Module 0

Chapter 1 : Pre-requisites 1-1 to 1-9

Syllabus : Von Neumann Model, Modulation, Demodulation, Encoding, Decoding.

1.1 Introduction 1-1
1.2 Introduction to Data Communication 1-1
1.2.1 Definition of Data Communication 1-1
1.2.2 Why Study Data Communication ? 1-1
1.2.3 Characteristics of Data Communication System 1-1
1.3 Components of Data Communication System 1-2
1.4 Data Communication Model 1-2
1.5 Data Representation 1-2
1.6 Line Configurations 1-3
1.6.1 Type of Connections (Topology) 1-3
1.6.2 Point-to-Point Connection 1-3
1.6.3 Multipoint Connection 1-3
1.7 Types of Communication Simplex, Half Duplex, Duplex 1-3
1.7.1 Simplex Systems 1-3
1.7.2 Half Duplex Systems 1-4
1.7.3 Full Duplex Systems 1-4
1.8 The Elements of Analog Communication System 1-4
1.9 Baseband and Bandpass Signals 1-5
1.10 Baseband Signal and Baseband Transmission 1-6
1.10.1 Baseband Signal 1-6
1.10.2 Baseband Transmission (Transmission without Modulation) 1-6
1.11 Modulation 1-6
1.12 Need of Modulation 1-7
1.13 Different Types of Modulation Systems 1-7
1.14 Demodulation or Detection 1-7
1.15 Bandwidth 1-7
1.15.1 Frequency Spectrum 1-7
1.15.2 Channel Bandwidth 1-8
1.16 Encoding 1-8
1.16.1 Digital to Digital Conversion 1-8
1.16.2 Digital to Analog Conversion 1-8
1.16.3 Analog to Analog Conversion 1-8
1.16.4 Analog to Digital Conversion 1-9
1.16.5 Decoding 1-9
• **Review Questions** 1-9

Module I

Chapter 2 : Introduction 2-1 to 2-35

Syllabus : Network criteria, Physical structures, Network types : LAN, WAN, Switching, OSI reference model, TCP/IP suite, Comparison of OSI and TCP/IP, Network devices.

2.1 Computer Networks 2-1
2.1.1 Introduction to Computer Networks 2-1
2.1.2 Computer Network Criteria 2-2
2.2 Goals of Computer Networking 2-2
2.3 Uses of Computer Networks 2-2
2.3.1 Service Provided by the Network for Companies 2-2
2.3.2 Networks for People 2-3
2.4 Physical Structures 2-3
2.4.1 Type of Connections (Topology) 2-3
2.4.2 Point-to-Point Connection 2-3
2.4.3 Multipoint Connection 2-3
2.5 Network Topology Types 2-4
2.5.1 Bus Topology 2-4
2.5.2 Ring Topology 2-5
2.5.3 Star Topology 2-6
2.5.4 STAR LANs 2-6
2.5.5 Mesh Topology 2-7
2.5.6 Tree Topology 2-7
2.5.7 Logical Topology 2-8
2.5.8 Comparison of Ring and Star Topologies 2-8
2.5.9 Comparison of Bus and Star Topologies 2-8
2.5.10 Hybrid Topology 2-8
2.5.11 Comparison of Star Bus and Star Ring Topologies 2-9
2.6 Network Classification by their Geography 2-9
2.6.1 Local Area Networks (LAN) 2-9
2.6.2 Metropolitan Area Network (MAN) 2-10
2.6.3 Wide Area Network (WAN) 2-11
2.6.4 Comparison of LAN, WAN and MAN 2-12

2.7 Introduction to Switched Network 2-13
2.7.1 Switching Methods 2-13
2.7.2 Circuit Switching Networks 2-13
2.7.3 Telegraph networks and message switching 2-14
2.7.4 Packet Switching 2-14
2.7.5 Comparison of Message, Circuit and Packet Switching 2-16
2.8 Network Models 2-16
2.9 Protocol Layering 2-16
2.9.1 Scenarios 2-17
2.9.2 Principles of Protocol Layering 2-18
2.9.3 Logical Connections 2-18
2.10 TCP/IP Protocol Suite 2-18
2.10.1 Layered Architecture 2-18
2.10.2 Layers in the TCP/IP Protocol Suite 2-19
2.11 Detailed Description of Each Layer 2-19
2.11.1 Detailed Introduction to Physical Layer 2-20
2.11.2 Detailed Introduction to Data Link Layer 2-20
2.11.3 Detailed Introduction to Network Layer 2-21
2.11.4 Detailed Introduction to Transport Layer 2-21
2.11.5 Detailed Introduction to Application Layer 2-22
2.12 Encapsulation and Decapsulation 2-22
2.12.1 Encapsulation at the Source Host 2-22
2.12.2 Decapsulation and Encapsulation at the Router 2-23
2.12.3 Decapsulation at the Destination Host 2-23
2.13 Addressing 2-23
2.14 Multiplexing and Demultiplexing 2-24
2.15 Connection Oriented and Connectionless Services 2-24
2.16 Relationship of Services to Protocols 2-25
2.16.1 Service 2-25
2.16.2 Protocol 2-25
2.17 OSI Model 2-25
2.17.1 Functions of Different Layers 2-27
2.17.2 Exchange of Information using the OSI Model 2-28
2.17.3 Physical Layer 2-28
2.17.4 Data Link Layer 2-29
2.17.5 Network Layer 2-30
2.17.6 Transport Layer 2-30
2.17.7 The Session Layer 2-31
2.17.8 Presentation Layer 2-31
2.17.9 Application Layer 2-32
2.17.10 Merits of OSI Reference Model 2-33
2.17.11 Demerits of OSI Model 2-33
2.18 Comparison of OSI and TCP/IP Models 2-33
2.19 Network Connecting Devices 2-34
• **Review Questions** 2-35

Module II

Chapter 3 : Application Layer 3-1 to 3-37

Syllabus : Introduction, Providing services, Application layer paradigm, Client-server paradigm : Application programming interface, Using services of transport layer, Standard client server applications : World wide web and HTTP, FTP, Electronic mail, Telnet, Secure shell (SSH) and Domain Name System (DNS).

