (denoted by ①), then from sending TCP to receiving TCP (denoted by ②) and finally from receiving TCP to receiving process (denoted by ③).



(G-1802) **Fig. 6.20.1 : Data flow and flow control feedback in TCP**

- Thus flow of data takes place from sender to receiver. But the flow control feedback signals travel from the receiver to sender as shown. They flow from receiving TCP to sender TCP (denoted by ④) and from sending TCP to sending process (denoted by ⑤).
- Most TCP versions however, do not provide the flow control feedback facility. Instead the receiving process is allowed to pull data from receiving TCP whenever the receiving process becomes ready.
- Thus the receiving TCP controls the sending TCP (due to flow control feedback) and the sending TCP controls the sending process as far as the data rate of the sending process is concerned.
- Consider the flow control feedback path denoted by ⑤ in Fig. 6.20.1. This feedback is practically achieved by simply rejecting the data by sending TCP when its window is full.
- So now let us concentrate on the flow control feedback signal from receiving TCP to sending TCP, denoted by path ④ in Fig. 6.20.1. i.e. how does the receiving process control the sending TCP.

Scanned by CamScanner

6.20.1 Opening and Closing Windows :

- In TCP the flow control is achieved by forcing the sender and receiver to adjust their window sizes. The size of the buffer for both sender and receiver will not be changed. It will remain fixed in size.
- Consider the receive window shown in Fig. 6.20.3. This window closes by moving its left wall to the right in response to arrival of more bytes from the sender.
- The receive window of Fig. 6.20.3 will open by moving its right wall towards right when the receiver process pulls more bytes from the receiver buffer.
- The send window can open, close or shrink in order to exercise the flow control. All the three functions of the send window are controlled by the receiver.
- The send window closes by moving its left wall to the right (see Fig. 6.20.3) in response to a new acknowledgement from the receiver.
- The send window opens by moving its right wall to the right when the advertised receive window size (rwnd) by the receiver allows it to do so.
- The send window may shrink on occasion. It is assumed that this situation does not arise.

6.20.2 Shrinking of Windows :

- As we know, the receiver window does not shrink. However the send window can shrink in the event of the receiver defining a value of "rwnd" which results in the shrinking of windows.
- Some versions of TCP do not allow the send window to shrink. That means they do not allow the right wall of the send window to move to the left.
- The receiver can prevent the shrinking of send window by maintaining the following relationship between the last and new acknowledgement and the last and new "rwnd" values.

$$\underbrace{(\text{new ackNo} + \text{new rwnd})}_{\text{New position of the right wall with respect to sequence number space}} \geq \underbrace{(\text{last ackNo} + \text{last rwnd})}_{\text{Old position of the right wall}}$$

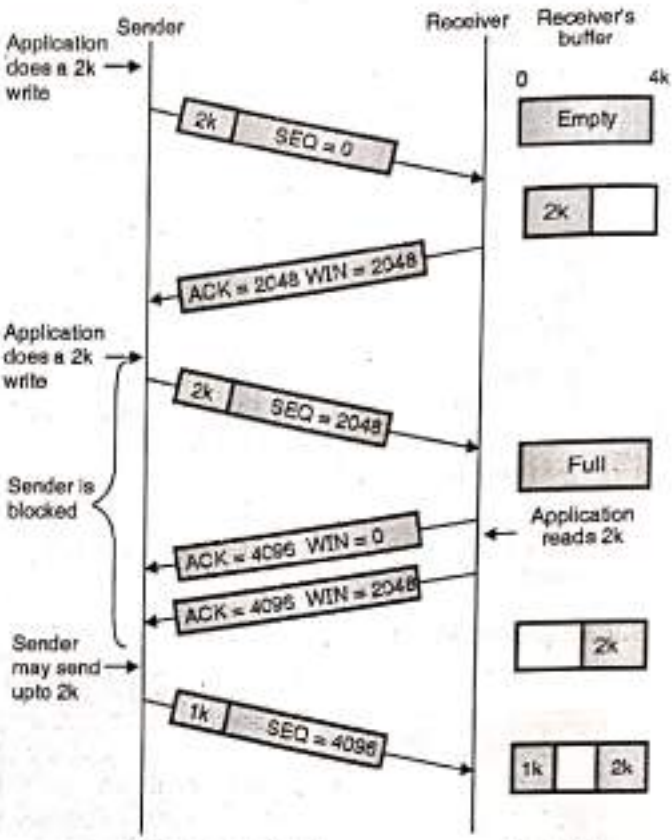
(G-1803)

- The above relationship shows that the right wall should not move to the left.

6.20.3 An Example of Flow Control :

- 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. 6.20.2.



(G-616) **Fig. 6.20.2 : Windows management in TCP**

Explanation :

- Let the receiver in Fig. 6.20.2, has a 4 kbyte i.e. 4096 byte buffer space.
- The sender transmits a 2048 byte (2 kbyte) segment with a sequence number SEQ = 0. These bytes occupy half space of the receiver's buffer and the receiver will send back acknowledgement of this segment (ACK 2048, WIN = 2048).
- Here WIN = 2048 is the window which tells the sender that an empty buffer space of 2048 is available on the receiver side.
- Now the sender sends another 2k i.e. 2048 bytes segment (SEQ = 2048) which is acknowledged by the receiver (ACK = 4096, WIN = 0) which shows that window = 0 because the receiver buffer space is 0. ACK = 4096 indicates that the receiver has received 4096 bits successfully.
- The sender must now be blocked until the application process on the receiver removes some data from the buffer and some buffer space becomes available.
- As soon as the application on the receiver side reads 2k bytes, the buffer becomes partially empty and an acknowledgement with a window of 2k (ACK = 4096,

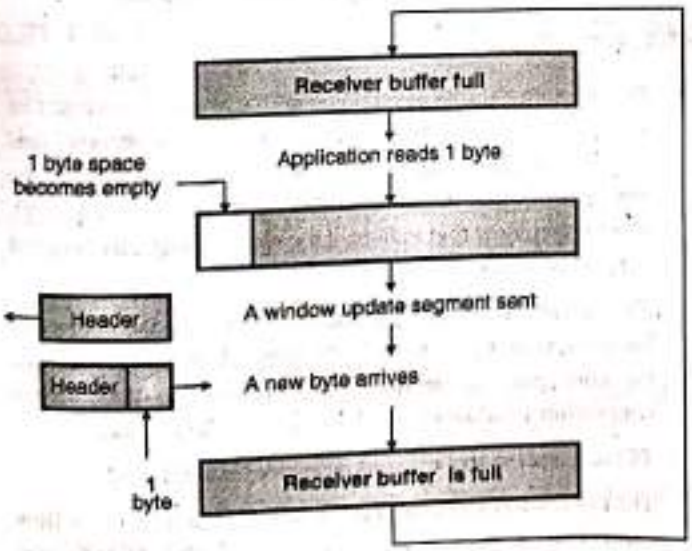
Scanned by CamScanner

WIN = 2048) is sent back to sender. Here WIN = 2048 indicates the empty buffer space on the receiver side.

- The sender may send upto 2 kbytes.
- When the window = 0, the sender should not normally send any segment. But under two exceptional conditions the sender will continue to send data even when it receives WIN = 0.
  1. First, urgent data may be send, e.g. to allow the user to kill the process running on the other machine.
  2. Second, the sender may send a 1-byte segment to make the receiver reannounce the next byte expected and the window size. This is used to prevent the possible confusion if a window announcement gets lost.
- Senders are not supposed to transmit data as soon as the data is obtained from an application. The receivers also are not supposed to send acknowledgements as soon as they receive it.
- This is done in order to reduce the usage of the system. One way to reduce the system usage is to use an algorithm called Nagle's algorithm is used.

6.20.4 Silly Window Syndrome :

- 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. 6.20.3.



(G-617) **Fig. 6.20.3 : Silly window syndrome**

1. Initially the receiver's buffer is full so it send a window size 0 to block the sender.
2. But the interactive application reads one byte from the buffer. So one byte space becomes empty.
3. The receiving TCP sends a window update to the sender informing that it can send 1 byte.
4. The sender send 1-new byte.
5. The buffer is full again and the window size is 0. This process can continue forever. This is known as the silly window syndrome.

6.20.5 Nagle's Algorithm :

- The Nagle's algorithm is very simple. It takes into account the speed of transmission of the sender and the speed of the network which is transporting the data. The algorithm is as follows :
  1. The first piece of data received from the sending application program is send by the sending TCP even if it is only 1 byte.
  2. Once the first segment is sent, the sending TCP will wait and accumulate data in the output buffer until either the acknowledgement is received from the receiving TCP or sufficient data is accumulated to fill the maximum size segment.
  3. Step 2 is repeated for the remaining transmission.
- If the sending application program data rate is higher than the speed of data transporting network then the segments are larger (maximum size segments). On the other hand if the sending application program is slower than the data transport network, the segments will be smaller than the maximum segment size.

Clark's solution to silly window syndrome :

- Clark suggested a solution to silly window syndrome as follows.
- He suggested that the receiver should not send a window update for 1 byte. Instead the receiver must wait until it has a considerable amount of buffer space available and then send the window update.
- To be specific, the receiver should wait until it can handle the maximum window size it has advertised at the time of establishing a connection or its buffer is half empty, whichever is smaller.
- The sender can also help to improve the situation. It should not send tiny segments. Instead it must wait and send a full segment or at least one containing half of the receivers buffer size.

Scanned by CamScanner

6.21 TCP Congestion Control :

MU : May 07, Dec. 07, May 08, May 09, Dec. 09, May 13, Dec. 14

University Questions

Q. 1 Explain how TCP controls congestion. **(May 07, May 09, 10 Marks)**

Q. 2 What is congestion control ? How it is different from flow control ? Explain various congestion prevention techniques. **(Dec. 07, 10 Marks)**

Q. 3 What is congestion ? Explain how it can be avoided. **(May 08, 10 Marks)**

Q. 4 How TCP controls the congestion ? **(Dec. 09, 10 Marks)**

Q. 5 How TCP controls the congestion, explain in detail. **(May 13, 10 Marks)**

- We have already discussed the reasons of congestion in networks and the Internet is no exception. So there are congestions occurring on Internet too.
- The network layers detects the congestion by looking at the growing queues at the routers and tries to manage it by dropping packets.
- The network layer has to give feedback to the transport layer about the possible congestion because only then the transport layer can reduce the sender's data rate.
- In the Internet, TCP plays a major role in controlling congestion. A control law called AIMD (Additive Increase Multiplicative Decrease) can be used in response to binary congestion signals received from the network. According to this law, in response to congestion signals the transport protocol should converge to a fair and efficient bandwidth allocation.
- TCP congestion control is based on this approach using a **window** and with a loss of packet used as the binary signal to indicate congestion.

Principle of congestion control :

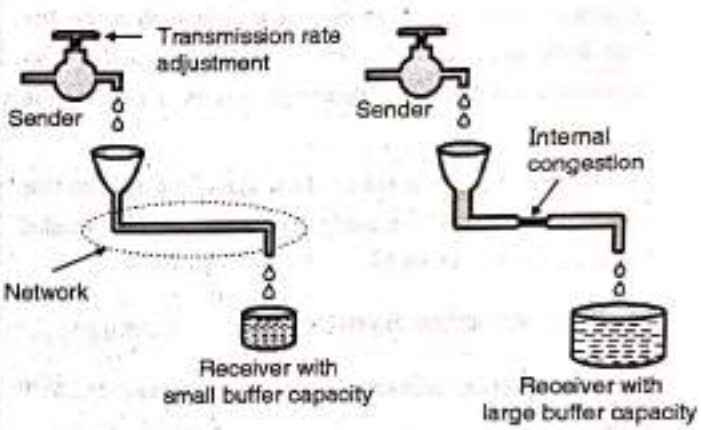
- The basic principle is do not inject a new packet into the network until an old one is delivered.
- TCP tries to do this by dynamically adjusting the window size. The steps followed in achieving the congestion control in TCP are as follows :

Step 1 : Detect the congestion :

- This is the first step in congestion control. Now-a-days packet loss due to transmission errors is very rare because the optical fiber links are being used. So most transmission time-outs (loss of packets) are due to congestions.
- So all the Internet TCP algorithms assume that time-outs are caused by congestion and so time outs can be used to detect the congestion.

Step 2 : Try to prevent congestion :

- After establishing a connection, a suitable window size is to be chosen. The receiver window size is based on its buffer capacity. If the sender adjusts its transmission rate according to this capacity as shown in Fig. 6.21.1(a), the congestion due to buffer overflow will never take place.
- Now consider Fig. 6.21.1(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.



(a) No congestion **(b) Internal**

(G-618) **Fig. 6.21.1 : Congestion**

Conclusion :

- To prevent congestion TCP has to deal with two problems separately – receiver capacity and network capacity.

Solution :

- To deal with the two problems mentioned earlier each sender maintains two windows : the window the receiver has granted (which indicates the receiver capacity) and the **congestion window** (which indicates the network capacity). The first window that indicates the receiver capacity is called as the **flow control window.**
- The size of the congestion window is equal to the number of bytes the sender may have in the network at any time. Hence the corresponding **sending rate** is equal to the ratio of **congestion window size** and the **RTT** of the connection.
- TCP adjusts the size of window as per the AIMD rule.
- The **congestion window** is maintained in addition to the **flow control window** (Which specifies the number of bytes that the receiver can buffer).

Scanned by CamScanner

- 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 AMID congestion window and added it to the existing TCP.
- While doing so he made following two important considerations :
  1. The rate at which the acknowledgements return to the sender is approximately equal to the rate at which packets can be sent over the slowest link in the path. This is the rate a sender wants to use to avoid congestion. This timing is known as **ACK clock** and it is an essential part of TCP. Using ACK clock TCP smoothes out traffic and avoids congestion.
  2. The second consideration was that AMID 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.

6.21.1 Slow Start Algorithm : MU : Dec. 07

University Questions

Q. 1 What is congestion control ? How it is different from flow control ? Explain various congestion prevention techniques. **(Dec. 07, 10 Marks)**

1. After establishing a connection, the sender initialises the congestion window to the size which is equal to the maximum segment in use on the connection. It then sends one maximum segment.
2. If this segment is acknowledged by the receiver indicating no congestion, it adds bytes corresponding to one full segment to the congestion window. So now the congestion window size is equal to two maximum size segments. The sender then sends two segments.
3. As each of these segments is acknowledged indicating that there is no congestion, the size of congestion window is increased by one maximum segment size. This is shown in Fig. 6.21.2. This is the exponential growth of the congestion window size.
4. When the congestion window is of n segments, if all n segments are acknowledged before time-out takes place, the congestion window is increased by the byte count corresponding to n segments.
5. But there is a limit on the exponentially growing congestion window. The congestion window stops growing as soon as either the time-out occurs or the receiver's window size is reached.
6. If the congestion window can grow to 1024 (1 kbyte) byte, 2048 byte, but a burst of 4096 bytes gives a time-out then we have to set the congestion window at 2048 in order to avoid congestion.
7. Once this is done, no data bursts longer than 2048 bytes will be sent by the sender even if receiver grants a wider window.
8. The name of this algorithm is slow algorithm and it is required to be supported by all the TCP implementations.

6.21.2 Internet Congestion Control Algorithm : MU : Dec. 07

University Questions

Q. 1 What is congestion control ? How it is different from flow control ? Explain various congestion prevention techniques. **(Dec. 07, 10 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. 6.21.2.
- Table 6.21.1 is used to plot the graph of Fig. 6.21.2. See how the threshold point acts as the boundary of the exponential growth and linear growth of the congestion window.

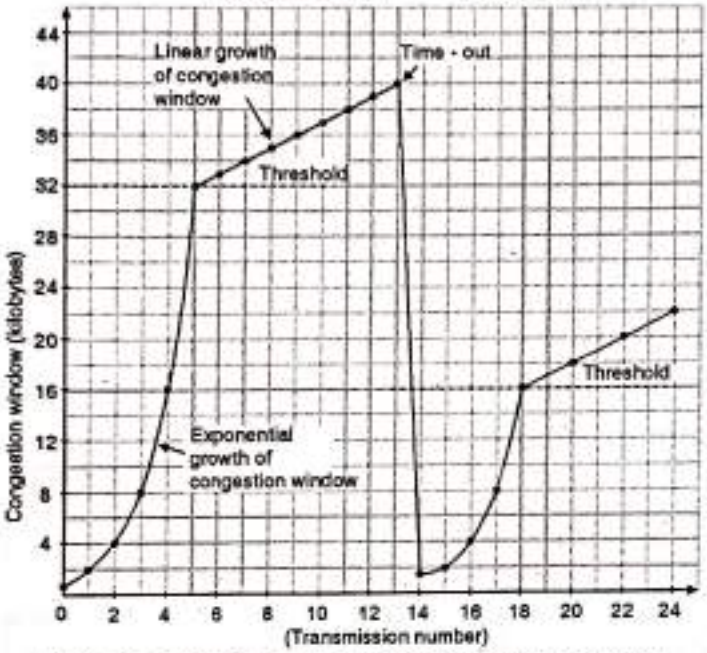
Scanned by CamScanner

(G-619(a)) **Table 6.21.1**

Threshold — Time - out

Transmission number	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Congestion window kilobytes	2	4	8	16	32	33	34	35	36	37	38	39	40	1

Exponential growth — Linear growth



(G-619) **Fig. 6.21.2 : Internet congestion control algorithm**

- 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. 6.21.2)
- Then the congestion window grows exponentially till the congestion window size reaches the threshold of 32 k.
- The threshold occurs at 32 k and the congestion window grows linearly after this point.
- The time-out occurs as the 13th transmission. Therefore the new threshold is set to half the current window (i.e. at 16 k) and slow start is initiated again. The process will repeat thereafter.
- If no more time-outs occur, the size of congestion window continues to grow upto the size of the receiver window.

6.21.3 Congestion Avoidance (Additive Increase) :

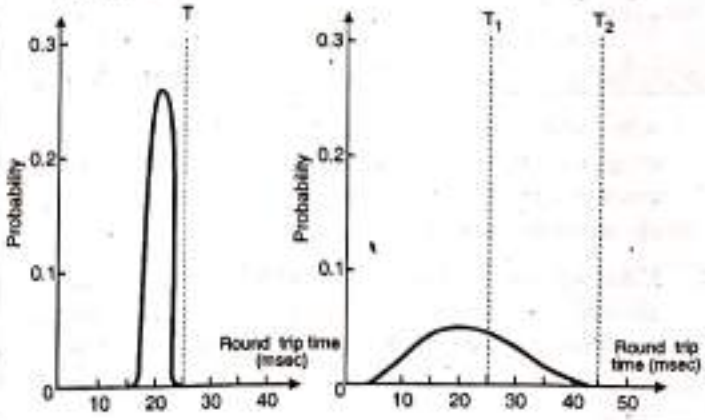
- In the slow start algorithm discussed earlier, the size of the congestion window initially increases exponentially (upto the threshold).
- In order to avoid congestion before it happens, we have to slow down such an exponential growth.
- TCP defines another algorithm called **congestion avoidance** 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. 6.21.2.

6.22 TCP Timer Management :

- The TCP, at least conceptually uses more than one timers. But the most important of them is the **Re-transmission Timer (RTO).**
- This timer is started as soon as a segment is sent. The timer is stopped if the acknowledgement corresponding to the sent segment is received, before the timer expires.
- But if the timer times out before the arrival of an "ack" signal then that segment is re-transmitted and the timer is started again.

What should be the time-out interval ?

- The most important question about the re-transmission timer is that how long should the time-out interval be ?
- The answer to this question is difficult in the transport layer as compared to that in the data link protocol.
- Fig. 6.22.1 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. 6.22.1(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.



(a) Data link layer (b) For TCP

(G-620) **Fig. 6.22.1: Probability density of acknowledgement arrival times**

Scanned by CamScanner

6.22.1 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,

$$SRTT = \alpha\, SRTT + (1 - \alpha)\, R \quad \text{...(6.22.1)}$$

- 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 $2 \times$ RTT. But practical observations showed that such a constant value was not flexible enough in the events of increased loads.
- When the load approaches capacity (maximum value); the delay becomes large and varies to a large extent. This can initiate retransmission when the original packet is still alive.
- Jacobson fixed this problem by making the time out value sensitive to the variance in RTT as well as the smoothed round trip time SRTT.
- In order to implement this change, we need to keep track of another smoothed variable called RTTVAR (Round Trip Time VARiation) which is updated by the following formula,

$$RTTVAR = \beta\,(RTTVAR) + (1 - \beta)\,|SRTT - R| \quad \text{...(6.22.2)}$$

- The typical value of $\beta = 3/4$. The retransmission timeout RTO is set by the following expression,

$$RTO = SRTT + (4 \times RTTVAR) \quad \text{...(6.22.3)}$$

- 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.

6.22.2 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 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.

6.22.3 Other Timers in TCP :

1. Persistence timer :

- The second timer in TCP is called **persistence timer.** It is designed to solve the following problem :

1. The receiver sends an ACK with window size = 0. So the sender will wait for the receivers buffer to have some free space.
2. After the receiver buffer becomes partially empty it sends a window update to the sender asking it to send.
3. But the packet containing this window update is lost on its way to sender.
4. So both sender and receiver will be waiting for ever.

- To solve this problem, the persistence timer is used. If it goes off, then sender transmits a probe to the receiver.
- The receiver sends the window size in response to this probe.
- If the window size is still zero then the persistence timer is set again and the cycle repeats. But if the window size is nonzero then sender can send data.

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.

Ex. 6.22.1 : If the round trip time is 30 msec and following acknowledgements come in after 26, 32 and 24 msec respectively, What is the new RTT estimate using the Jacobson algorithm ?

Assume suitable value of α.

Scanned by CamScanner

Soln. :

Given : RTT = 30 msec, M = 26, 32, 24 msec

Choose : $\alpha = 7/8$

1. For M = 26 msec :

$$D = \alpha D + (1-\alpha)\,|RTT - M|$$

$$\therefore (1-\alpha)\,D = (1-\alpha)\,|RTT - M|$$

$$\therefore D = |RTT - M| = |30 - 26| = 4 \text{ msec}$$

$$\therefore \text{Time out} = RTT + 4D$$

$$= 30 \text{ ms} + (4 \times 4) = 46 \text{ msec}$$

2. For M = 32 msec :

$$D = |RTT - M| = |30 - 32| = 2 \text{ msec}$$

$$\therefore \text{Time out} = RTT + 4D$$

$$= 30 + (4 \times 2) = 38 \text{ msec}$$

3. For M = 24 msec :

$$D = |RTT - M| = |30 - 24| = 6 \text{ msec}$$

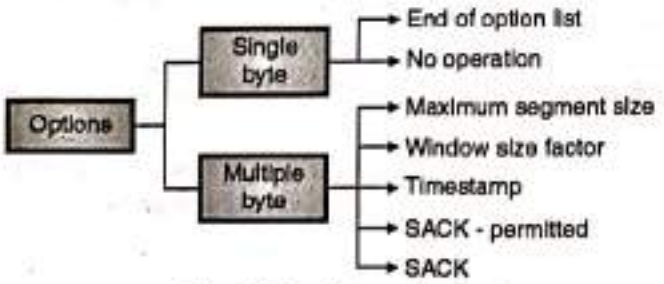
$$\therefore \text{Time out} = 30 + (4 \times 6) = 54 \text{ msec}$$

6.23 Options :

- We have already discussed the TCP header which can contain the optional information of upto 40 bytes.
- The options are there to provide some additional information to the destination or for aligning other options.

Types or categories of options :

- The options can be of two types :
  1. One byte options or
  2. Multiple byte options.
- The one-byte options can be of two types namely : end of option list and no operation.
- The multiple byte options contain five types of options namely : Maximum segment size, window scale factor, timestamp, SACK-permitted and SACK as shown in Fig. 6.23.1.

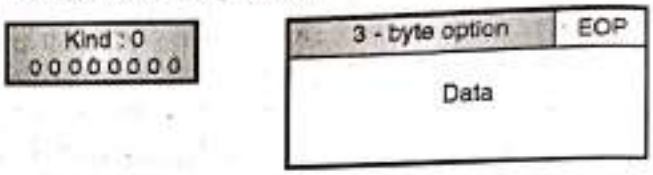


(G-2037) **Fig. 6.23.1 : Categories of options**

- Let us discuss all these options one by one.

6.23.1 End of Option (EOP) :

- EOP is a 1-byte option. It is used when padding is to be done at the end of the option section.
- EOP can be used only as the last option. It is allowed to occur only once.
- Once EOP is received, the receiver will look for the payload data, as shown in Fig. 6.23.2.



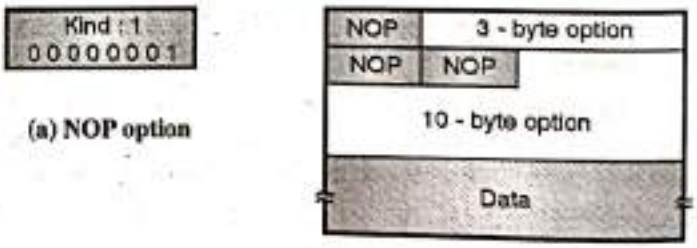
(a) End of option list **(b) Used for padding**

(G-2038) **Fig. 6.23.2 : End of option**

- The information given by EOP to the destination is as follows :
  1. EOP tells the destination that there are no more options in the header.
  2. The beginning of the next 32-bit word is the starting point of the data coming from the application program.

6.23.2 No Operation (NOP) :

- The NOP option is also a 1-byte option. It is used as a **filler** by including it before another option to help in aligning it in a four word slot.
- To understand it, refer Fig. 6.23.3. The NOP is used for aligning one 3-byte option (like window scale factor) and one 10-byte option like timestamp.



(a) NOP option

(b) Used to align beginning of an option

(G-2039) **Fig 6.23.3 : No operation option**

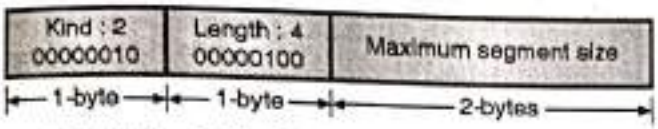
- From Fig. 6.23.3(b) it is evident that we can use the NOP option more than once.

6.23.3 Maximum Segment Size (MSS) :

- Fig. 6.23.4 shows the format of this multiple byte option. MSS option is used for defining the size of the biggest unit of data which a destination of a TCP segment can receive.

Scanned by CamScanner

- The name of this option is slightly misleading, because it actually defines the maximum size of data and not the maximum size of the segment.
- From Fig. 6.23.4 it is seen that this field is 16-bit (2 byte) long. Hence the value can be 0 to 65,635 bytes.



(G-2040) **Fig. 6.23.4 : Maximum segment size option**

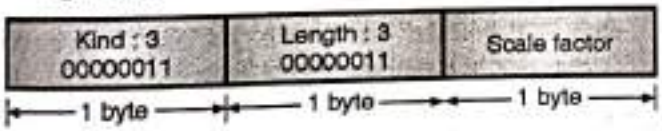
- During the TCP connection establishment, the MSS is defined by each party, for the segment it is going to receive during the connection.
- If a party does not define MSS, then its default value of 536 is used.
- The value of MSS which is fixed during the connection established cannot be changed during the connection.

6.23.4 Window Scale Factor :

- We have seen that there is a field called window size field in the header which defines the size of the sliding window. As this field is 16 bit long the window size can range from 0 to 65,535 bytes.
- The window size of 65,535 bytes appears to be very large but it is not actually true in practice. Even this window size may not be sufficient especially if the data is traveling over a long channel with a large bandwidth.
- Therefore it is necessary to increase the window size further, beyond 65,535 bytes. To do so we can use the **window scale factor.** This can be done as given in the following expression.

$$\text{New window size} = \text{Window size defined header} \times 2^{\text{window scale factor}}$$

- The format of **window scale factor** option has been shown in Fig. 6.23.5.



(G-2041) **Fig. 6.23.5 : Format of window scale factor**

- The other name of scale factor is **shift count** because multiplication by 2 is equivalent to shifting the number being multiplied, to left by one position.
- As shown in Fig. 6.23.5, the scale factor is an 8-bit number. Therefore its maximum value can be 255. But the largest value of scale factor allowed by TCP/IP is only 14.
- Hence the corresponding maximum window size in TCP / IP is given by,

$$\text{Maximum window size} = 2^{16} \times 2^{14} = 2^{30}$$

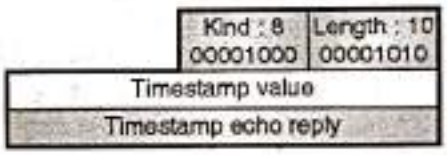
- This maximum window size of 2^{30} bits is less than the maximum value of sequence number. It is important to remember that the window size can never be greater than the maximum value of sequence number.
- It is also possible to obtain the window scale factor only during the connection establishment phase.
- If one end sets the value of window scale factor to 0, then it means that the particular end supports this option, but does not want to use it.

6.23.5 Timestamp :

- Fig. 6.23.6 shows the format of the 10 byte long **timestamp** option.
- The end with active open would announce a timestamp in its connection request segment i.e. SYN segment.
- If it receives a timestamp in next segment (SYN + ACK) from the other end only then it can use the timestamp, otherwise it cannot use it any more.

Applications :

- The two possible applications of timestamp option are as follows :
  1. To measure the round trip time (RTT).
  2. To prevent wrap around sequence numbers.

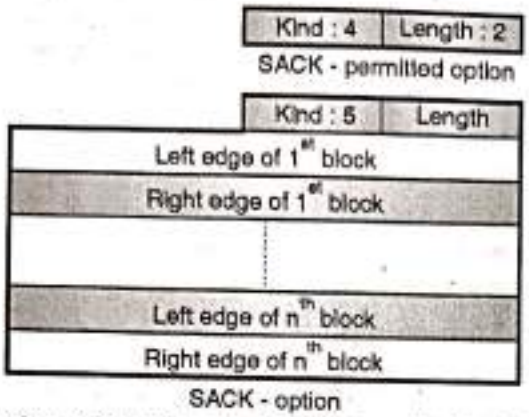


(G-2042) **Fig. 6.23.6 : Format of timestamp option**

6.23.6 SACK-Permitted and SACK Options :

- It has been discussed earlier that, the acknowledgement field in TCP segment has been designed to work as an **accumulative acknowledgement.**
- That means it reports the receipt of the last consecutive byte. It does not report the out of order arrived bytes or the duplicate segments.
- This will affect the TCP performance adversely. In case some packets are lost or dropped, the sender will wait till time - out and resend all the unacknowledged packets. Thus receiver may receive duplicate packets. This degrades the performance of TCP.
- The **selective acknowledgement** (SACK) option was proposed to improve the performance of TCP.
- In this new proposal a list for duplicate packets is also included which allows the sender to resend only those segments which are really lost.
- There are two new options proposed by this new proposal. They are **SACK - permitted** and **SACK** and their formats are as given in Fig. 6.23.7.

Scanned by CamScanner



(G-2043) **Fig. 6.23.7 : Formats of SACK-permitted and SACK options**

SACK - permitted option :

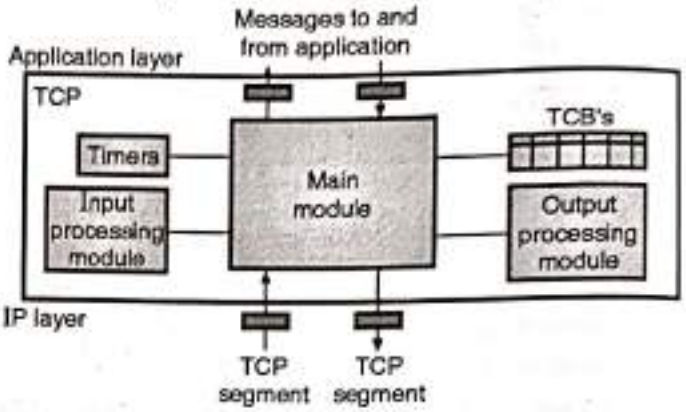
- As shown in Fig. 6.23.7, the SACK - permitted option is of two byte length. This option is used only during the connection establishment.
- The host sending the SYN segment includes the SACK - permitted option into it to announce its support to the SACK - permitted option.
- If the destination host also includes this option in its SYN + ACK segment, then both the hosts can use the SACK option at the time of data transfer.
- It is important to note here that TCP cannot use the SACK - permitted option during the data transfer phase.

The SACK option :

- If both ends agree then the SACK - option can be used only during the data transfer phase. The SACK option is of variable length.
- A list of blocks arriving out of order at the destination is included in this option. Each block is 32-bit long and define the beginning and end of the blocks.
- We can use the first block of SACK option to report the duplicates.

6.24 TCP Package :

- TCP is a connection oriented protocol, with stream service, a complex state diagram, flow control and error control.
- Therefore it is a very complex protocol. It takes tens of thousands of lines of actual code for TCP.
- In this section, a simplified TCP package has been presented. The purpose of doing so is to demonstrate an easy way of simulating the heart of TCP.
- The TCP package is as shown in Fig. 6.24.1. As shown the TCP package consists of following :
  1. Tables called transmission control blocks.
  2. A set of timers.
  3. Three software modules namely the main module, an input processing module and an output processing module.
- Thus in all, there are five components of the TCP package.



(G-2044) **Fig. 6.24.1 : TCP package**

- We will go into details of all these five components of TCP package one by one.

6.24.1 Transmission Control Blocks (TCBs) :

- A connection in the connection oriented protocol TCP may be open for a long time.
- In order to control connections, TCP makes use of a **structure** which holds information about each and every connection.
- Such a structure is known as a **transmission control block (TCB).**
- In TCP at any given time, there can be several connections present. Therefore TCP keeps ready an array of TCBs in a tabular form, which is also referred to as TCB and it is as shown in Fig. 6.24.2.

(G-2045) **Fig. 6.24.2 : TCBs**

- Each TCB contains many fields, such as state, process, pointer ...etc as shown in Fig. 6.24.2.

6.24.2 Timers :

We have discussed earlier in this chapter that there are many TCP timers that are required to keep track of its operations.

6.24.3 Main Module :

- The main module is a very complicated module, as the action to be taken by it depends entirely upon the current state of TCP. (Current state in the TCP state diagram).
- The main module is basically a software module which is invoked by any of the following three events :
  1. Arrival of TCP segment.
  2. A time out event.

Scanned by CamScanner

3. A message from an application program.

- The main module's operation is based on the implementation of TCP state transition diagram.
- Many approaches have been used for implementing the TCP state transition diagram.
- In order to simplify the discussion, we use cases for handling the state (one case per state).
- That means we have to use 11 cases because there are 11 states in the state transition diagram which is to be implemented.
- Each state is implemented as defined in the state transition diagram.

6.24.4 Input Processing Module :

- The input processing module in the TCP package has been designed to handle all the details required to process data or process an acknowledgement received when the TCP is in the ESTABLISHED state.
- The responsibilities of the input processing module are as follows :
  1. To send an ACK if needed.
  2. To take care of announcement of window size.
  3. To carry out error checking.

6.24.5 Output Processing Module :

- The output processing module has been designed to handle all the details needed to send out data received from the application layer program when TCP is in the ESTABLISHED state.
- This module is designed to handle the following :
  1. Retransmission of time outs.
  2. Persistent time-outs.
- This module can be implemented using various approaches. But the one used here uses a small transition diagram to handle different output conditions.