3.1 Introduction 3-1
3.1.1 Position of Application Layer 3-1
3.2 Providing Services 3-2
3.2.1 Standard and Non-standard Protocols 3-2
3.2.2 Standard Protocols (Application Layer) 3-2
3.2.3 Nonstandard Protocols (Application Layer) 3-2
3.3 Application Layer Paradigms 3-2
3.3.1 Traditional Paradigm Client Server 3-2
3.3.2 New Paradigm Peer-to-Peer (P2P) 3-4
3.3.3 Mixed Paradigm 3-4
3.4 Client Server Paradigm 3-4
3.4.1 Application Programming Interface (API) 3-5
3.4.2 Types of APIs 3-5
3.5 Socket 3-5
3.5.1 Socket Interface 3-5
3.5.2 Socket Address 3-6
3.5.3 Finding Socket Addresses 3-6

Scanned by CamScanner

3.5.3.1 At The Server Site 3-6
3.5.3.2 At the Client Site 3-6
3.6 Using the Services of The Transport Layer 3-7
3.6.1 Users Datagram Protocol (UDP) 3-7
3.6.2 TCP Protocol 3-7
3.6.3 SCTP Protocol 3-8
3.7 Standard Client Server Applications 3-8
3.8 World Wide Web (WWW) 3-8
3.8.1 Web from the Users Side 3-8
3.8.2 Web from the Servers Side 3-9
3.8.3 WWW Architecture 3-10
3.8.4 Browser (Web Client) 3-10
3.8.5 Server 3-10
3.8.6 Uniform Resource Locator (URL) 3-11
3.8.7 Cookies User-Server Interaction 3-11
3.9 Web Documents 3-11
3.9.1 Static Documents 3-11
3.9.2 HTML (Hypertext Markup Language) 3-12
3.9.3 Dynamic Document 3-12
3.9.4 Common Gateway Interface (CGI) 3-12
3.9.5 Active Documents 3-12
3.10 HTTP(Hypertext Transfer Protocol) 3-13
3.10.1 Principle of HTTP Operation 3-13
3.10.2 The Web and HTTP 3-14
3.10.3 Non-persistent and Persistent Connection 3-14
3.10.4 HTTP Messages 3-15
3.10.5 Request Message 3-15
3.10.6 Methods (Request Type) 3-16
3.10.7 Response Message 3-16
3.10.8 Headers 3-16
3.11 Proxy Server 3-17
3.11.1 HTTP Security 3-17
3.12 File Transfer Protocol (FTP) 3-17
3.12.1 Communication in FTP 3-18
3.12.2 File Types 3-19
3.12.3 Data Structure 3-19
3.12.4 Transmission Mode 3-19
3.12.5 File Transfer 3-19
3.12.6 FTP Commands 3-19
3.12.7 Anonymous FTP 3-19
3.12.8 Security for FTP 3-20
3.13 Electronic Mail 3-20
3.13.1 E-mail Architecture and Services 3-20
3.13.2 Message Formats 3-21
3.14 MIME – Multipurpose Internet Mail Extensions 3-22
3.14.1 Principle of MIME 3-22
3.15 Message Transfer Agent SMTP 3-23
3.15.1 Commands and Responses 3-24
3.15.2 SMTP (Simple Mail Transfer Protocol) 3-24
3.15.3 Components of E-mail System 3-24
3.15.4 SMTP Commands 3-25
3.15.5 SMTP Operation 3-25
3.15.6 Comparison of HTTP and SMTP 3-25
3.16 Message Access Agent POP and IMAP 3-26
3.16.1 POP 3 3-26
3.16.2 IMAP4 3-26
3.16.3 Comparison of IMAP and POP 3 3-27
3.17 Remote Login TELNET and SSH 3-27
3.17.1 TELNET 3-27
3.17.2 Network Virtual Terminal (NVT) 3-28
3.17.3 Security Problems of TELNET 3-28
3.17.4 Secure Shell (SSH) 3-29
3.17.5 Port Forwarding 3-29
3.17.6 SSH Packet Format 3-30
3.18 Domain Name System (DNS) 3-30
3.18.1 How does DNS Work ? 3-30
3.18.2 Name Space 3-30
3.18.3 Flat Name Space 3-30
3.18.4 Hierarchical Name Space 3-30
3.19 Domain Name Space 3-30
3.20 Distribution of Name Space 3-32
3.20.1 Hierarchy of Name Servers 3-32
3.21 DNS in the Internet 3-33
3.21.1 Generic Domains 3-33
3.21.2 Country Domain 3-33
3.21.3 Inverse Domain 3-33
3.22 Name Address Resolution 3-33
3.22.1 Recursive Resolution 3-34
3.22.2 Iterative Resolution 3-34

3.22.3 The DNS Message Format 3-34
3.22.4 Caching 3-35
3.23 DNS Records 3-35
3.23.1 Question Records 3-35
3.23.2 Resource Record 3-35
3.23.3 Encapsulation 3-36
3.23.4 Registrars 3-36
3.24 DDNS 3-36
3.24.1 Security of DNS 3-36
• **Review Questions** 3-36

Module II

Chapter 4 : Multimedia 4-1 to 4-40

Syllabus : Compression : Lossless compression, Lossy compression, Multimedia data : Text, Image, Video, Audio, Multimedia in Internet : Streaming stored Audio / Video, Streaming live audio / video, Real time interactive audio / video, Optimal compression algorithms, Huffman coding, Adaptive Huffman compression, Dictionary based compression, Speech compression, LZW, RLE, Image compression GIF, JPEG.