6.25 Comparison of UDP and TCP :

MU : Dec. 04, Dec. 05, Dec. 07, May 11

University Questions

Q. 1 What do TCP and UDP use as transport layer addresses ? List the services offered by both to their upper layers. Bring out the major differences between the two. **(Dec. 04, 10 Marks)**

Q. 2 Differentiate between TCP and UDP. **(Dec. 05, Dec. 07, May 11, 4 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.
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.

Scanned by CamScanner

Characteristic / Description	UDP	TCP
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.

6.26 Socket Programming with TCP :

- Many network applications consist of two programs namely a client program and a server program.
- When these programs are executed a client and a server process are created which communicate with each other by reading from and writing through the sockets.
- When creating a network application, a developer has to write the code for both client and sever programs.
- There are two different types of network applications. The first type of network application is an implementation of a protocol standard defined in, for example RFC.
- For such an implementation, the client and server programs must be written as per the rules of RFC.
- It is possible for two independent developers to write the client and server programs that can operate with each other properly.
- The other type of network application is a proprietary application. In this case the application layer protocol used by the client and server programs may not conform to any existing RFC.
- A single developer or developing team writes the client and server programs. As the code does not implement a public domain protocol, the other independent developers can not develop code that interoperates with the application.
- So when developing a proprietary application, the developer should not use one of the well known port numbers defined in the RFCs.

Key issues in developing proprietary application :

- When developing a proprietary type application, the developer needs to first decide whether the application is to run over TCP or UDP.
- TCP is connection oriented and provides a reliable byte-stream channel for the data to flow between the end systems.
- The UDP is connectionless and sends data in packets between the end systems. But it is an unreliable protocol.
- These TCP and UDP applications are written in Java. It is possible to write the code in C or C++ but Java has many advantages.

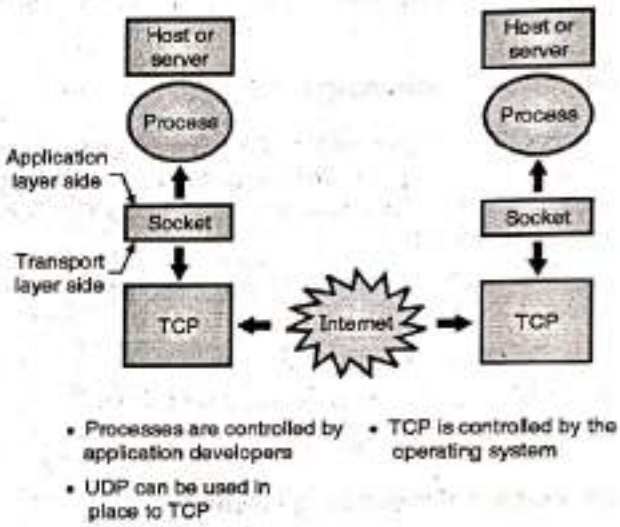
6.26.1 Socket Programming with TCP :

MU : May 16, Dec. 17

University Questions

Q. 1 Write a program for client-server application using socket programming (TCP). **(May 16, Dec. 17, 10 Marks)**

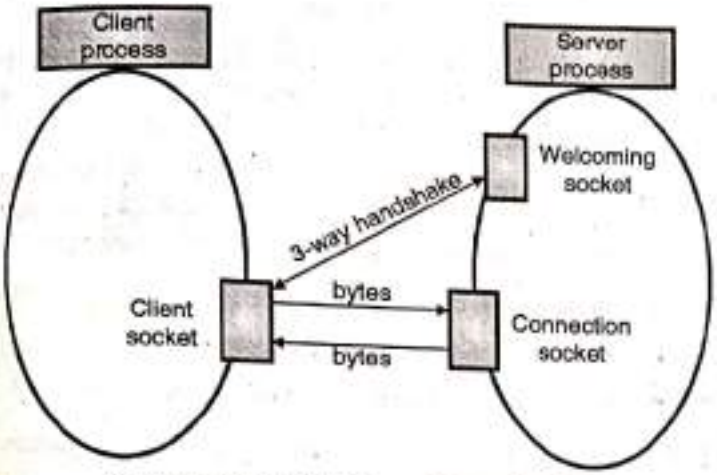
- The processes running on different machines communicate with each other by sending messages into sockets. This is demonstrated in Fig. 6.26.1.



(G-630) **Fig. 6.26.1 : Communicate between processes through TCP sockets**

- Socket acts as a door between the application process and TCP as shown in Fig. 6.26.1. 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.

Scanned by CamScanner



(G-1247) **Fig. 6.26.2 : Different types of sockets**

- 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. 6.26.2.
- 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. 6.26.2.
- 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.

6.26.2 Socket Programming with UDP :

MU : Dec. 16, New Syll. : Dec. 18

University Questions

Q. 1 Write a program for client-server application using Socket Programming (UDP). **(Dec. 16, 10 Marks)**

- As discussed in the previous section, when two processes communicate over a TCP connection, it is equivalent to communicating over a virtual pipe between the two processes.
- This pipe will remain in place until one of the processes terminates the TCP connection.
- The sending process does not have to insert the destination address to the bytes to be sent because the virtual connection is existing.
- Also the pipe provides a reliable byte transfer without altering the sequence in which the bytes are received.
- Like TCP, the UDP also allows two or more processes running on different hosts to communicate. But there is a major difference.
- The first difference is that UDP provides a connectionless service so there is no handshaking process in order to establish the virtual pipe like TCP.
- As there is no virtual pipe existing, when a process wants to send a batch of bytes to the other process, the sending process has to attach the address of the destination process.
- The destination address is a tuple consisting of the IP address of the destination host and the port number of the destination process. The IP address and port number together are called as **"packet"**.
- UDP provides an unreliable message oriented service in which there is no guarantee that the bytes sent by the sending process will reach the destination process.
- After creating a "packet", the sending process will push the packet into the network through a socket. This packet is then driven in the direction of destination process.
- The code for UDP socket programming is different than that for TCP in the following ways :
  1. No need for a welcoming socket as no handshaking is needed.
  2. No streams are attached to the socket.
  3. The sending host has to create packets.
  4. The receiving process has to obtain information from each received packet.

Review Questions

Q. 1 What do you mean by congestion control and QoS ?

Q. 2 What are the parameters of QoS ?

Q. 3 Define the term : Socket.

Q. 4 List the types of socket.

Q. 5 What are the steps used for socket programming ?

Q. 6 What are the elements of transport layer ?

Q. 7 What is difference between IP addresses and port number ?

Q. 8 What are the functions of client and server ?

Q. 9 What problems will occur in establishing a connection ?

Q. 10 What is TCP and UDP ?

Q. 11 Define threshold condition in congestion.

Q. 12 Explain the significance of listen call. Does it apply to all sockets ?

Q. 13 What parameters are specified by its various arguments.

Q. 14 Explain in detail how TCP provides flow control.

Scanned by CamScanner

Q. 15 Define a term silly window syndrome and possible solution to overcome its effect.

Q. 16 What are the techniques used to improve Qos ?

Q. 17 What is fair queueing ?

Q. 18 What are the disadvantages of fair queueing ?

Q. 19 What are the duties of transport layer ? Explain in brief.

Q. 20 Draw and explain the relation between network layer, transport layer and application layer.

Q. 21 What are the transport service primitives ?

Q. 22 Draw and explain the various fields of socket structure.

Q. 23 Explain connection oriented concurrent server.

Q. 24 Write a note on : Addressing in transport layer.

Q. 25 Write note on : Flow control and buffering.

Q. 26 Explain multiplexing and demultiplexing used in transport layer.

Q. 27 Write note on : Crash recovery.

Q. 28 Explain the following issues of transport protocol : Addressing.

Q. 29 State any two socket primitives for TCP and state their function.

Q. 30 Write short notes on two-army problem in releasing a transport connection.

Q. 31 Explain Tom-Winson's three way handshake protocol to establish the transport level connection.

Q. 32 Explain how you will choose between TCP and UDP ? Compare them.

Q. 33 How does TCP tackle congestion problem using the internet congestion control algorithm.

Q. 34 Explain how TCP connections are established using the three way handshake. What happens when two hosts simultaneously try to establish a connection.

Q. 35 What is TCP state machine ? Explain its structure and use with suitable diagram.

Q. 36 Explain TCP connection management with the help of TCP connection management finite state machine.

Q. 37 Explain how TCP connections are established using the three way handshake. What happens when two hosts simultaneously try to establish a connection ?

Q. 38 Write a note on FIFO queueing.

Q. 39 Explain in brief weighted fair queueing.

Q. 40 Explain a congestion control algorithm.

Q. 41 Explain the TCP transmission policy, congestion control.

Q. 42 Explain the following issues of transport protocol :

1. Establishing a connection.
2. Releasing a connection.

Q. 43 Give the structure of UDP header.

Q. 44 Explain the TCP header and working of the TCP protocol.

Q. 45 Explain the various fields of TCP header with the help of neat diagram.

Q. 46 Explain the various steps that are followed in releasing a TCP connection.

6.27 University Questions and Answers (New Syllabus) :

Dec. 2018 [Total Marks : 10]

Q. 1 Write a program for client server application using Socked Programming (UDP).

(Section 6.26.2) **(10 Marks)**

□□□

Scanned by CamScanner

CHAPTER 7

Module 6

Application Layer

Syllabus :

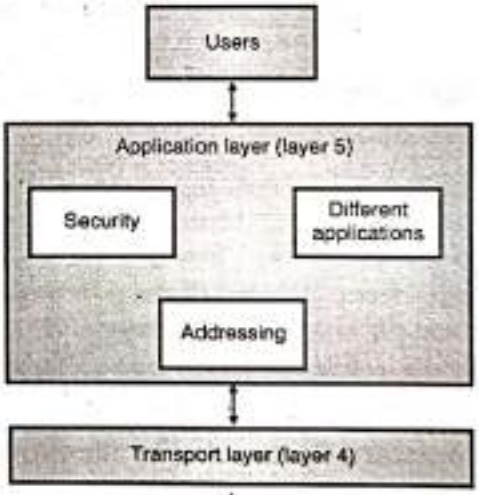
DNS : Name space, Resource record and types of Name server, HTTP, SMTP, Telnet, FTP, DHCP.

7.1 Introduction :

- Application layer is the topmost layer in the TCP/IP protocol suite. The hardware and software of the Internet was designed and developed for providing various types of services at the application layer.
- All the other layers (4 of them) make these services possible. We will discuss various services provided at the application layer first (in this chapter) and later on study the supporting role of the other layers, providing these services.
- Many application programs have been created and used during the lifetime of the Internet. Some of them could never become standards. Some others have become obsolete. Some have been modified, other have been replaced by new ones.
- But some applications have survived the test of time and have become standard applications.
- Everyday new application protocols are being added to Internet.
- The Internet can provide services via two types of applications :
  1. The traditional applications.
  2. The new applications.
- The traditional applications make use of the **client server** paradigm whereas the new applications are based on the **peer-to-peer** paradigm.
- The application layer provides communication with the help of a **logical connection** which is an **imaginary connection** between the application layers of the two communicating computers. This is not the physical connection.
- The actual communication however involves all the lower layer and different types of devices such as routers, switches etc.

7.1.1 Position of 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-629)**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.
- In this chapter we are going to discuss some common client - server applications that are used in the Internet.
- Some of the important applications discussed in this chapter are : DNS, FTP, TFTP, HTTP, SMTP, MIME and SNMP.

Scanned by CamScanner

7.2 Providing Services :

- All the communication networks which were designed to be used in the era prior to the Internet era were designed to provide a specific type of service.
- An example of such a service is the telephone service. The network for telephony was originally designed to provide only the voice service.
- Later on the same network was used to provide some other services such as the FAX.
- In a similar manner, the Internet also was designed for providing service to the users all over the world.
- But the Internet is more flexible than the other services such as postal service or telephone service, due to the layered architecture of TCP/IP suite.
- Application layer being the topmost layer in the TCP/IP suite, is slightly different from the other layers.
- The application layer protocols only take services from the other layer protocols but they do not provide any service to the protocols belonging to the other layers in TCP/IP suite.
- Therefore it is easily possible to add or remove protocols to/from the application layer. This layer is the only layer which can provide services to the Internet users.
- Due to the flexibility of the application layer, it is possible for us to add new application protocols to the Internet.

7.2.1 Standard and Non-standard Protocols :

- The protocols belonging to the first four layers of the TCP/IP suite have to be standardized and documented in order to ensure proper operation of the Internet.
- These protocols are generally included in the package along with an operating system such as windows or UNIX.
- However the application programs can be either standard or nonstandard, for ensuring flexibility.

7.2.2 Standard Protocols (Application Layer) :

- In our day to day life, we use several application layer programs for our interaction with the Internet. These programs are standardized and well documented by the Internet authorities.
- Each standard protocol is in the form of a pair of computer programs. These programs have been designed to interact with the user and the transport layer so as to provide a specific service to the user.

7.2.3 Nonstandard Protocols (Application Layer) :

- By writing two programs which can interact with a user and the transport layer to provide a specific service to the user, any programmer can create a nonstandard application layer program.
- The creation of a nonstandard protocol does not need any approval of the Internet authorities if it is used privately.
- The Internet has become so popular because of these nonstandard application layer protocols.

7.3 Application Layer Paradigms :

During the life time of the Internet, two different paradigms have been developed. They are as follows :

1. Client-server paradigm.
2. Peer to peer paradigm.

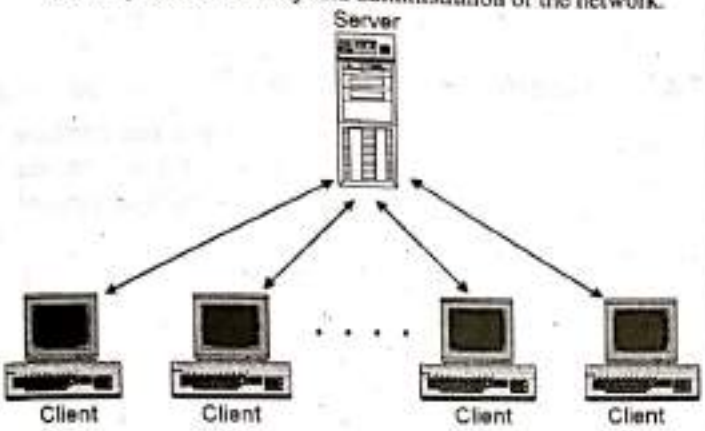
7.3.1 Traditional Paradigm : Client Server :

- The **client-server paradigm** is a traditional application layer paradigm which was the most popular paradigm until a few years ago.
- **Server process :** An application program called as the server process is basically the service provider in this paradigm.
- The server process runs continuously and waits for an other application program called as the **client process** to make a connection through the Internet to ask for a service.
- Some server processes have been designed to provide some specific type of services. The server processes are supposed to run continuously but the client process does not run continuously.
- In fact it is started when the client needs some service from a server process.
- A server process can provide the same specific service to a number of client processes which request for that service.
- 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

Scanned by CamScanner

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. 7.3.1 shows client-server network relationship. The server provides security and administration of the network.



(G-41) **Fig. 7.3.1 : 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.
- In short we can define a **client** as a program running on the local machine which requests some services from the server.
- It is said that the client program is a **finite** program. We have discussed it later on in this chapter.

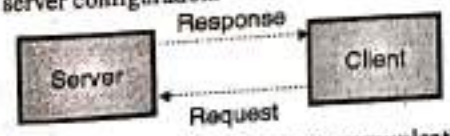
Server :

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.
- Generally we can define as **server** as a program which is running on the remote server computer to provide service to all the clients. It only initiates a service when requested by that client computer.
- The server program is called as an **infinite** program. We have discussed the reason for it later on in this chapter.

Communication in client-server configuration :

- Fig. 7.3.2 explains the principle of communication in the client server configuration.



(G-42) **Fig. 7.3.2 : Client/server communication**

- The client places a request on the server machine when he wants an access to the centralised resources.
- The server responds to this request and sends the signal accordingly to the client as shown in Fig. 7.3.2.
- 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.
- A server program when started, will run infinitely unless it faces some problem. Therefore it is called as an **infinite** program.
- A server program waits for incoming requests from clients. On receiving a request, it will respond to the request in one of the following way :
  1. Iteratively 2. Concurrently
- A client program will be started by the user and gets automatically terminated when the service is complete. Therefore it is called as the **finite** program.
- Generally the communication with the server is initiated by the client by using the IP address of the remote machine and the well known port address of the specific server program which running on that machine.
- The request respond process in client - server communication can get repeated multiple times. But still this process will eventually come to an end.
- Therefore it is called as the finite process.

Problems :

- As one server is providing service to the multiple clients, the server has to shoulder the majority of communication load. Therefore the server should be a very powerful computer. Sometimes if too many clients are using the service at a time the even a powerful server can be overwhelmed or get crashed.
- Another problem with client server paradigm is that a service provider should be ready to bear the cost of creating a powerful server to provide a specific service. In order to encourage such an arrangement, the server (service provider) should be able to get some kind of an income to provide the specified service.

Applications :

- The following traditional services are still using the client server paradigm for their operation :
  1. WWW : World wide web
  2. HTTP : Hyper Text Transfer Protocol
  3. FTP : File Transfer Protocol
  4. E-mail
- Some of these protocols have been discussed in this chapter.