4.1 Multimedia 4-1
4.2 Compression 4-1
4.2.1 Lossless Compression 4-1
4.2.2 Lossy Compression 4-1
4.2.3 Lossless Compression 4-2
4.2.4 Lossy Compression 4-2
4.2.5 Pulse Code Modulation (PCM) 4-2
4.2.6 Delta Modulation (D.M.) 4-3
4.2.7 Adaptive Delta Modulation (ADM) 4-5
4.2.8 Differential Pulse Code Modulation (DPCM) 4-5
4.2.9 Adaptive Differential PCM (ADPCM) 4-5
4.2.10 Linear Predictive Coding 4-5
4.3 Transform Coding 4-5
4.3.1 Difference between Lossless and Lossy Compression 4-6
4.4 Multimedia Data 4-6
4.4.1 Text 4-6
4.4.2 Images 4-6
4.4.3 Video 4-7
4.4.4 Audio 4-7
4.5 Multimedia in Internet 4-7
4.5.1 Streaming 4-7
4.5.2 Streaming Live Audio / Video 4-7
4.5.3 Interactive Audio / Video 4-7
4.5.4 Problems for Multimedia in Today's Internet 4-7
4.5.5 Expectations of Multimedia from the Internet 4-8
4.6 Streaming Stored Audio and Video 4-10
4.6.1 Functions Performed by Media Players 4-10
4.6.2 Accessing Audio and Video Through a Web Server 4-11
4.7 Streaming Stored Audio / Video 4-11
4.7.1 Using a Web Server 4-11
4.7.2 Using a Web Server with a Metafile 4-12
4.7.3 Using a Media Server 4-12
4.7.4 Using a Media Server and RTSP 4-13
4.7.5 Example Video on Demand (VOD) 4-13
4.8 Streaming Live Audio and Video 4-14
4.8.1 Example Internet Radio / Web Radio 4-14
4.8.2 Example Internet Television (ITV) 4-14
4.8.3 Example IPTV (Internet Protocol Television) 4-14
4.9 Real Time Interactive Audio and Video 4-15
4.10 Forward Error Correction in Real Time Multimedia 4-15
4.10.1 FEC Techniques 4-15
4.10.2 Error Correction Using Hamming Distance 4-15
4.10.3 Error Correction using XOR 4-16
4.10.4 Chunk Interleaving 4-16
4.10.5 Combining Hamming Distance and Chunk Interleaving 4-16
4.10.6 Compounding High and Low Resolution Packets 4-17
4.11 Skype (Example of Real Time Application) 4-17
4.11.1 SkypeIn 4-17
4.11.2 SkypeOut 4-17
4.12 Optimal Compression 4-18
4.12.1 Optimal Compression Algorithms 4-18

Scanned by CamScanner

4.13 Huffman Coding 4-18
4.13.1 Huffman Encoding and Decoding 4-23
4.13.2 Adaptive Huffman Compression 4-23
4.14 Arithmetic Coding 4-24
4.14.1 Arithmetic Encoding Algorithm 4-24
4.14.2 Steps Followed for Arithmetic Encoding 4-24
4.14.3 Arithmetic Decoding Algorithm 4-25
4.14.4 Steps Followed for Arithmetic Decoding 4-26
4.15 Dictionary Based Compression 4-26
4.15.1 Lempel ZIV Coding 4-27
4.15.2 LZW (Lempel Ziv Welch) Data Compaction 4-30
4.16 Run Length Encoding (RLE) 4-30
4.16.1 Alternative Format of RLE 4-31
4.17 Speech Compression 4-31
4.17.1 Digitizing Audio 4-32
4.17.2 Audio Compression 4-32
4.17.3 Audio Compression for Telephone Speech Signal 4-32
4.17.4 Audio Compression for Wideband Speech Signals 4-33
4.18 Image Compression 4-33
4.18.1 Digitizing Video 4-33
4.18.2 Characteristics of Images 4-34
4.18.3 JPEG Standards 4-34
4.18.4 The JPEG Standard for Lossless Compression 4-34
4.18.5 The JPEG Standard for Lossy Compression 4-35
4.18.6 Discrete Cosine Transform (DCT) 4-35
4.18.7 Types of DCT 4-36
4.18.8 One-dimensional DCT 4-36
4.18.9 Properties of DCT Transformation 4-38
4.18.10 Two-Dimensional DCT 4-38
4.19 The MPEG Standards 4-38
4.20 Graphics Interchange Format (GIF) 4-39
4.20.1 Advantages 4-40
4.20.2 Disadvantages 4-40
• **Review Questions** 4-40

Module III

Chapter 5 : Session Layer 5-1 to 5-4

Syllabus : Session layer design issues, Session layer protocol-Remote procedure call (RPC).

5.1 The Session Layer 5-1
5.2 Session Layer Design Issues 5-1
5.3 Session Layer Protocols 5-2
5.4 RPC (Remote Procedure Call) 5-2
5.5 Presentation Layer 5-3
• **Review Questions** 5-4

Module III

Chapter 6 : Transport Layer 6-1 to 6-57

Syllabus : Transport layer services, Transport layer protocols : Simple protocol, Stop-and wait protocol, Go-Back-N protocol (GBN), Selective repeat protocol, Bidirectional protocols : Piggybacking, Internet transport layer protocols, User datagram protocol : User datagram, UDP services, UDP applications, Transmission Control Protocol : TCP services, TCP features, Segment, A TCP connection, State transition diagram, Windows in TCP, Flow control, Error control, TCP congestion control, TCP timers, Options.

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 6-3
6.3.5 Flow Control 6-4
6.3.6 Flow Control at Transport Layer 6-4
6.3.7 Error Control 6-5
6.3.8 Combination of Flow and Error Control 6-6
6.3.9 Congestion Control 6-6
6.3.10 Connectionless and Connection Oriented Services 6-7
6.3.11 Reliability at Transport Layer Versus Reliability at DLL 6-9
6.3.12 Quality of Service (QoS) 6-9
6.4 Transport Layer Protocols 6-10
6.4.1 Simplex Protocol 6-10

6.4.2 Stop and Wait Protocol 6-11
6.4.3 Go Back-N Protocol (GBN) 6-13
6.4.4 Selective Repeat Protocol 6-15
6.4.5 Bidirectional Protocols Piggybacking 6-16
6.4.6 The Internet Transport Protocols (TCP and UDP) 6-16
6.5 User Datagram Protocol (UDP) 6-16
6.5.1 Responsibilities of UDP 6-17
6.5.2 Advantages of UDP 6-17
6.5.3 User Datagram 6-17
6.5.4 UDP Pseudo Header 6-18
6.6 UDP Services 6-19
6.6.1 Process to Process Communication 6-19
6.6.2 Connectionless Services 6-19
6.6.3 Flow and Error Control 6-19
6.6.4 Checksum 6-19
6.6.5 Congestion Control 6-19
6.6.6 Encapsulation and Decapsulation 6-19
6.6.7 Queuing 6-20
6.6.8 Multiplexing and Demultiplexing 6-21
6.6.9 Comparison of UDP and Generic Simple Protocol 6-21
6.7 UDP Applications 6-21
6.8 UDP Features 6-21
6.8.1 Connectionless Service 6-21
6.8.2 Lack of Error Control 6-21
6.8.3 Lack of Congestion Control 6-21
6.8.4 Typical Applications of UDP 6-22
6.9 Transmission Control Protocol (TCP) 6-22
6.9.1 Relationship Between TCP and IP 6-22
6.9.2 Ports and Sockets 6-22
6.10 TCP Services 6-23
6.10.1 Process to Process Communication 6-23
6.10.2 Stream Delivery Service 6-23
6.10.3 Sending and Receiving Buffers 6-24
6.10.4 Bytes and Segments 6-24
6.10.5 Full Duplex Service 6-24
6.10.6 Connection Oriented Service 6-24
6.10.7 Reliable Service 6-25
6.11 Features of TCP 6-25
6.11.1 Numbering System 6-25
6.11.2 Flow Control 6-25
6.11.3 Error Control 6-25
6.11.4 Congestion Control 6-25
6.12 The TCP Protocol 6-25
6.12.1 TCP Segment 6-26
6.12.2 The TCP Segment Header 6-26
6.12.3 Checksum 6-27
6.12.4 Encapsulation 6-28
6.13 A TCP Connection 6-28
6.13.1 TCP Connection Establishment 6-29
6.13.2 Connection Termination Protocol [Connection Release] 6-29
6.13.3 TCP Connection Management 6-30
6.13.4 TCP Connection Release 6-30
6.14 TCP State Transition Diagram 6-30
6.15 Windows in TCP 6-31
6.15.1 Send Window 6-31
6.15.2 Receive Window 6-32
6.16 Flow Control 6-33
6.16.1 Opening and Closing Windows 6-33
6.16.2 Shrinking of Windows 6-33
6.16.3 An Example of Flow Control 6-34
6.16.4 Silly Window Syndrome 6-34
6.16.5 Nagle's Algorithm 6-35
6.17 Congestion Control 6-35
6.17.1 Need of Congestion Control 6-35
6.17.2 Causes of Congestion 6-36
6.17.3 Effects of Congestion 6-36
6.17.4 Difference between Congestion Control and Flow Control 6-36
6.17.5 Principle of Congestion Control 6-37
6.17.6 Congestion Prevention Policies 6-37
6.17.7 Congestion Control in Virtual Circuit Subnets 6-38
6.17.8 Approaches to Congestion Control 6-38
6.18 Congestion Control in Datagram Subnets 6-39
6.18.1 Choke Packets 6-40
6.18.2 Load Shedding 6-41
6.19 Quality of Service (QoS) 6-41
6.19.1 Techniques for Achieving Good QoS 6-41

Scanned by CamScanner

6.19.2 Traffic Shaping 6-41
6.19.3 Leaky Bucket Algorithm 6-42
6.19.4 Token Bucket Algorithm 6-43
6.19.5 Combination of Token Bucket and Leaky Bucket 6-44
6.19.6 Resource Reservation 6-44
6.19.7 Admission Control 6-44
6.19.8 Queuing Disciplines 6-44
6.19.9 FIFO Queuing 6-44
6.19.10 Fair Queuing 6-44
6.19.11 Weighted Fair Queuing 6-45
6.20 TCP Congestion Control 6-45
6.20.1 Slow Start Algorithm 6-46
6.20.2 Internet Congestion Control Algorithm 6-47
6.20.3 Congestion Avoidance (Additive Increase) 6-47
6.21 TCP Timer Management 6-48
6.21.1 Jacobson's Algorithm 6-48
6.21.2 Karn's Algorithm 6-48
6.21.3 Other Timers in TCP 6-49
6.22 Options 6-49
6.22.1 End of Option (EOP) 6-49
6.22.2 No Operation (NOP) 6-50
6.22.3 Maximum Segment Size (MSS) 6-50
6.22.4 Window Scale Factor 6-50
6.22.5 Timestamp 6-51
6.22.6 SACK-Permitted and SACK Options 6-51
6.23 Comparison of UDP and TCP 6-51
6.24 Transitional TCP 6-52
6.25 Sockets and their Programming 6-52
6.25.1 Socket Types 6-53
6.25.2 Berkeley Sockets 6-53
6.25.3 Steps Followed for Socket Programming 6-54
6.25.4 Connectionless Iterative Server (Datagram Socket) 6-54
6.25.5 Connection Oriented Concurrent Server (Stream Socket) 6-54
6.26 Socket Programming with TCP 6-55
6.26.1 Socket Programming with TCP 6-55
6.26.2 Socket Programming with UDP 6-56
6.27 University Questions and Answers 6-57
• **Review Questions** 6-56