Scanned by CamScanner

7.3.2 New Paradigm : Peer-to-Peer (P2P) :

- In response to the needs of some new applications on the Internet, a new paradigm called as peer to peer paradigm has emerged in recent days.
- It is also known as the **P2P** paradigm. Here the continuously running server process is not needed. Instead the responsibility of the server process is shared by the **peers.**
- Most of the Internet applications available today operate on the client-server paradigm. But gradually the **peer-to-peer (P2P) paradigm** also has gained some importance.
- The principle of P2P paradigm is that two peers (laptops, desktops or mainframes) can exchange services by communicating directly with each other.
- If the file requested by a client to server is a large file such as a music or video file, then it puts a lot of load on the server machine.
- In such situations the **P2P** paradigm becomes attractive. The P2P paradigm is also attractive in a situation in which two peers want to exchange files without involving the server.
- However it should be noted that the **P2P** paradigm does not ignore the client-server paradigm completely. Instead the P2P allows some users to share the duty of the server.
- Instead of sharing of a big file using client-server connection, the P2P paradigm will let the server download a part of that file and then share it among themselves.
- Thus in P2P paradigm the same computer has to sometimes behave like a client and at some other time like a server.
- In other words, the same computer will be a client for some applications for certain amount of time and server at other times. However such applications are not a part of the Internet, but they are controlled commercially.
- In P2P paradigm any computer connected to the Internet can provide service as well as request for a service. That means it can work as a **server** at one time and as a **client** at some other time.
- One of the best examples of Internet application in which the P2P paradigm is used is **Internet.**

Telephony :

Another situation in which the P2P paradigm can be more useful is when one Internet users wants to share something (a file for example) with another Internet user.

Advantages :

The main advantages of P2P paradigm are as follows :

1. It is easily scalable.
2. It is cost effective because an expensive server need not be used.

Disadvantages :

Alongwith the above stated advantages, there are some drawbacks of P2P paradigm.

1. Providing a secured communication is difficult.
2. This paradigm cannot be used by all the Internet applications.

Applications :

The following Internet applications use the P2P paradigm.

1. Skype
2. Internet telephony
3. IPTV.

7.3.3 Mixed Paradigm :

In order to get the benefits of both the paradigms, some applications may try to use the mixture of the two paradigms.

7.4 Client Server Paradigm :

- A client and a server are two running application programs called processes, and in the client server paradigm, the communication takes place at the application layer between these processes.
- A client sends a request to initialize the communication with server which is waiting for the request.
- In response to such request the server prepares a result and sends the results back to the client. In order to achieve this, the server should be running continuously but the client process does not have to run continuously.
- Therefore if we have two computers connected somehow to each other then we can run the client programs on one of them and the server program on the other.
- The server program should start running before the client program and it should run continuously. In other words, a **server** has an **infinite lifetime.**
- On the other hand a client has a **finite lifetime.**

7.4.1 Application Programming Interface (API) :

- We need to now understand that how a client process communicates with a server process.
- A client process is basically a computer program which like any other program, written in a computer language but with certain additional instructions.
- These new or additional set of instructions makes the client process capable of communicating with the other process.,
- These new instructions tell the lowest four layers of the TCP/IP suite to perform the following functions :
  1. Open a connection
  2. Send and receive data to / from the other end
  3. Close the connection.
- A set of instructions of this type are collectively called as **Application Programming Interface (API).**
- We can define an **interface** as the set of instructions required to facilitate communication between any two entities.
- In this case one entity is the application layer process (client or server) and the other entity is the operating system.
- Therefore an API should be included while building the first four layer of an operating system, by the computer manufacturer.
- This will enable all the application layer processes to communicate with the operating system to send and receive their messages.

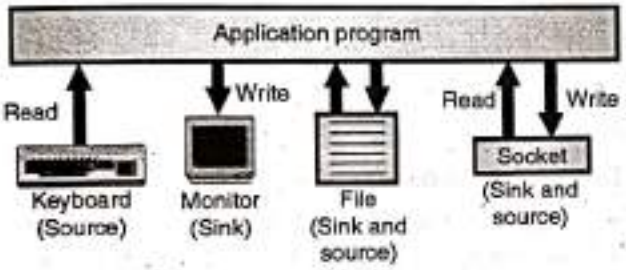
Scanned by CamScanner

7.4.2 Types of APIs :

- Eventhough many APIs have been designed for communication, the following three are the most commonly used APIs.
  1. Socket interface
  2. Transport Layer Interface (TLI)
  3. STREAM
- Out of these the socket interface is the most common one which we will be discussing in this section.

Why Sockets ?

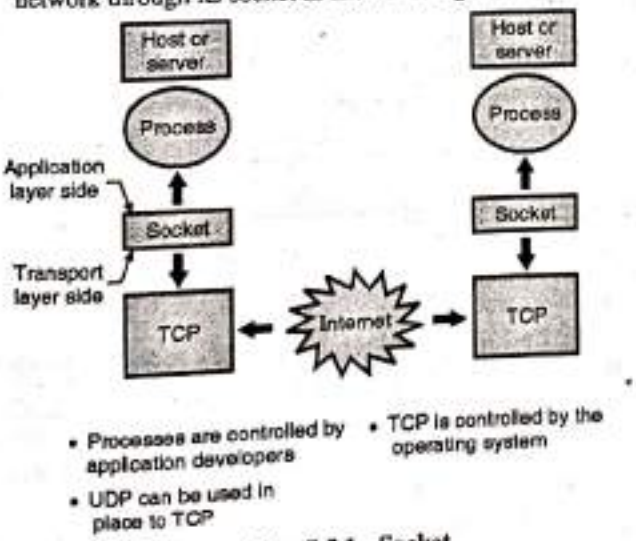
- With the **socket interface**, it is possible to use all the instructions that can read and write data in the programming languages like C, C+ and Java.
- All these preexisting instructions can be used to read and write data from the **sockets**.
- Thus **socket** is new source or sink of data which is being added to the programming language. It is very similar to the other sources and sinks such as a file, a keyboard or a monitor as shown in Fig. 7.4.1.



(G-2209)**Fig. 7.4.1 : Sockets are like any other sinks and sources**

7.5 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. 7.5.1.



(G-638) **Fig. 7.5.1 : Socket**

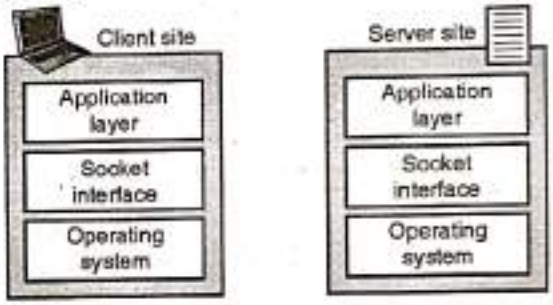
- Thus **socket** is defined as an interface between the application layer and the transport layer within a host.
- It is also called as the Application Programming Interface (API) between the application and the network.
- In Fig. 7.5.1 we have assumed that the transport protocol being used is TCP. But note that UDP can also be used.
- In the Internet, a socket is a software **data structure.**

7.5.1 Socket Interface :

- We can understand the socket interface better if we learn more about the relationship between the operating system (Unix, Windows etc.) and the TCP/IP protocol suite.
- Refer Fig. 7.5.2 to understand the conceptual relationship between an operating system and TCP/IP suite.

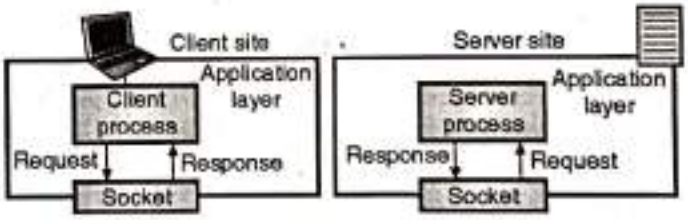
Definition :

- We may define the **socket interface** as the set of instructions which helps an application access the services provided by the TCP/IP protocol suite. It is located between the application program and operating system.
- A socket is suppose to behave like a file or a terminal but it does not have a physical existence like them. It is basically a **data structure** which is created and used by the application layer program.



(G-2210)**Fig. 7.5.2 : Relation between application layer, socket interface and operating system**

- Hence the communication between a client and a server actually takes place between the sockets created on either sides via a logical connection at the application layer level as shown in Fig. 7.5.3.



(G-2211) **Fig. 7.5.3 : Client server communication via socket interface**

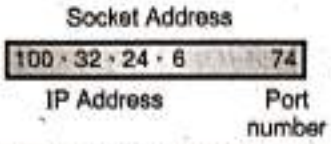
- In this way for a successful client server communication, we need to create sockets at either ends and define the source and destination socket addresses correctly.

7.5.2 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.

Scanned by CamScanner

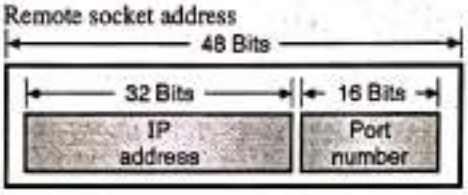
- The combination of IP address and port number is as shown in Fig. 7.5.4 and it is known as the socket address.
- The client socket address defines the client process uniquely whereas the server socket address defines the server process uniquely.



(G-1548) **Fig. 7.5.4 : 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.
- The socket address is thus 48 bit long because it consists of a 32-bit IP address and a 16-bit port number.
- A socket defines the end points of the client-server communication. Therefore it is identified by the following two socket addresses :

1. Local socket address
2. Remote socket address



(G-2212)**Fig. 7.5.5 : Structure of socket address**

7.5.3 Finding Socket Addresses :

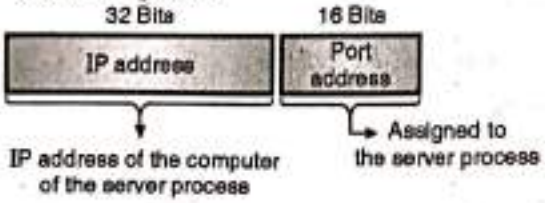
- Let us discuss now about how a client or a server find the two socket addresses mentioned above.
- The situation at the client site is completely different than that at the server site.
- Therefore we will consider them separately.

7.5.3.1 At The Server Site :

- It is easy to understand that the server is identified with a local (server) and a remote (client) socket address.
- Let us see how to find them.

1. Local (Server) Socket Address :

- The operating system at the server provides the local (server) address. This local address consists of the IP address of the computer on which the server process is running (which the O.S. knows) and the port number of the server process (which is to be assigned). This is shown in Fig. 7.5.6.



(G-2213)**Fig. 7.5.6 : Local (server) address of a socket at the server**

- For a standard server process, the port number is already assigned by the Internet authorities.
- For a nonstandard server, its designer can choose a port number, and assign it to the server process.
- The server knows its local socket address as soon as the server process starts running.

2. Remote Socket Address :

- The remote socket address of a server is actually the socket address of the client which wants to communicate.
- A server knows this address only when a client tries to connect to it. The socket address of the connecting client is present in the request packet sent by it to the server which automatically becomes the remote socket address of the server.
- The server then communicates on this socket address with that client.

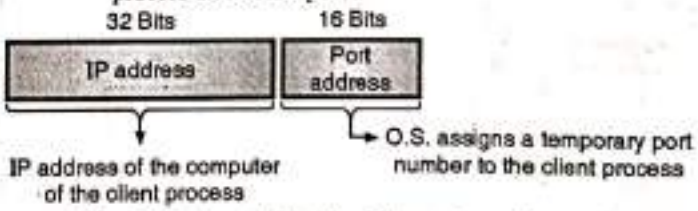
> **Note :**
> The local socket address of the server is fixed for its lifetime, but the remote socket address changes in each interaction with a different client.

7.5.3.2 At the Client Site :

A client also needs a pair of socket addresses, namely local (client) address and remote (server) address.

1. Local Socket Address :

- The local (client) socket address consists of the IP address of the computer on which the client process is running and a 16-bit port number as shown in Fig. 7.5.7.
- Therefore the operating system itself provides the local (client) socket address. It knows the IP address and assigns a temporary 16 bit port number to the client process each time when it wants to initiate a communication.
- However this temporary port number should be chosen from a list of port numbers provided by the Internet authority and the O.S. should ensure that the same port number has not been assigned to any running client process on the computer.



(G-2214)**Fig. 7.5.7 : Local (client) address of a socket at the client**

2. Remote (server) Socket Address :

- The remote (server) socket address of a client process is actually the socket address of the server it wants to communicate with.
- A client process must know this address when it wants to send the request message to the server, it wants to connect with.
- We will consider two different situations for this.

Scanned by CamScanner

Situation 1 :

- If we ourselves have written both the client and server programs then we will know both IP address of the server computer and port number of the server process.
- In this situation the remote (server) socket address can be obtained very easily.

Situation 2 :

- In this situation, the well known port numbers for some standard applications are known but generally the IP number server computer is not known.
- Hence the unknown IP address of the server computer should be obtained by using another client server application called **Domain Name System (DNS).**
- A DNS system is equivalent to a directory on the Internet, which maps the server name to the IP address of the server computer.

7.6 Using the Services of The Transport Layer :

- As discussed earlier a pair of processes (client and server) provide services to the Internet users. However, to provide this service the client and server need to take services from their respective **transport layers** to facilitate the **physical communication** which is absent at the application layer.
- The three most common transport layer protocols are : UDP, TCP and SCTP. So we can take the services of one of these protocols.
- We will discuss the use of these protocols one by one.

7.6.1 Users Datagram Protocol (UDP) :

- The important features of UDP protocol service are as follows :
  1. It provides a connectionless service
  2. Its service is unreliable
  3. It is a datagram service
- This means that there is no logical connection between the two ends of communication. Each message is an independent entity which is encapsulated in a packet called **datagram.**
- Each datagram can follow its own path of travel from the source to destination and may arrive at the destination in an out of order manner.
- UDP service does not provide any **error control** or **flow control.**
- It can at the meet check the received data for presence of errors. If errors are found UDP simply discords those datagrams but does not request sender to resend them. Therefore the UDP service is called as an **unreliable service.**
- Still the UDP service is suitable for the application programs which send small messages and for those applications for which the simplicity and speed are more important than reliability.
- The examples of application programs which use the UDP protocol services are some management and multimedia applications.

7.6.2 TCP Protocol :

- The important features of TCP protocol service are as follows :
  1. It provides a connection oriented service.
  2. Its service is a reliable one.
  3. It is a byte stream service.
- The two ends have to create a logical connection between for the exchange of data.
- The TCP packets travel the route from source to destination only over this logical connection. Therefore all the packets arrive at the destination in the proper order.
- TCP provides the **flow control congestion control,** and **error control**. The packets containing errors are discarded and a request of retransmission of the lost of corrupted packets is made to the sender. That is why the TCP service is a **reliable service.**
- One problem with the TCP is that it is not a message oriented protocol like UDP. So it does not put any boundaries on the messages being exchanged.
- The TCP services are used by those applications which need to send long messages and for which reliability is more important than simplicity and speed.

7.6.3 SCTP Protocol :

- The features of service provided by SCTP protocol is a combination of the features of UDP and TCP services.
- The important features of SCTP protocol service are as follows :
  1. It provides a connection oriented reliable service.
  2. It is a message oriented service.
  3. It can provide a multistream service which neither UDP not TCP can provide.
- SCTP protocol service is preferred by these applications that need reliability as well as a continuity in connection via an alternate connection even if one connection fails.

7.7 Standard Client Server Applications :

- Several client server application programs have been developed during the lifetime of the Internet.
- We will study some of these applications so that we can create new applications in future.
- In the following sections, six standard applications have been discussed.
- Initially the world wide web (WWW) and HTTP which are used by almost all the Internet user, have been discussed.
- Next the remote login and how to achieve it using the TELNET and SSH protocol is explained

Scanned by CamScanner

- And finally the DNS protocol which is used by all the applications to map the server name to its IP address has been described.
- In between we have also included the two high load applications on the Internet i.e. file transfer protocol (FTP) and Electronic mail.

7.8 Domain Name System (DNS) :

MU : Dec. 14, May 15, Dec. 17

University Questions

Q. 1 Explain the need for DNS and describe the protocol functioning. **(Dec. 14, May 15, 10 Marks)**

Q. 2 Write a short notes on : DNS **(Dec. 2017, 5 Marks)**

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.

7.8.1 How does DNS Work ?

- 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.

7.8.2 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 :
  1. Flat name space.
  2. Hierarchical name space.

7.8.3 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.

7.8.4 Hierarchical Name Space :

- 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.

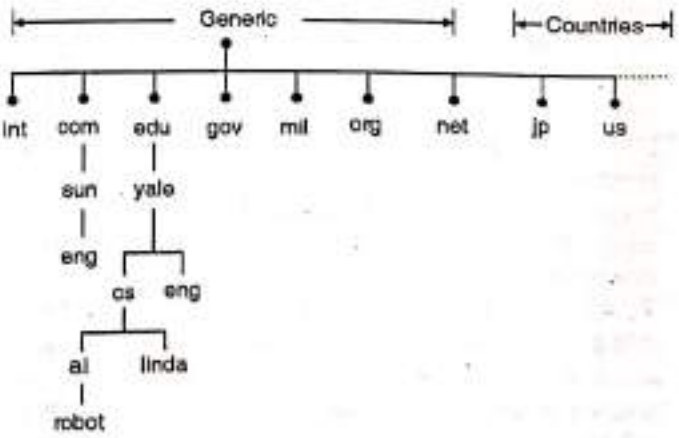
7.9 Domain Name Space :

MU : Dec. 14, May 15

University Questions

Q. 1 Explain the need for DNS and describe the protocol functioning. **(Dec. 14, May 15, 10 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. 7.9.1.