Module IV

Chapter 7 : Network Layer **7-1 to 7-117**

Syllabus : Introduction, Network layer services, Packet switching, Network layer performance, Network layer congestion, Structure of a router, Network layer protocols : IPv4 datagram format, IPv4 addresses, Forwarding of IP packets ICMPv4, Unicast routing : General idea, Routing algorithms, Unicast routing protocols, Multicast routing : Introduction, Multicasting basics, Intradomain routing protocols, Interdomain routing protocols, Next generation IP, Packet format, IPv6 addressing, ICMPv6, Mobile IP; Addressing, Agents, Three phases, Inefficiency in mobile IP.

7.1 Network Layer 7-1
7.2 Network Layer Services 7-1
7.2.1 Logical Addressing 7-1
7.2.2 Services Provided at the Source Computer 7-1
7.2.3 Services Provided at Each Router 7-2
7.2.4 Services Provided at the Destination Computer 7-3
7.3 Routing and Forwarding 7-3
7.3.1 Routing 7-3
7.3.2 Forwarding 7-3
7.4 Other Services 7-3
7.4.1 Error Control 7-3
7.4.2 Flow Control 7-3
7.4.3 Congestion Control 7-4
7.4.4 Quality of Service (QoS) 7-4
7.4.5 Security 7-4
7.5 Packet Switching 7-4
7.5.1 Datagram Approach Connectionless Service 7-4
7.5.2 Forwarding Process in a Datagram Network 7-5

7.5.3 Virtual Circuit Approach Connection Oriented Service 7-5
7.5.4 Advantages of Datagram Packet Switching 7-8
7.5.5 Disadvantages of Datagram Packet Switching 7-8
7.5.6 Advantages of Virtual Circuit Packet Switching 7-8
7.5.7 Disadvantages of Virtual Circuit Packet Switching 7-8
7.5.8 Comparison of Datagram and Virtual Circuits 7-8
7.6 Network Layer Performance 7-9
7.6.1 Delay 7-9
7.6.2 Throughput (T) 7-10
7.6.3 Packet Loss 7-11
7.7 Network Layer Congestion 7-11
7.7.1 Congestion 7-12
7.7.2 Need of Congestion Control 7-12
7.7.3 Causes of Congestion 7-12
7.7.4 Difference between Congestion Control and Flow Control 7-13
7.7.5 Principle of Congestion Control 7-13
7.7.6 Congestion Prevention Policies 7-14
7.7.7 Congestion Control in Virtual Circuit Subnets 7-15
7.7.8 Approaches to Congestion Control 7-15
7.7.9 Congestion Control in Datagram Subnets 7-16
7.8 Structure of a Router 7-18
7.8.1 Components of a Router 7-18
7.8.2 Input Ports 7-18
7.8.3 Output Ports 7-19
7.8.4 Routing Processor 7-19
7.8.5 Switching Fabric 7-19
7.8.6 Types of Switching Fabrics 7-19
7.8.7 Crossbar Switch 7-19
7.8.8 Banyan Switch 7-19
7.8.9 Batcher Banyan Switch 7-19
7.9 Network Layer Protocols 7-20
7.10 Internet Protocol Version 4 (IPv4) 7-20
7.10.1 Position of IP 7-20
7.10.2 Internet Protocol (IP) 7-21
7.10.3 Datagrams 7-21
7.10.4 IPv4 Header Format 7-21
7.11 Fragmentation 7-25
7.11.1 Maximum Transfer Unit (MTU) 7-25
7.11.2 Fields Related to Fragmentation 7-26
7.12 Options 7-26
7.12.1 Format 7-26
7.13 Option Types 7-27
7.13.1 No Operation Option 7-27
7.13.2 End of Option Option 7-27
7.13.3 Record-Route Option 7-27
7.13.4 Strict-Source-Route Option 7-27
7.13.5 Loose-Source-Root Option 7-28
7.13.6 Time Stamp Option 7-28
7.14 Checksum 7-28
7.14.1 Checksum Calculation at the Sender 7-28
7.14.2 Checksum Calculation at the Receiver 7-28
7.15 IPv4 Addresses 7-29
7.15.1 Uniqueness of IP Addresses 7-29
7.15.2 Address Space 7-29
7.15.3 Notation 7-29
7.15.4 IPv4 Address Format 7-29
7.16 Classful Addressing 7-30
7.16.1 IPv4 Address Classes 7-30
7.16.2 Formats of Various Classes 7-30
7.16.3 How to Recognize Classes ? 7-31
7.16.4 Two Level Addressing 7-32
7.16.5 Extracting Information in a Block 7-32
7.16.6 Network Address 7-32
7.16.7 Network Mask or Default Mask 7-33
7.16.8 Default Masks for Different Classes 7-33
7.16.9 Finding Network Address using Default Mask 7-34
7.16.10 Three Level Addressing Subnetting 7-34
7.16.11 Special IP Addresses 7-35
7.16.12 Limitations of IPv4 7-35
7.16.13 Classless Addressing 7-36
7.16.14 Supernetting 7-36
7.16.15 Who Decides the IP Addresses ? 7-36

Scanned by CamScanner

7.16.16 Registered and Unregistered Addresses 7-36
7.16.17 Solved Examples 7-37
Classless Addressing in IPv4 7-42
7.17.1 Variable Length Blocks 7-42
7.17.2 The Slash Notation (CIDR Notation) 7-43
7.17.3 Network Mask 7-43
7.17.4 Extracting the Block Information 7-44
7.17.5 Block Allocation 7-45
7.17.6 Relation to Classful Addressing 7-46
7.17.7 Subnetting 7-46
7.17.8 Designing Subnets 7-46
7.17.9 Finding Information about Each Network 7-46
7.17.10 Address Aggregation 7-47
8 Special Addresses 7-48
7.18.1 Special Blocks 7-48
7.18.2 All Zeros Address 7-48
7.18.3 All one Address-Limited Broadcast Address 7-48
7.18.4 Loopback Address 7-48
7.18.5 Private Addresses 7-48
7.18.6 Multicast Addresses 7-48
7.18.7 Special Addresses in Each Block 7-48
7.18.8 Network Address 7-48
7.18.9 Direct Broadcast Address 7-48
19 Host Configuration DHCP 7-49
7.19.1 Previously used Protocols 7-49
7.19.2 DHCP 7-49
7.19.3 Advantages of DHCP 7-50
7.19.4 Components of DHCP 7-50
7.19.5 DHCP Operation 7-50
7.19.6 DHCP Operation on Different Networks 7-51
7.19.7 UDP Ports 7-51
7.19.8 Using TFTP 7-52
7.19.9 Error Control 7-52
7.19.10 Optimizations in DHCP 7-52
7.19.11 Packet Format 7-52
20 Configuration of DHCP 7-53
7.20.1 Static Address Allocation 7-54
7.20.2 Dynamic Address Allocation 7-54
7.20.3 Transition States 7-54
7.20.3.1 Address Acquisition States 7-54
7.20.3.2 Early Lease Termination 7-54
7.20.3.3 Lease Renewal States 7-55
7.21 NAT – Network Address Translation 7-55
7.22 Delivery and Forwarding of IP Packets 7-56
7.22.1 Delivery 7-56
7.22.2 Forwarding 7-56
7.23 ICMPv4 (Internet Control Message Protocol) 7-58
7.23.1 ICMP Encapsulation 7-58
7.23.2 ICMP Messages 7-59
7.23.3 Message Format 7-59
7.24 Error Reporting Messages (ICMPv4) 7-59
7.24.1 Destination Unreachable 7-60
7.24.2 Source Quench Error Message 7-60
7.24.3 Time Exceeded Error Message 7-61
7.24.4 Parameter Problem Error Message 7-61
7.24.5 Redirection Error Message 7-61
7.25 Query Messages (ICMPv4) 7-62
7.25.1 Echo Request and Reply 7-62
7.25.2 Timestamp Request and Reply 7-63
7.25.3 Deprecated Messages 7-63
7.25.4 Checksum 7-64
7.26 Routing 7-64
7.26.1 Types of Routing 7-64
7.26.2 Intra and Interdomain Routing 7-64
7.26.3 Unicast Routing 7-64
7.26.4 Broadcast Routing 7-65
7.26.5 Multicast Routing 7-65
7.27 Routing Algorithms 7-65
7.27.1 Desired Properties of a Routing Algorithm 7-66
7.27.2 Types of Routing Algorithms 7-66
7.27.3 Optimality Principle 7-66
7.28 Static Algorithms 7-67
7.28.1 Shortest Path Routing 7-67
7.29 Dynamic Routing Algorithms 7-67
7.29.1 Distance Vector Routing Algorithm 7-68
7.29.2 Count to Infinity Problem 7-70