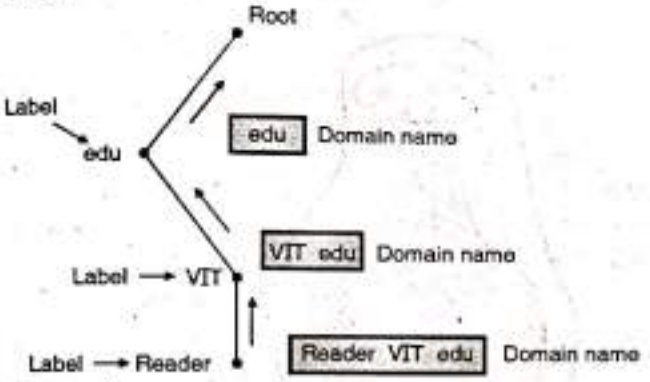
(G-631) **Fig. 7.9.1 : A portion of Internet domain name space**

Scanned by CamScanner

- The top level domains are of two types namely generic and countries.

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. 7.9.2. The upward followed path has been shown by an arrow.



(G-632)**Fig. 7.9.2 : 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 ?

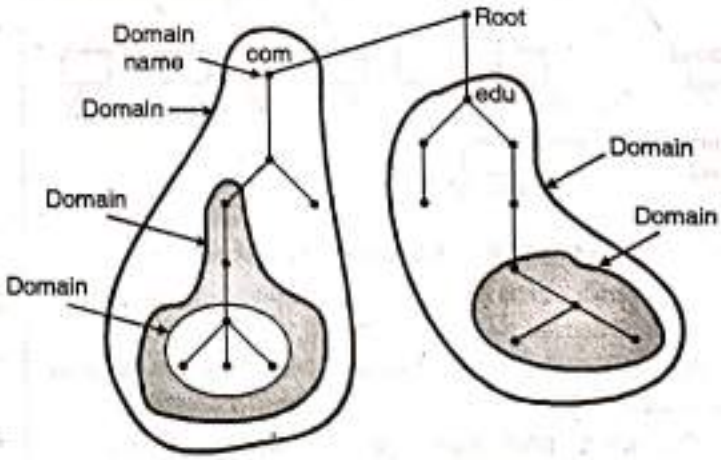
No they are not case sensitive. So com and COM means the same thing.

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. 7.9.3. The name of the domain is the domain name of the node at the top of the subtree as shown in Fig. 7.9.3. e.g. com or edu.
- A domain can be divided into subdomains as shown in Fig. 7.9.3.
- 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.



(G-633)**Fig. 7.9.3 : Domains**

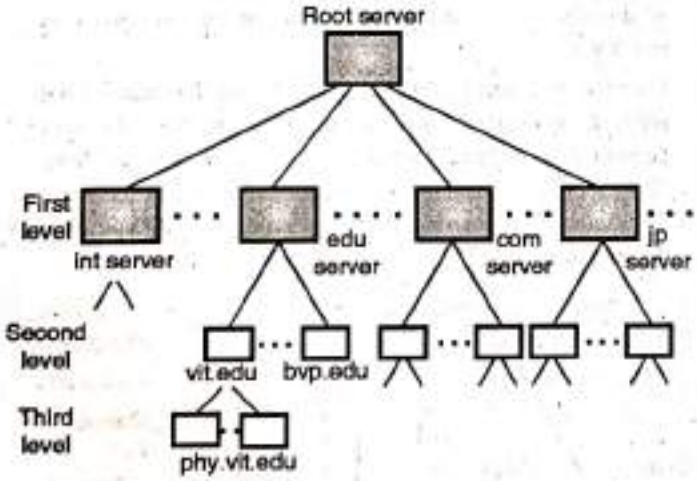
Scanned by CamScanner

7.10 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.

7.10.1 Hierarchy of Name Servers :

- 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.**
- Then we have to use a hierarchy of the Name servers as shown in Fig. 7.10.1.
- 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. 7.10.1.

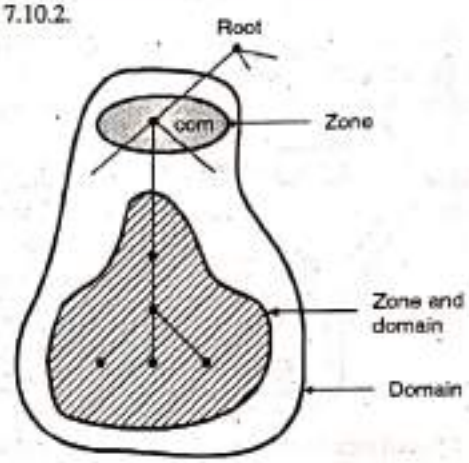


(G-634)**Fig. 7.10.1 : Hierarchy of name servers**

- 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. 7.10.2.
- 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. 7.10.2.



(G-635)**Fig. 7.10.2 : 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 :

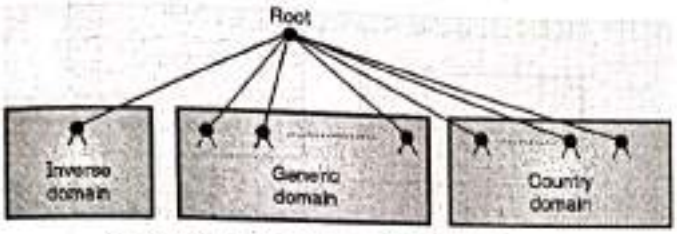
- This server transfers complete information about a zone from another server which may be primary or secondary server. The transferred information is saved on the disc storage of the secondary server.

Scanned by CamScanner

- 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.

7.11 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. 7.11.1.
  1. Generic domain 2. Country domain
  3. Inverse domain.



(G-636)Fig. 7.11.1 : Use of DNS in Internet

7.11.1 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 lables. Some of them are given in Table 7.11.1.

Table 7.11.1 : Generic domain lables

Lable	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.

7.11.2 Country Domain :

- This domain section uses two character country abbreviations eg. US for united states.
- Second lable in this domain can specify organization or national designations.

7.11.3 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.

7.12 Name Address Resolution :

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 :

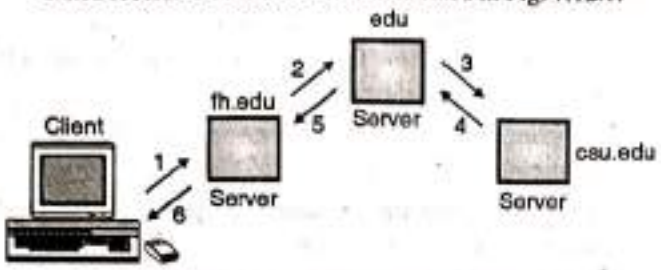
  118.48.36.142.in_addr.arpa.
- This is received by the local DNS and resolved.

7.12.1 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.

Scanned by CamScanner

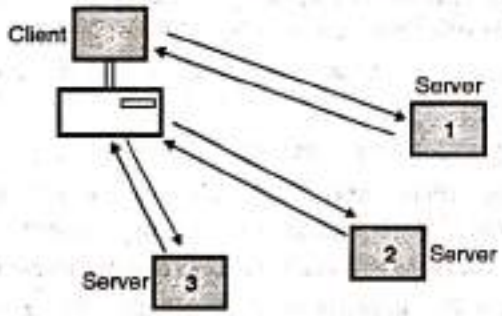
- Such a query is called as recursive query and the process is called recursive resolution. It is illustrated in Fig. 7.12.1.



(G-637)Fig. 7.12.1 : Recursive resolution

7.12.2 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.
- 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. 7.12.2 illustrates the iterative resolution.



(G-638)Fig. 7.12.2 : 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 :

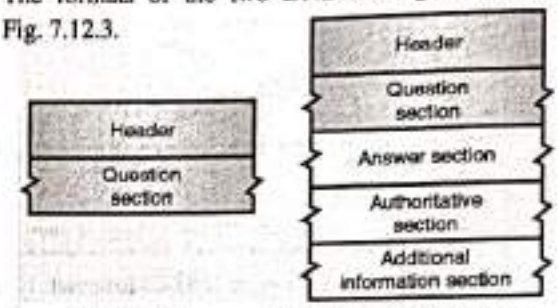
- www.yahoo.com - the world's best-known name
- www.mit.edu - a popular EDU name
- encarta.msn.com - a Web server that does not start with www
- www.bbc.co.uk - a name using four parts rather than three
- ftp.microsoft.com - an FTP server rather than a Web server
- www.spce.ac.in - Server in India 'in' 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.

7.12.3 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. 7.12.3.



(a) Query (b) Response or reply

(G-639)Fig. 7.12.3

- 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. 7.12.3.

7.12.4 Caching :

- 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.

7.13 DNS Records :

- There are two types of records used in DNS as follows :

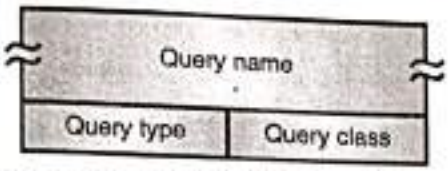
  1. Question records and 2. Resource records

- The question records are used in the query and response messages whereas the resource records are used in the response messages.

Scanned by CamScanner

7.13.1 Question Records :

- The client uses the question record to get the required information from the server. The format of question record has been shown in Fig. 7.13.1.
- Various fields in the question record format are query types and query class.



(G-1791) **Fig. 7.13.1 : Question record format**

Query name :

This field has a variable length and it contains a domain name. The count field tells us how many characters are present in each section.

Query type :

- This field is 16-bit long and it defines the type of query.
- Some of the commonly used query types are A, NS, CNAME, SOA, ANY etc.

Query class :

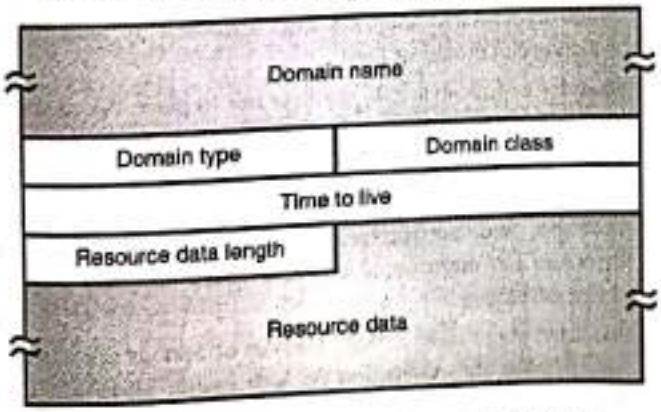
- This field also is 16-bit long. It defines the specific protocol using DNS. Table 7.13.1 has listed some of possible classes. However the most important class would be IN i.e. internet (class 1).

Table 7.13.1 : Query classes

Class	Mnemonic	Explanation
1.	IN	Internet
2.	CSNET	CSNET network (Not used now)
3.	CS	COAS network
4.	HS	The Hesiod server (MIT)

7.13.2 Resource Record :

- Each domain name i.e each node on the tree in DNS is associated with the resource record which is a part of the server database.
- Resource records are returned by the server to the client. The format of RR has been shown in Fig. 7.13.2.



(G-1792) **Fig. 7.13.2 : Format of resource record**

1. **Domain name :**

   This field contains the domain name and its length is not fixed. It has a variable length. The domain name in the question record is duplicated here.

2. **Domain type :**

   This field and the query type field in the question record are the same except the last two types i.e. AXFR and ANY are not allowed.

3. **Domain class :**

   This field is same as the query type field in the question record.

4. **Time to - live :**

   This field is 32 bit long and it defines the time for which the answer is valid (in seconds). If the contents of this field is zero, then it indicates that the resource record is used only in a single transaction.

5. **Resource data length :**

   This field is 16 bit long. It is used for defining the length of the resource data.

6. **Resource data :**

- As shown in Fig. 7.13.2 the resource data field is a variable length field. It contains the answer to the query or domain name or the additional information.
- The format and contents of this field depend on the value of the type field. It can be one of the following :

  1. A number
  2. A domain name
  3. An offset pointer
  4. A character string.

7.13.3 Encapsulation :

- DNS can use either TCP or UDP. It may choose any one of these protocol but in either case the server uses port 53.
- The UPD is preferred if the length of response message is upto 512 bytes whereas TCP is used if the message length is larger than 512 bytes.

7.13.4 Registrars :

- New domains are added to DNS through a registrar, which is a commercial entity.
- Whenever an organization applies for DNS domain name, a registrar first checks that the requested domain name is unique.
- The applying organization has to give the name of its server and IP address of the server to the registrar.

7.14 DDNS :

- When DNS was designed no one imagined that there will be so many address changes.
- In the conventional DNS if a change is to take place (such as adding or removing a host or change in IP address etc.) then all such changes should take place in the DNS master file.

Scanned by CamScanner

This would need a lot of updating manually. Due to the size of Internet manual updating is practically not possible.

- The remedy is that the DNS master file should get updated dynamically. In order to address this need the Dynamic Domain Name System (DDNS) was developed.
- The operation of DDNS takes place as follows :
  1. The binding between a Name and an Address is determined.
  2. The information is sent using DHCP to the primary DNS server.
  3. Primary DNS server notifies the secondary DNS servers either actively or passively about the change in zone.
  4. DDNS can use authentication mechanism so as to avoid any unauthorised changes in DNS records.

7.14.1 Security of DNS :

- DNS is very important in the internet infrastructure. It can get attacked by intruders in several ways as discussed below :
  1. An intruder can access the DNS server's response which enables him to know user's favourite sites, or user's profile. This should be avoided by making the DNS message confidential.
  2. The attacker can create a bogus server response of a DNS server. This will divert the user to those sites the attacker wants him to visit. The message origin authentication and message integrity are the remedies which will prevent this type of attacks.
  3. The attacker may flood the DNS server to crash it. This can be prevented by using the provision against denial - of - service attack.
- The DNS is made more secure by using a technology called DNS security (DNSSEC).
- DNSSEC does the following using digital signature :
  1. Message origin authentication
  2. Message integrity
- But DNSSEC does not do the following :
  1. Does not provide DNS message confidentiality
  2. No protection against denial - of - service attack.

7.15 World Wide Web (WWW) :

- 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.

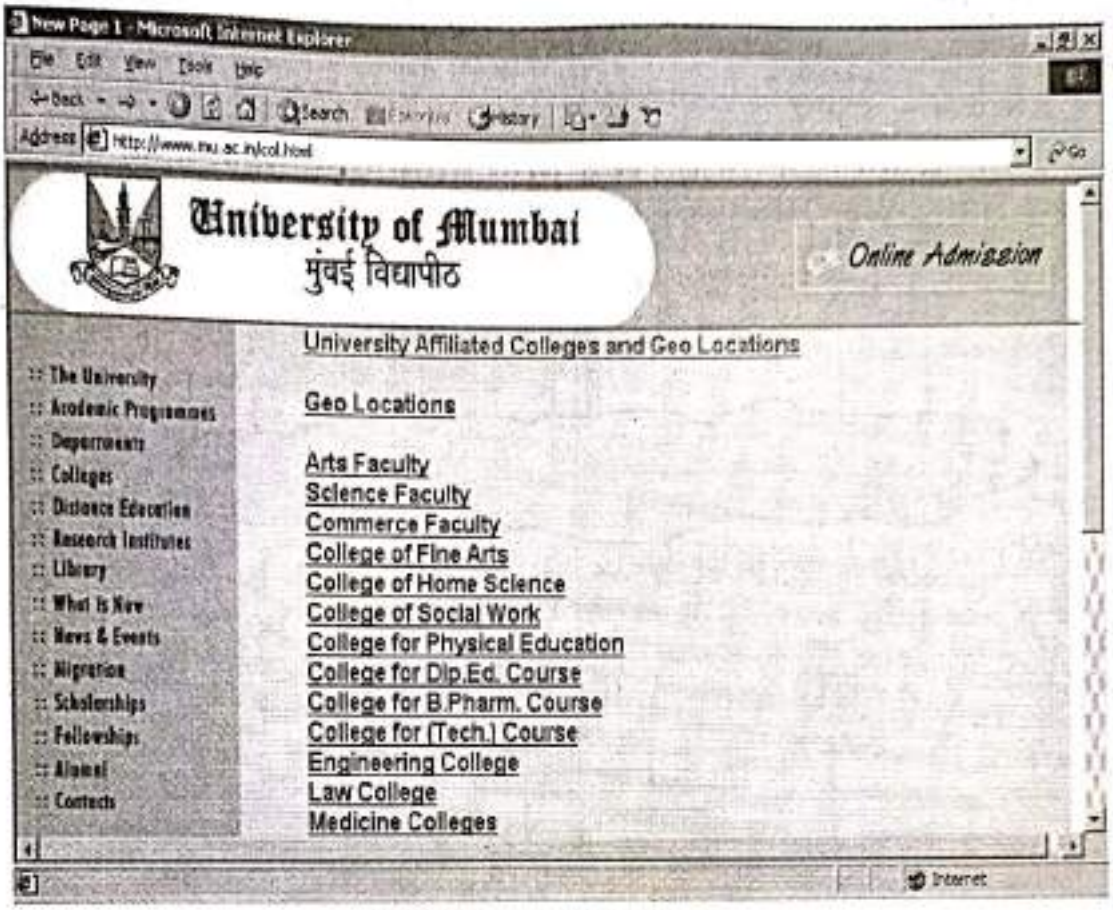
Difference between Web and Internet :

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.
- 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.