7.29.4 Comparison of Link State Routing and Distance Vector Routing 7-72
7.29.5 Hierarchical Routing 7-72
7.30 Unicast Routing Protocols 7-73
7.30.1 Routing 7-73
7.30.2 Cost or Metric 7-74
7.30.3 Routing Tables 7-74
7.31 Routing Protocols 7-74
7.31.1 Unicast Routing Protocols 7-74
7.32 RIP (Routing Information Protocol) 7-74
7.32.1 RIP Updating Algorithm 7-75
7.32.2 Initializing the Routing Table 7-75
7.32.3 Updating the Routing Table 7-75
7.32.4 RIP Operation 7-75
7.32.5 RIP Message Format 7-75
7.33 Request and Response Messages (RIP) 7-76
7.33.1 Request Message 7-76
7.33.2 Response Message 7-76
7.33.3 Timers in RIP 7-76
7.33.4 RIP Version 2 7-77
7.33.5 Problems in RIP 7-78
7.34 OSPF 7-79
7.34.1 Features of OSPF 7-80
7.34.2 Metric 7-80
7.34.3 Types of Links 7-80
7.34.4 Virtual Link 7-81
7.34.5 Graphical Representation 7-81
7.34.6 Link State Advertisements (LSAs) 7-82
7.34.7 OSPF Packet Types 7-82
7.34.8 Link State Update Packet 7-83
7.34.9 General LSA Header 7-83
7.34.10 Router Link LSA 7-84
7.34.11 Router Link Packet 7-84
7.34.12 Network Link LSA 7-84
7.34.13 Summary Link to Network LSA 7-85
7.34.14 Summary Link to AS Boundary Router LSA 7-85
7.34.15 External Link LSA 7-85
7.34.16 Other Packets 7-86
7.34.17 Encapsulation 7-86
7.34.18 Comparison between RIP and OSPF 7-86
7.35 Path Vector Routing 7-86
7.35.1 Path Vector Messages 7-87
7.35.2 Loop Prevention 7-87
7.35.3 Path Attributes 7-87
7.36 Border Gateway Protocol (BGP) 7-87
7.36.1 Types of Autonomous Systems 7-87
7.36.2 CIDR 7-88
7.36.3 Path Attributes 7-88
7.36.4 Types of Attributes 7-88
7.37 BGP Sessions 7-88
7.37.1 External and Internal BGP 7-88
7.37.2 Types of Messages 7-88
7.37.3 Packet Format 7-88
7.37.4 Open Message 7-89
7.37.5 The Update Message 7-89
7.37.6 Keepalive Message 7-90
7.37.7 Notification Message 7-90
7.37.8 Encapsulation 7-90
7.37.9 How does BGP Solve the Count to Infinity Problem ? 7-90
7.38 Multicast Routing Protocols 7-90
7.38.1 Unicasting 7-91
7.38.2 Multicasting 7-91
7.38.3 Broadcasting 7-91
7.38.4 Multiple Unicasting Versus Multicasting 7-91
7.38.5 Emulation of Multicasting with Unicasting 7-92
7.38.6 Applications of Multicasting 7-92
7.39 Multicasting Basics 7-92
7.39.1 Multicast Addresses 7-92
7.39.2 Multicast Addresses in IPv4 7-94
7.39.3 Selection of Multicast Address 7-94
7.39.4 Collection of Information about Groups 7-95
7.40 Internet Group Management Protocol (IGMP) 7-95
7.40.1 Operation of IGMP 7-95
7.40.2 Multicast Forwarding 7-96
7.40.3 Multicasting Approaches 7-97
7.41 Intradomain Routing Protocols 7-97
7.42 MOSPF 7-97
7.43 Multicast Distance Vector DVMRP 7-97

Scanned by CamScanner

7.44 Core Based Tree (CBT) Protocol 7-100
7.45 PIM (Protocol Independent Multicast) 7-100
7.46 MBONE (Multicast Backbone) 7-101
7.47 Interdomain Routing Protocols 7-101
7.48 IPv6 (Next Generation IP) 7-101
7.48.1 IPv6 Packet Format 7-102
7.48.2 Payload 7-102
7.49 IPv6 Addressing 7-103
7.49.1 IPv6 Address 7-103
7.49.2 Notations 7-103
7.49.3 Abbreviation 7-104
7.50 Address Space 7-104
7.50.1 Three Address Types 7-104
7.50.2 Broadcasting and Multicasting 7-105
7.51 Address Space Allocation 7-105
7.51.1 The First Section 7-105
7.51.2 Second Section 7-105
7.51.3 Algorithm 7-106
7.51.4 Assigned or Reserved Blocks 7-106
7.51.5 Unspecified Address 7-106
7.51.6 Loopback Address 7-107
7.51.7 Difference between Loopback Address of IPv4 and IPv6 7-107
7.51.8 Embedded IPv4 Addresses 7-107
7.51.9 Compatible Address 7-107
7.51.10 A Mapped Address 7-107
7.51.11 Calculation of Checksum 7-107
7.52 Global Unicast Block 7-107
7.52.1 Unique Local Unicast Block 7-107
7.52.2 Link Local Block 7-108
7.52.3 Multicast Block 7-108
7.53 Global Unicast Address 7-108
7.53.1 Three Levels of Hierarchy 7-108
7.53.2 Global Routing Prefix 7-108
7.53.3 Autoconfiguration 7-109
7.54 Renumbering 7-109
7.54.1 Migrating to IPv6 (Compatibility to IPv4) 7-109
7.54.2 Comparison between IPv4 and IPv6 7-110
7.54.3 Extension Headers 7-110
7.55 ICMPv6 (Internet Control Message Protocol) 7-111
7.55.1 ICMPv6 Messages 7-111
7.56 Mobile IP 7-112
7.56.1 Addressing 7-112
7.56.1.1 Addressing in Stationary Hosts 7-112
7.56.1.2 Mobile Hosts 7-113
7.56.2 Agents 7-113
7.56.3 Three Phases 7-113
7.56.4 Transparency 7-115
7.56.5 Inefficiency in Mobile IP 7-115
7.56.6 Remedy 7-116
• Review Questions 7-117

Module V

Chapter 8 : Data Link Layer 8-1 to 8-42

Syllabus : Wired Networks : Introduction : Nodes and links, Two types of links, Two sublayers, Data link control : Framing, Flow and Error control, Error detection and correction, Two DLC protocols

8.1 Wired Networks 8-1
8.2 Analog and Digital Signals 8-2
8.2.1 Analog and Digital Data 8-2
8.2.2 Sources of Digital Signal 8-2
8.2.3 Advantages of Digital Signals 8-2
8.2.4 Comparison of Digital and Analog Signals 8-2
8.2.5 Classification of Signals 8-2
8.2.6 Periodic and Non-periodic Signals 8-2
8.2.7 Signal Propagation 8-3
8.3 Data Link Layer Design Issues (Functions of Data Link Layer) 8-3
8.4 Nodes and Links 8-4
8.5 Services Provided to Network Layer 8-4
8.5.1 Types of Services Provided 8-4
8.5.2 Unacknowledged Connectionless Service 8-5
8.5.3 Acknowledged Connectionless Service 8-5
8.5.4 Acknowledged Connection Oriented Service 8-5
8.6 Two Sublayers 8-5
8.6.1 Two Categories of Links 8-5
8.6.2 Two Sublayers 8-5