Scanned by CamScanner



(G-653) **Fig. 7.15.1 : A Web 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 :

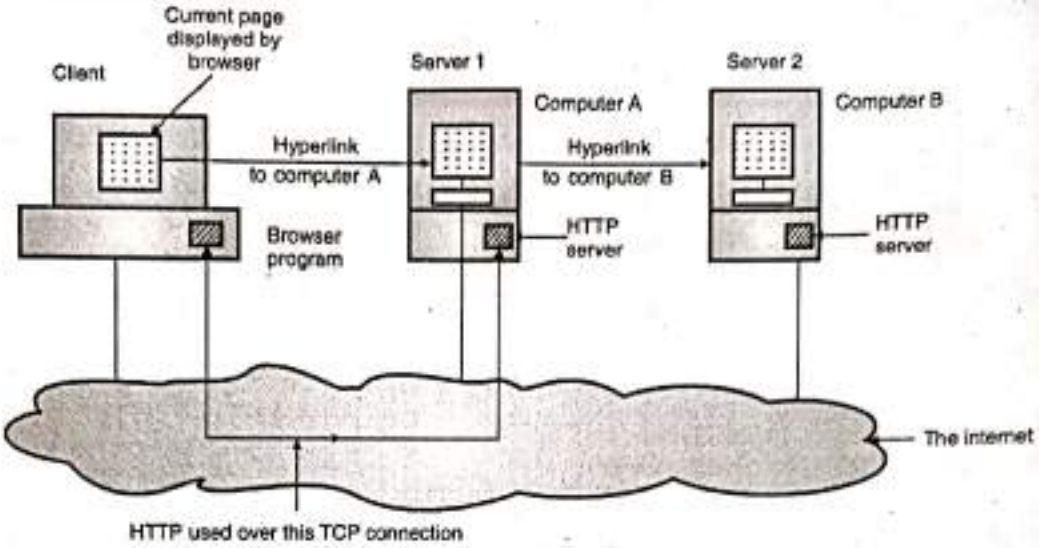
- All pages may not be viewable in the conventional way because some pages may contain audio tracks, video clips or both.
- If the hypertext pages are mixed with other media, the result of such a mixing is called as hypermedia.
- Some browsers are capable of displaying all kinds of hypermedia but others cannot do so.
- 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 :

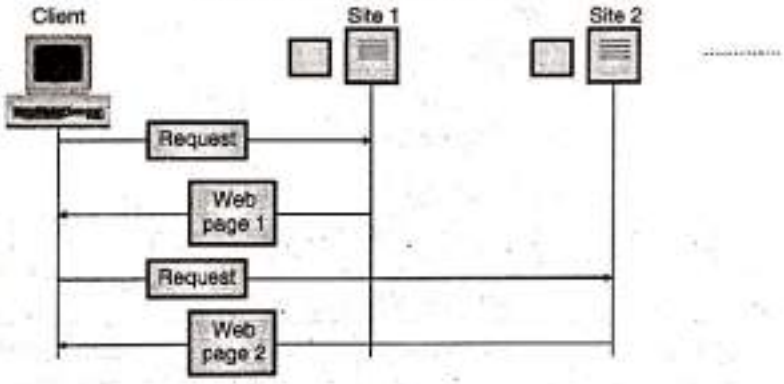
- Every website has a server process. It is listening to TCP port 80 on which incoming clients (browsers) are connected.
- Once a connection is established, the client sends a request and the server sends a reply for that. Then the connection is released.
- The protocol used for defining the legal request and replies is called HTTP.
- Fig. 7.15.2 shows various parts of the web model.

Scanned by CamScanner

7.15.3 WWW Architecture :



(G-654) **Fig. 7.15.2 : Web model**

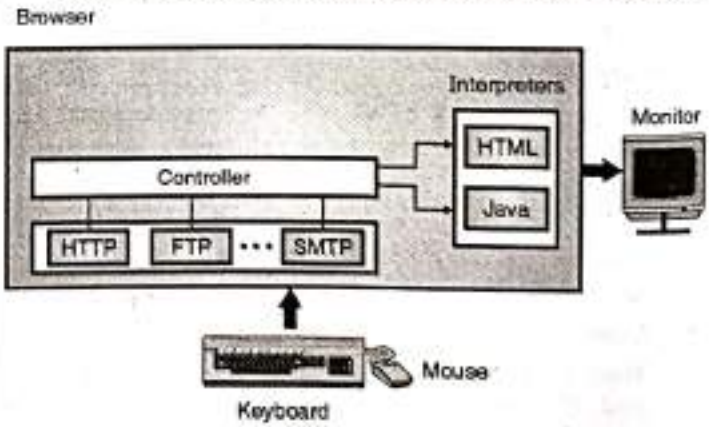


(G-655) **Fig. 7.15.3 : WWW architecture**

- 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.

7.15.4 Browser (Web 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 :
  1. A controller
  2. Client programs
  3. Interpreters.
- Fig. 7.15.4 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.



(G-665) **Fig. 7.15.4 : Browser architecture**

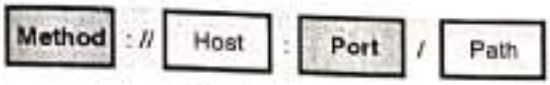
7.15.5 Server :

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.

Scanned by CamScanner

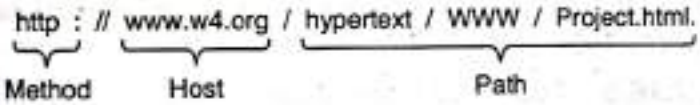
7.15.6 Uniform Resource Locator (URL) :

- 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. 7.15.5(a). They are as follows :
  1. Method or protocol
  2. Host computer
  3. Port
  4. Path.



(G-660) **Fig. 7.15.5(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. 7.15.5(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. 7.15.5(b). Note that the port is not included.



(G-1969) **Fig. 7.15.5(b) : Example of URL**

7.15.7 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 :
  1. A cookie header line in HTTP response message.
  2. A cookie header line in the HTTP request message.
  3. A cookie file kept on the user's end system and managed by user's browser.
  4. 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.

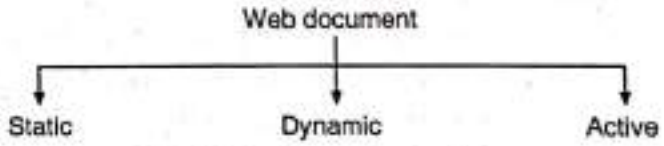
  For example the header line can be :

  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.

7.16 Web Documents :

- The web documents can be classified into three categories as shown in Fig. 7.16.1.

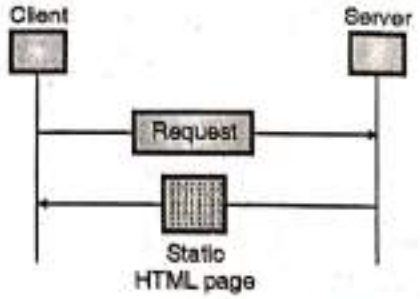


(G-668) **Fig. 7.16.1 : Categories of web documents**

7.16.1 Static Documents :

- 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. 7.16.2.

Scanned by CamScanner



(G-669) **Fig. 7.16.2 : Static document**

7.16.2 HTML (Hypertext Markup Language) :

- 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 :

  <B> – Beginning of boldface

  </B> – End of boldface.

- Here <B> and </B> 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.

7.16.3 Dynamic Document :

- 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. 7.16.3 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.

7.16.4 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.

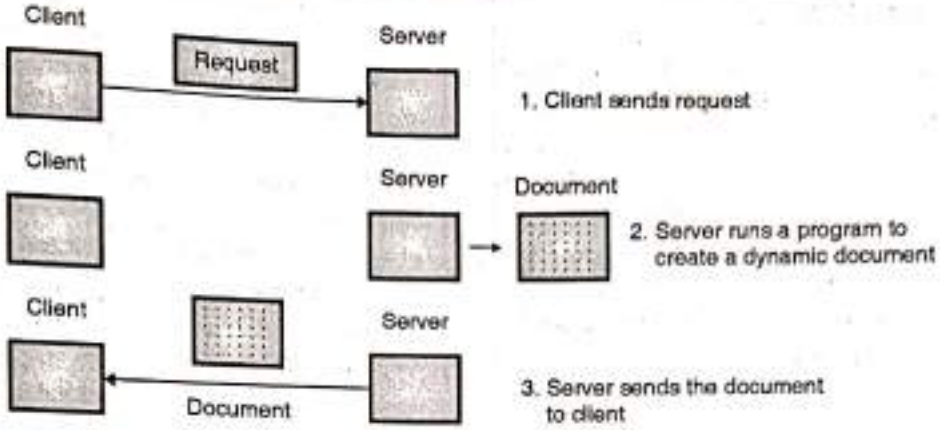
CGI Program :

It is a code which is written in one of the languages that supports CGI (such as C, C ++, etc.).

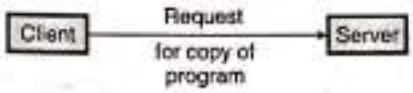
7.16.5 Active Documents :

- 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. 7.16.4 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.
- 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 clients site.
- This will save the bandwidth as well as the transmission time.

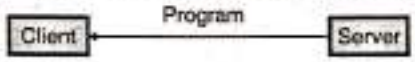
Scanned by CamScanner



(G-670) **Fig. 7.16.3 : Dynamic document**



(a) Client request for copy of program



(b) Server sends a copy of program

(c) Clients runs the program and creates the documents

(G-671) **Fig. 7.16.4 : Active document**

Steps in creation of an active document :

Refer Fig. 7.16.4 to understand the creation, compilation and execution of an active document.

1. At the server, a program is written in source code and stored in a file.
2. Then the program is compiled and binary code is creates and stored in a file at the server's site.
3. A client (browser) requests for a copy of program as shown in Fig. 7.16.4(a). This program is transported from the server to the client in the compressed form.
4. The client converts the received program from binary code into executable code using its own software.
5. The client runs the program to create the desired result which can include animation or interaction with the user.

7.17 HTTP (Hypertext Transfer Protocol) : MU : Dec. 14

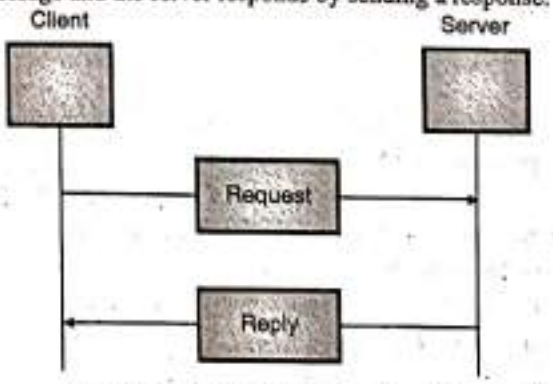
University Questions

Q.1 Give short notes on : HTTP. (Dec. 14, 5 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 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.

7.17.1 Principle of HTTP Operation :

- 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. 7.17.1 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-657) **Fig. 7.17.1 : HTTP transaction**

Scanned by CamScanner

7.17.2 The Web and HTTP :

- 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 :
  1. A client's program 2. A server's program.
- These programs are executed on different and 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 under lying 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 processes 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.**

7.17.3 Non-persistent and Persistent Connection :

- 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.

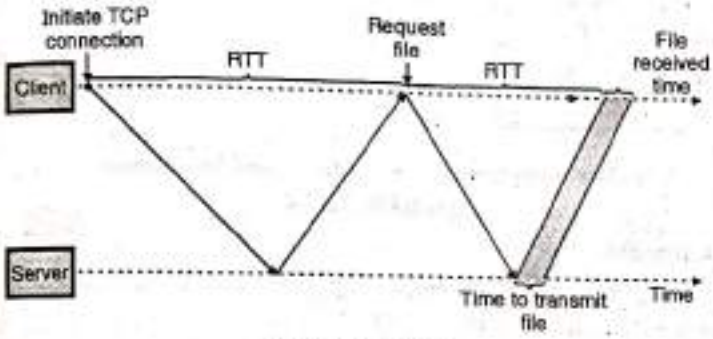
  The components of RTT are :
  1. Packet propagation delays
  2. Packet queuing delays
  3. Packet processing delays.
- Now consider the sequence of events taking place when a user clicks on a hyperlink. These events are illustrated in Fig. 7.17.2.
  1. The browser initiates a TCP connection between the 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

Scanned by CamScanner

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. 7.17.2 is equal to 2RTT plus the time taken by the server to transmit the file.



(G-658) **Fig. 7.17.2**

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.

2. 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 reciding 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.

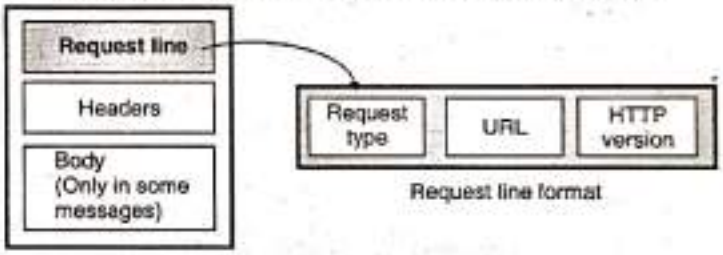
With pipelining only one RTT will be expended for all the referenced objects. Another advantage is that the pipelined TCP connection remains idle for a very short time.

7.17.4 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.

7.17.5 Request Message :

- Fig. 7.17.3(a) shows the format of the request message. It consists of a request line, headers and sometimes a body.



(G-659) **Fig. 7.17.3(a) : HTTP request message**

1. Request line :

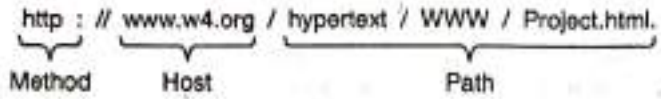
- The request line is used for defining the request type, resource (URL) and HTTP version as shown in Fig. 7.17.3(a).
- **Request type :** Several request types are defined.
- **Uniform Resource Locator (URL) :** The client accessing a web page needs an address. The HTTP uses the URL to facilitate the access of any document distributed over the world. The URL defines four thing as shown in Fig. 7.17.3(b). They are as follows :
  1. Method 2. Host computer
  3. Port 4. Path

(G-660) **Fig. 7.17.3(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.

Scanned by CamScanner

The example of URL is shown in Fig. 7.17.3(c).



(G-1969) **Fig. 7.17.3(c) : Example of URL**

7.17.6 Methods (Request Type) :

- This is one of the fields in the request line format. It defines different types of messages referred to a 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 :

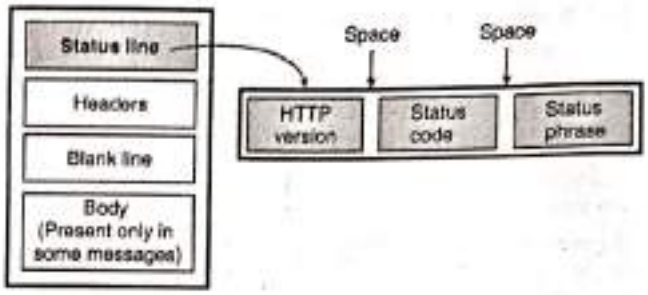
It is used for deleting the links created by the LINK method.

11. OPTION :

It is used by the client to ask the server about various options that are available.

7.17.7 Response Message :

Fig. 7.17.4(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. 7.17.4**

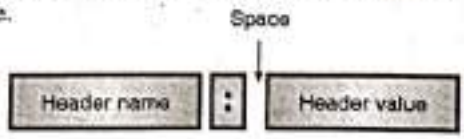
Status line :

The status line is used for defining the status of the response message. As shown in Fig. 7.17.4(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.

7.17.8 Headers :

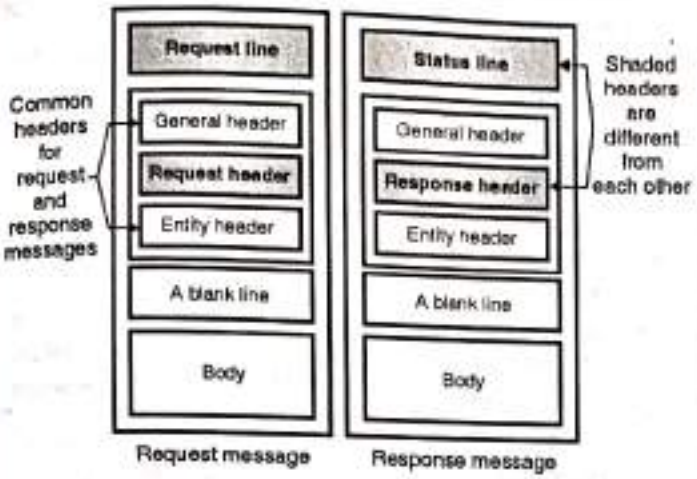
- Headers in the response message are used for exchanging additional information between the client and server.
- The header can be a one liner or multiple lines. The format of a header line is shown in Fig. 7.17.5 which shows that it consists of a header name, a colon, a space and a header value.



(G-663) **Fig. 7.17.5 : 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. 7.17.6. The common headers and different headers have been indicated clearly.

Scanned by CamScanner

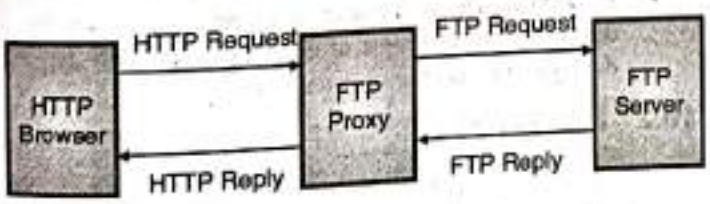


(G-664) **Fig. 7.17.6 : Comparison of request message and response message**

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. 7.17.6.
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. 7.17.6.

7.18 Proxy Server :

- 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.
- The other solution to this problem is proxy server, shown in Fig. 7.18.1.



(G-656) **Fig. 7.18.1 : Proxy server**

- 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. 7.18.1.
- 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.

7.18.1 HTTP Security :

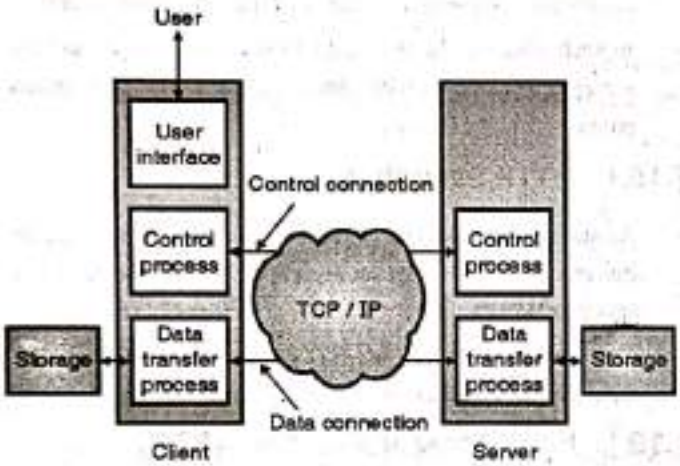
- As such HTTP does not provide any security. But it can be run over the secured socket layer (SSL). If so, the HTTP is called as HTTPS.
- The security features of HTTPS include confidentially, authentication of client and server and data integrity.

7.19 File Transfer Protocol (FTP) :

- 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. 7.19.1.
- 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.

Scanned by CamScanner

- As shown in Fig. 7.19.1 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. 7.19.1.
- 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.



(G-648)**Fig. 7.19.1 : Basic model of FTP**

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.

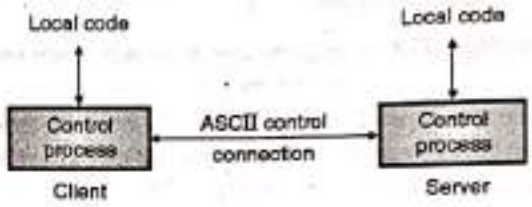
Data connection :

- 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.

7.19.1 Communication In FTP :

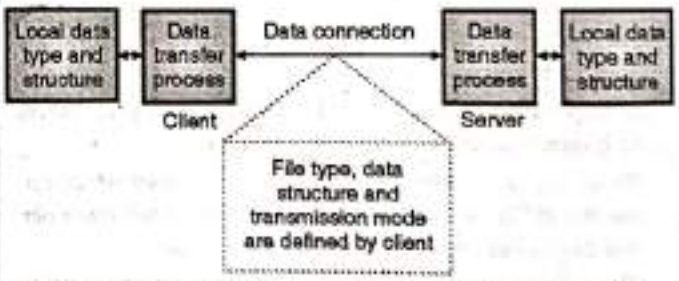
- FTP operates in client – server environment. The two computers involved in communication may be different in terms of the operating systems, character sets, file structures and file formats etc.
- FTP can make them compatible. The approaches for communication over control connection and data connection are different from each other.

1. **Communication over control connection :**
   - Refer Fig. 7.19.2 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. 7.19.2 : 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 :
     1. Type of file being transferred.
     2. Structure of data in the file
     3. Mode of transmission.
   - Before the transmission over data connection, the communication over control connection is performed.



(G-650)**Fig. 7.19.3 : Communication over the data connection**

- Refer Fig. 7.19.3 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.

7.19.2 File Types :

- FTP can use one of the following file types for transfer of data over the data connection :

  1. ASCII file 2. EBCDIC file 3. 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.

Scanned by CamScanner

- With ASCII or EBCDIC files one more attribute must be added for defining the printability of the file. This attribute is nonprint or TELNET.

7.19.3 Data Structure :

- FTP can use one of the following data structures :
  1. File structure (default) 2. Record structure and
  3. 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.

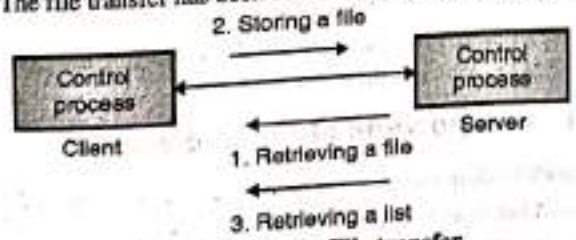
7.19.4 Transmission Mode :

FTP uses one of the following modes to transfer a file :
1. Stream mode 2. Block mode and
3. Compressed mode.

1. **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.
2. **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.
3. **Compressed mode :** For big files the data can be compressed. Generally a run length encoding is used for compression.

7.19.5 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 :
  1. **Retrieving a file :** Server copies a file onto a client.
  2. **Storing of a file :** A file can be copied from client to the server.
  3. 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. 7.19.4.



(G-651)**Fig. 7.19.4 : File transfer**

7.19.6 FTP Commands :

- The following commands are used for copying files using FTP.

Table 7.19.1 : 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 7.19.2.

Table 7.19.2 : 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 7.19.3.

Table 7.19.3 : 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.

7.19.7 Anonymous FTP :

- 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.

7.19.8 Security for FTP :

- In the early days of FTP its security was not a big issue. FTP is password protected but the password is sent in the unencrypted (plaintext) form. Therefore it is susceptible to interceptions from the attackers.
- The data which is being transferred on the data connection of FTP is also unencrypted. So the data also is not secure.
- In order to improve security of FTP, the Secure Socket Layer (SSL) may be added between the FTP application layer and the TCP layer. If done so, the improved FTP is called as SSL-FTP.

Scanned by CamScanner

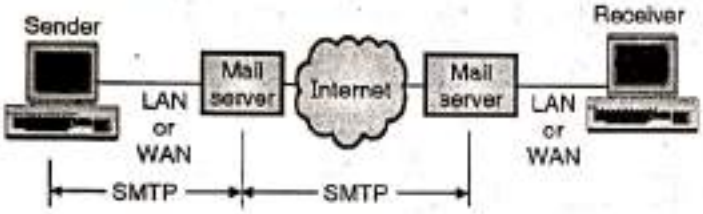
7.20 Message Transfer Agent : SMTP :

MU : Dec. 16, Dec. 17

University Questions

Q. 1 Write short notes on : SMTP. **(Dec. 16, Dec. 17, 5 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.

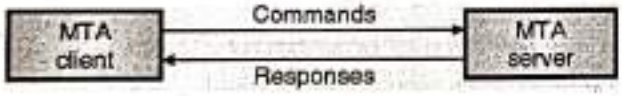


(G-641)**Fig. 7.20.1 : SMTP range**

- As shown in Fig. 7.20.1, 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.

7.20.1 Commands and Responses :

- As shown in Fig. 7.20.2, SMTP the transfer of messages between MTA client and MTA server takes place using the command and response principle.



(G-642)**Fig. 7.20.2 : Commands and responses in HTTP**

- Each command or response is terminated by a two character end of line token. The two characters used are carriage return and line feed.

7.20.2 SMTP (Simple Mail Transfer Protocol) :

New Syll. : MU : Dec. 18

- 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 decares its identity and announces its willingness/ unwillingness to receive mail. If the server is not prepared, the client will release the connection, wait for sometime 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.

7.20.3 Components of E-mail System :

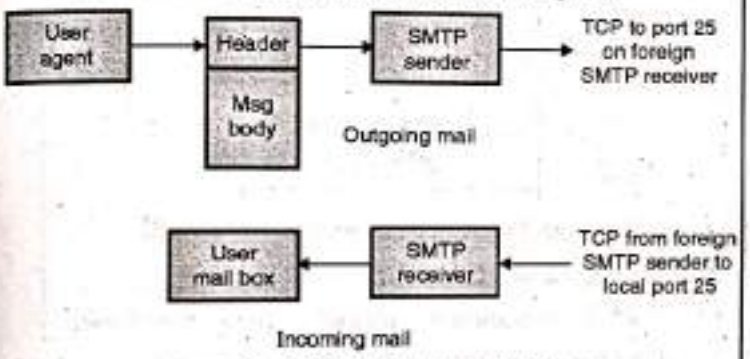
The three main components of internet mail system are :

1. User Agent (UA)
2. SMTP sender
3. SMTP receiver

They are shown in Fig. 7.20.3.

Scanned by CamScanner

- 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. 7.20.3 : SMTP mail flow**

7.20.4 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 7.20.1 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 7.20.1 : 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.

7.20.5 SMTP Operation :

The basic SMTP operation occurs in three phases :

1. Connection setup
2. Exchange of one or more command-response pairs
3. 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 :
  1. A MAIL command identifies the originator of message.
  2. One or more RCPT commands identify the recipient for this message.
  3. 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.

7.20.6 Comparison of HTTP and SMTP :

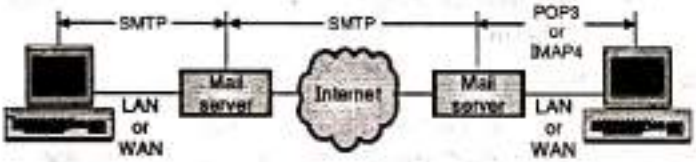
Sr. No.	SMTP	HTTP
1.	Message is transferred from client to server.	Message transfer is from client to server or the other way round.
2.	Uses TCP.	Uses TCP.
3.	Uses port 25 for transmission.	Uses port 80 for transmission.

Scanned by CamScanner

Sr. No.	SMTP	HTTP
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.

7.21 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 :
  1. Post Office Protocol, version 3 (POP 3).
  2. Internet Mail Access Protocol (IMAP 4).



(G-645) **Fig. 7.21.1 : Use of POP 3 or IMAP 4**

7.21.1 POP 3 :

- The POP3 consists of client POP3 software and server POP3 software. Out of these, the client POP3 software is installed on the receiving computer whereas the mail server gets the server POP3 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. 7.21.1.
  1. The client (user) establishes a connection with the server on TCP port 110.
  2. The client then sends its user name and password to the server in order to access the mailbox.
  3. 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. 7.21.2.

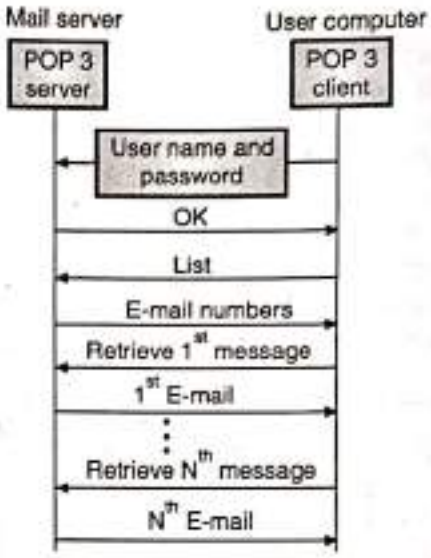
Modes of POP 3 :

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-647) **Fig. 7.21.2 : Downloading in POP3**

Disadvantages of POP3 :

1. POP3 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 down loading.

7.21.2 IMAP4 :

- Internet Mail Access Protocol Version 4 (IMAP4) is another mail access protocol which is very similar to POP3 but has more features.
- This makes IMAP4 more powerful but more complex as compared to POP3.
- IMAP is more sophisticated than POP3 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.

Scanned by CamScanner

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.

7.21.3 Comparison of IMAP and POP 3 :

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
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

7.22 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 :

- The long form of TELNET is TErminal 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 :

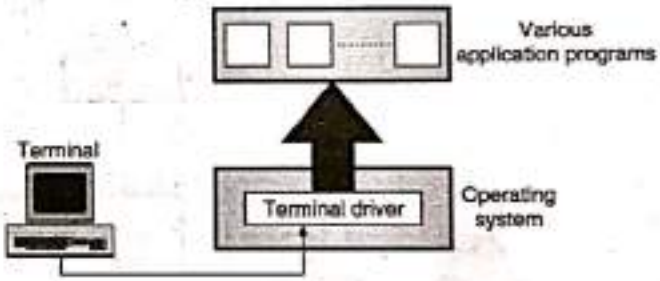
- TELNET was designed during those days when almost all the operating systems were operating on the time - sharing principle.
- In the time sharing environment there is a large central computer which supports all the users.
- All the processing is done by the central computer, and each user feels that 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.

Scanned by CamScanner

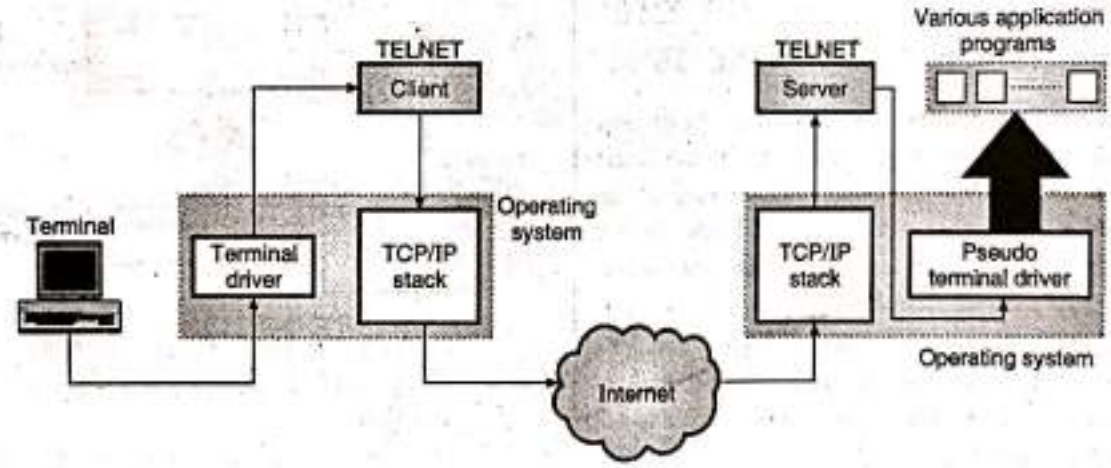
2. The terminal driver at local O.S. accepts the characters but sends them to TELNET client without interpreting them.
3. TELNET client converts them into NVT characters. NVT is Network Virtual Terminal. This is a universal character set.
4. NVT characters are delivered to TCP/IP stack (local).
5. The 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.

7.22.2 Network Virtual Terminal (NVT) :

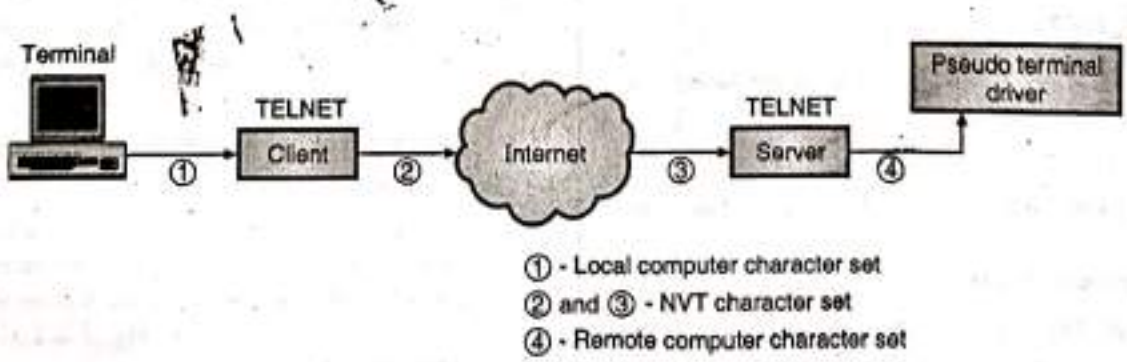
- NVT character set is a universal interface defined by TELNET in order to ensure that a user can access any remote computer in this world.
- Fig. 7.22.3 illustrates the concept of NVT.
- The local computer character set is used for the communication between the user terminal and TELNET client.
- Then 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.



(G-1794) **Fig. 7.22.2 : Principle of remote login**



(G-1795) **Fig. 7.22.3 : Concept of NVT**

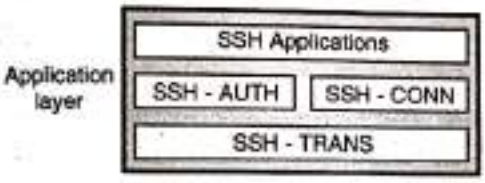
Scanned by CamScanner

7.22.4 Secure Shell (SSH) :

- Secure Shell or SSH is another popular remote login application program. The underlaying 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 SSH_1 and SSH_2, out of which SSH_2 is being used. We will discuss SSH_2 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.	3. SSH – CONN.
2. SSH – AUTH.	4. SSH – Applications.

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 :

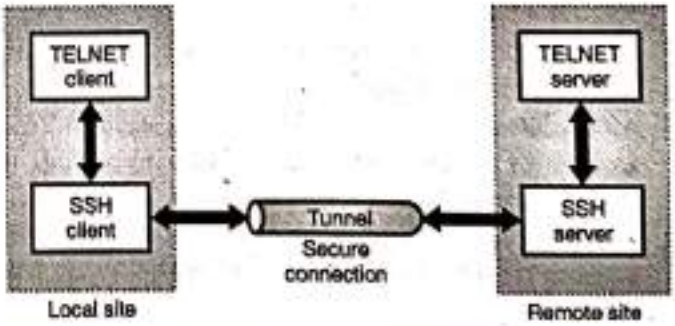
- The third component of SSH is SSH – CONN. i.e. SSH connection protocol.
- This piece of software is called for by the SSH once a secure connections has been established and authentication done.
- SSH – CONN performs the multiplexing as one of its services. It allows the client to create multiple logical 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.

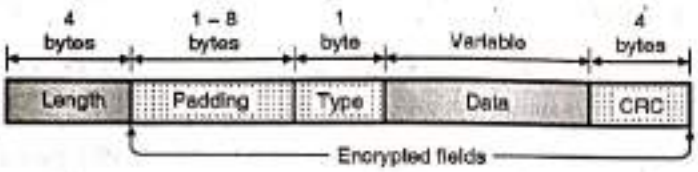


(G-1797) **Fig. 7.22.5 : Port forwarding**

7.22.6 SSH Packet Format :

- The SSH packet format is as shown in Fig. 7.22.6.

Scanned by CamScanner



(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 :

- DHCP (Dynamic host configuration protocol) is the first client server application program that is 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 :
  1. Subnet mask of the computer
  2. IP address of the router, so that it can communicate with other networks.
  3. 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.
- But what will happen if the workstation is discless or the computer is with a disc but it is being booted for the first time.
- If a computer is discless, then it is possible to store the operating system and networking software in the ROM.
- But this information is not known to the manufacture and therefore cannot be stored in ROM.
- This information is dependent on the configuration of individual machine and it defines which network the machine is connected to.

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.

RARP :

We will discuss this protocol in section 5.25.1.

BOOTP :

- The Boot strap protocol (BOOTP) was being used exclusively prior to DHCP. This protocol is a client/server protocol and it is designed in such a way that the demerits of RARP could be overcome.
- Due to the client / server nature of BOOTP, its server can be present anywhere in the Internet.
- Also it can provide all the information that we mentioned earlier. It removes all the restrictions faced by RARP on providing this information.
- The problem with BOOTP is that is a **static configuration protocol.** That means when a client asks BOOTP to find its IP address, the BOOTP server will go through **a table** which contains the IP addresses corresponding to the physical addresses of the client and sends the IP address of the requesting client.
- But there are some situations in which the static configuration protocol like BOOTP does not work properly.
- For example when a host moves from one physical network to the other, its physical address is bound to change.
- Or another example is when a host wants a temporary IP address for using over only a short period of time.
- It is not possible for BOOTP to handle the situations mentioned above due to its static nature. Instead we need a **protocol** with **dynamic configuration** to deal with deal with there situations.

7.23.2 DHCP :

- The Dynamic Host Configuration Protocol (DHCP) was devices 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.
- Thus DHCP allows the use of computers that, run server software as well as computers that run client software.

Scanned by CamScanner

- 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 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.

7.23.4 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.

Scanned by CamScanner

- 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.

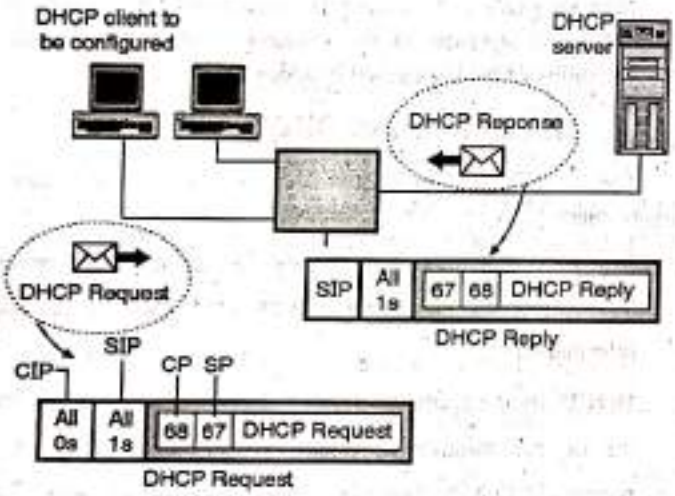
7.23.5 DHCP Operation :

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.

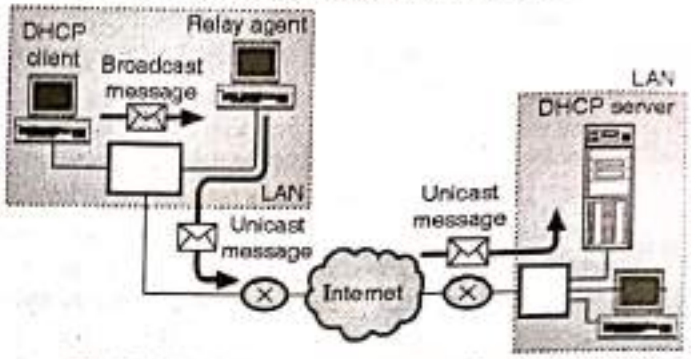


(G-1789) **Fig. 7.23.1 : Operation of DHCP when client and server are on the same network**

- 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.
  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.

7.23.6 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.



(G-1790) **Fig. 7.23.2 : DHCP operation when client and server are on different networks**

- 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.

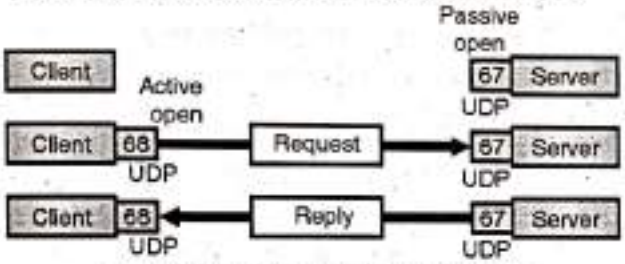
Note : In Fig. 7.23.2 only the message between the relay agent and client is it broadcast type. All the other messages are unicast types.

7.23.7 UDP Ports :

- The interaction between a client and DHCP server has been shown in Fig. 7.23.3. The well known port 67 is used by the server, which is normal. But the client uses the well known port 68, which is not normal. It is unusual.
- Why does a client choose the well known port 68 rather than an ephemeral port ? The answer is for prevention of a problem when the reply from the server to client is of **broadcast** type.
- In order to understand the exact nature of the problem, let us assume that an **ephemeral port** is used instead of the well known port 68 and study its effect.

Scanned by CamScanner

- Suppose host A on a network is using a DHCP client. It is using the ephemeral port say 2017 which we have chosen randomly.
- On the same network, there is another host B, which is using a DAYTIME client on ephemeral port 2017 which is accidentally the same.
- In this situation, the DHCP server sends a broadcast reply message with the destination port number 2017 and broadcast IP address $FFFFFFFF_{16}$.
- Every host has to open a packet which carries this destination IP address.
- Host A would find a message from an application program on ephemeral port 2017. Thus the DHCP client receives a **correct message** but the DAYTIME client receives an **incorrect message.**
- This confusion takes place due to the process of demultiplexing which is based on the **socket address.** Remember that a socket address is the combination of IP address and port number and both are same in this case.



(G-1994) **Fig. 7.23.3 : Use of UDP ports**

- If a well known port (less than 1024) is used then the use of same two destination port numbers would be prevented. It would not be possible for host B to select port 68 as the ephemeral port due to the fact that ephemeral port numbers are greater than 1023.
- The final question is what happens if host B is also running the DHCP client ? The answer is that because of the same socket address, both the clients will receive the message.
- In order to handle such a situation, **the third identification number** is used to differentiate the clients.
- In DHCP this another number is called as the **transactional ID** and for each DHCP connection, it is chosen randomly.
- It is almost impossible that both the host choose the same transactional ID.

7.23.8 Using TFTP :

- Note that all the information needed by a client for booting purpose is not sent by the server.
- The server, in its reply message will define the **pathname** of a file in which all the booting information needed for the client is sent.
- The client can then use a TFTP message that is encapsulated in a UDP user datagram, to obtain the remaining necessary information.

7.23.9 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.

7.23.10 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 its 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 reduce network traffic.

7.23.11 Packet Format :

- The format of a DHCP packet has been shown in Fig. 7.23.4. Let us describe each field in the DHCP packet.

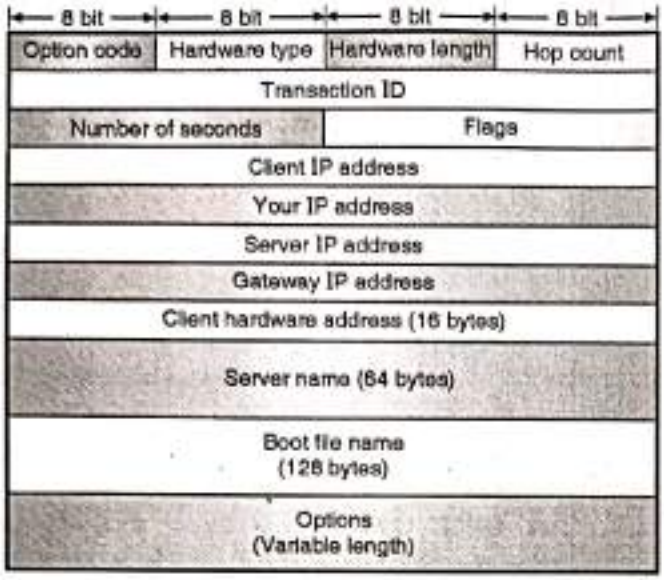
1. Operation code :

- This is an 8 bit field which is used to define the type of DHCP packet.
- If this field contains (1) then the packet is **request type** and if this field contains (2) then the packet is **reply type.**

2. Hardware type :

- This 8-bit field is used to define the type of physical network.
- An integer has been assigned to each type of network e.g. the value of this field is 1 for Ethernet.

Scanned by CamScanner



(G-1995) **Fig. 7.23.4 : DHCP packet format**

3. Hardware length :

- This is an 8-bit field which is used for defining the length of the physical address in bytes.
- The value of this field is 6 for Ethernet because the physical address of Ethernet is 6 byte long.

4. Hop count :

- This is an 8-bit field which is used for define the maximum number of hops a packet can travel.

5. Transaction ID :

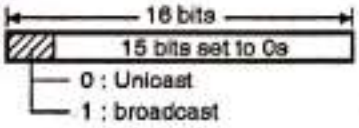
- This is a 32-bit or 4-byte long field which carries an integer in it. The contents of this field are known as **transaction identification** and it is set by the client.
- This field is used for matching a reply with the request. The same value is returned by the server in its reply packet.

6. Number of seconds :

- This is a 16-bit field which is used to indicate the amount of time (in seconds) elapsed from the instant at which the client started to boot.

7. Flag :

- This is a 16-bit long field, as shown in Fig. 7.23.5. Out of these 16 bits, only the leftmost bit is used and the remaining 15 bits are set to 0s.



(G-1996) **Fig. 7.23.5 : Format of the flagfield**

- The leftmost bit is used to specify a forced broadcast reply (instead of unicast) from the server.

8. Client IP address :

- This 4-byte long field is used to carry the client IP address. A "0" in this field indicates that the client does not have this information.

9. Your IP address :

- This is also a 4-byte long field which is used to carry the clients IP address. This address is requested by the client and filled by the server in the reply message.

10. Server IP address :

- This is also a 4-byte long field which contains the IP address of the server. This address is sent by the server in the reply message

11. Gateway IP address :

- This is a 4-byte or 32 bit long field that contains the IP address of a router which is filled in the reply message by the server.

12. Client hardware address :

- This is a 16-byte field which contains the physical address of the client.

13. Server name :

- This is a 64 byte long field which is filled on the optional basis by the server in a reply packet.
- This field consists of a null terminated string containing the domain name of the server.
- If no information about the server name is to be given, then the server should fill up this field with all zeros.

14. Boot filename :

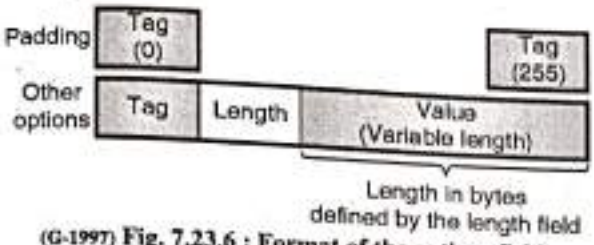
- This is a 128-byte field which contains a null terminated string consisting of full pathname of the boot file.
- This path can be used by the client in order to obtain additional information about booting.
- This field is filled by the server in the reply message on the optional basis.
- If the server does not want to fill data in this field, then the entire field should be filled up with 0s.

15. Options :

- This is a 64-byte field which can be used for a dual purpose as follows :
  1. It is used to carry some additional information such as default router address or network mask.
  2. Or it is used to carry some specific information about the vendor.
- It is important to note that, the **options** field is used only in the **reply message.**
- The server makes use of a number called **magic cookie.** After finishing reading of the message the client searches for the magic cookie.
- If it is present, then the next 60 bytes data will correspond to **options.**
- Fig. 7.23.6 shows the format of the option. It consists of three fields as follows : a 1-byte **tag** field, a 1-byte **length** field and a variable length **value** field.

Scanned by CamScanner

- The function of the length field is to specify the length of the variable length **value** field and not of the whole option.



(G-1997) **Fig. 7.23.6 : Format of the options field**

Review Questions

Q. 1 Explain in brief about the application layer.

Q. 2 Write a short note on providing services.

Q. 3 Explain about the standard and nonstandard protocols at the application layer.

Q. 4 Explain in brief client-server paradigm.

Q. 5 State the problems and applications of client-server paradigm.

Q. 6 Explain the P2P paradigm.

Q. 7 State the merits, demerits and applications of P2P paradigm.

Q. 8 Explain the term API and state its types.

Q. 9 Define a socket and state its role.

Q. 10 Explain the concept of socket interface.

Q. 11 Define the socket address.

Q. 12 Explain how to find the socket addresses at the server site.

Q. 13 Explain how to find the socket addresses at the client site.

Q. 14 Draw and explain the structure of www.

Q. 15 Explain the term URL.

Q. 16 Write a note on web documents.

Q. 17 Explain the non-persistant and persistant connections in HTTP.

Q. 18 Write a note on : HTTP messages.

Q. 19 What is FTP ? Explain the communication in FTP.

Q. 20 Write a note on E-mail.

Q. 21 Explain the principle of MIME.

Q. 22 Compare SMTP and HTTP.

Q. 23 Write a note on message access agents.

Q. 24 Explain the concept of TELNET.

Q. 25 Explain SSH and its packet format.

Q. 26 Briefly discuss the following terms, emphasis more on implementation details :
(a) DNS (b) Mail server

Q. 27 When web pages are sent out, they are prefixed by MIME headers ? Why ?

Q. 28 What is domain name system ? How does it work ? Explain resolution process.

Q. 29 What is mailing list ? Explain with suitable block diagram.

Q. 30 Describe a typical resolution process in DNS.

Q. 31 Write short notes on domain name resolution.

Q. 32 Explain how file transfer protocol clients servers are configured. Discuss the various FTP and telnet commands.

Q. 33 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.

7.24 University Questions and Answers (New Syllabus) :

Dec. 2018 [Total Marks : 10]

Q. 1 Write a short note on SMTP.
(Section 7.20.2) **(10 Marks)**

□□□

Scanned by CamScanner

Solved University Question Paper of Dec. 2018

Dec. 2018

[TIME - 3 Hours] [Total Marks : 80]

N.B. : Question No. 1 is compulsory.

Attempt any three questions out of remaining questions.

Make suitable assumption whenever necessary.

Q. 1 Any – 5 **(20 Marks)**

(a) What are the design issues for the OSI layers ? **(Section 1.12)**

(b) Differentiate between connection oriented and connectionless service ? **(Section 1.14.3)**

(c) List the advantages of fiber optics as a communication medium. **(Section 2.8.10)**

(d) Explain with examples the classification of IPv4 addresses. **(Section 5.9.1)**

(e) Explain in short different framing methods. **(Sections 3.4.1, 3.4.2, 3.4.3, 3.4.4 and 3.4.5)**

(f) Explain the need of subnet mask in subnetting. **(Section 5.9.10)**

Q. 2 (a) What is topology ? Explain the types of topologies with diagram, advantages and disadvantages. **(Sections 1.4, 1.4.1, 1.4.2, 1.4.3, 1.4.5 and 1.4.6)** **(10 Marks)**

(b) What is IPv4 protocol ? Explain the IPv4 header format with diagram. **(Sections 5.13.2 and 5.13.4)** **(10 Marks)**

Q. 3 (a) Explain CSMA protocols. Explain how collision are handled in CSMA / CD. **(Sections 4.5, 4.5.1 and 4.5.2)** **(10 Marks)**

(b) What is traffic shaping ? Explain leaky bucket algorithm and compare it with token bucket algorithm. **(Sections 5.38.2, 5.38.3 and 5.38.5)** **(10 Marks)**

Q. 4 (a) What is ICMP protocol ? Explain the ICMP header format with diagram. **(Sections 5.26 and 5.26.3)** **(10 Marks)**

(b) Write a program for client server application using Socked Programming (UDP). **(Section 6.26.2)** **(10 Marks)**

Q. 5 (a) Explain the use of TCP timers in detail. **(Section 3.5.1)** **(10 Marks)**

(b) Compare open loop congestion control and closed loop congestion control. **(Section 5.37.5)** **(10 Marks)**

Scanned by CamScanner

Q. 6 Write a short note on the following **(Any Two) :** **(20 Marks)**

(a) Internetworking Devices **(Section 4.23)**

(b) Distance Vector Routing **(Section 5.21.1)**

(c) ARP / RARP **(Sections 5.24 and 5.25.1)**

(d) SMTP **(Section 7.20.2)**

Scanned by CamScanner

Your Success is Our Goal

Strictly as per the New Revised Syllabus (Rev - 2016) of Mumbai University w.e.f. academic year 2018-2019 (As per Choice Based Credit and Grading System)

MU

Semester V - Computer Engineering

Computer Networks
J. S. Katre

Database Management System
Mahesh Mali

Microprocessor
Harish G. Narula

Theory of Computer Science
Dilip Kumar Sultania

Multimedia System (Dept. Elective I)
Tulsiram Sule, Poonam Kadam

Advance Operating System (Dept. Elective I)
Rajesh D. Kadu

coming soon.....
easy-solutions
now with TechKnowledge Publications

Head Office :
B/5, First Floor, Maniratna Complex, Taware Colony, Aranyeshwar Corner,
Pune - 411009. Maharashtra State, India. Tel. : 91-20-24221234, 91-20-24225678

ISBN : 978-93-89233-52-0

Price ₹ 365/-

M045A

Distributors

Student's Agencies (I) Pvt. Ltd. T. : (022) 40496161, 91672 90777 | Vidyarthi Sales Agencies T. : (022) 23867279, 98197 76110 | Bharat Sales Agency T. : (022) 23819359, 86572 92797

Our Branches : Pune | Mumbai | Kolhapur | Nagpur | Solapur | Nashik

For Library Orders Contact - Ved Book Distributors M : 80975 71421 / 92208 77214

Email : info@techknowledgebooks.com | Website : www.techknowledgebooks.com | Like us at: TechknowledgePublications

Scanned by CamScanner