8.7 Three Types of Addresses 8-5
8.7.1 Unicast Address 8-5
8.7.2 Multicast Address 8-5
8.7.3 Broadcast Address 8-5
8.8 Data Link Control (DLC) 8-6
8.9 Framing 8-6
8.9.1 Framing Methods 8-6
8.9.2 Character Count 8-6
8.9.3 Starting and Ending Character with Character Stuffing 8-6
8.9.4 Character Stuffing 8-6
8.9.5 Starting and Ending Flags, with Bit Stuffing 8-7
8.9.6 Physical Layer Coding Violations 8-7
8.10 Flow and Error Control 8-8
8.11 Error Control 8-8
8.11.1 Function of a Timer 8-8
8.12 Introduction to Error Control Coding 8-9
8.12.1 Need of Error Control Coding 8-9
8.12.2 Types of Errors 8-9
8.12.3 Disadvantages of Coding 8-10
8.12.4 Redundancy 8-10
8.13 Detection Versus Correction 8-10
8.14 Coding 8-10
8.14.1 Modular Arithmetic 8-10
8.14.2 Modulo – 2 Arithmetic 8-10
8.15 Linear Block Codes 8-11
8.15.1 Code Word Structure 8-11
8.16 Error Detection in Block Coding 8-11
8.17 Error Correction 8-11
8.17.1 Hamming Weight of a Code Word [w(x)] 8-12
8.17.2 Hamming Distance 8-12
8.17.3 Minimum Hamming Distance d_{min} 8-12
8.18 Linear Block Codes 8-13
8.18.1 Some Linear Block Codes 8-13
8.18.2 Error Detection 8-13
8.18.3 Parity Checking 8-13
8.18.4 Use of Parity Bit to Decide Parity 8-13
8.18.5 Simple Parity Check Block Code 8-14
8.18.6 Two Dimensional Parity Check (Block Parity) 8-15
8.19 Cyclic Codes 8-16
8.20 Cyclic Redundancy Check (CRC) 8-16
8.20.1 CRC Encoder and Decoder 8-16
8.20.2 Procedure to obtain CRC 8-17
8.20.3 Requirements of CRC 8-17
8.20.4 CRC Generator 8-17
8.20.5 CRC Checker 8-18
8.20.6 Advantages of Cyclic Codes 8-19
8.20.7 Disadvantage of Cyclic Codes 8-19
8.20.8 Solved Examples 8-19
8.21 Checksum 8-22
8.21.1 Advantage of the Checksum Method 8-22
8.21.2 One's Complement Checksum 8-23
8.21.3 Internet Checksum 8-23
8.21.4 Performance 8-24
8.22 Flow Control 8-24
8.23 Elementary Data Link Protocols 8-25
8.23.1 An Unrestricted Simplex Protocol 8-25
8.23.2 A Simplex Stop and Wait Protocol 8-25
8.23.3 A Simplex Protocol for Noisy Channel 8-25
8.23.4 Piggybacking 8-26
8.24 Sliding Window Protocols 8-27
8.24.1 A One Bit Sliding Window Protocol (Stop and Wait ARQ) 8-29
8.24.2 A Protocol using GO Back n 8-31
8.24.3 Pipelining 8-33
8.24.4 Selective Repeat ARQ 8-33
8.24.5 Protocol Performance 8-34
8.25 Two Data Link Control Protocols 8-35
8.26 High Level Data Link Control (HDLC) Protocol 8-35
8.26.1 Frame Structure in HDLC 8-36
8.26.2 Frame Types in HDLC 8-36
8.26.3 Transparency in HDLC 8-38
8.26.4 Bit Stuffing 8-38
8.27 The Data Link Layer in the Internet 8-38
8.28 SLIP-Serial Line IP 8-38
8.29 Point-to-Point Protocol (PPP) 8-39
8.29.1 Services Provided by PPP 8-39

Scanned by CamScanner

8.29.2 Frame Format of PPP 8-39
8.29.3 Transition Phases 8-40
8.29.4 Multiplexing 8-40
8.29.5 PPP Stack 8-40
8.29.6 Link Control Protocol (LCP) 8-41
8.29.7 Authentication Protocols 8-41
8.29.8 Network Control Protocol (NCP) 8-41
8.29.9 Multilink PPP 8-41
8.29.10 Difference between SLIP and PPP 8-41
8.30 University Questions and Answers 8-42
• **Review Questions** 8-42

Module V

Chapter 9 : Medium Access Control 9-1 to 9-27

Syllabus : Medium access control protocols : Random access, Controlled access, Channelization, Link layer addressing, Wired LANs : Ethernet protocol, IEEE project 802, Standard Ethernet, Fast Ethernet (100 Mbps), Gigabit Ethernet, 10 Gigabit Ethernet, Virtual LANs.

9.1 Introduction 9-1
9.1.1 MAC and LLC Sublayers 9-1
9.2 The Channel Allocation Problem 9-1
9.2.1 Static Channel Allocation in LANs and MANs 9-2
9.2.2 Dynamic Channel Allocation in LAN and MAN 9-2
9.3 Multiple Access 9-2
9.3.1 Random Access 9-2
9.3.2 Evolution of Random Access Methods 9-2
9.3.3 Taxonomy (Classification) of Multiple Access Protocols 9-3
9.4 Multiple Access (ALOHA System) 9-3
9.4.1 Pure ALOHA 9-3
9.4.2 Protocol Flow Chart for ALOHA 9-4
9.4.3 Efficiency of an ALOHA Channel 9-4
9.4.4 Slotted ALOHA 9-5
9.4.5 Comparison of Pure and Slotted ALOHA 9-6
9.5 Carrier Sense Multiple Access (CSMA) 9-7
9.5.1 Carrier Sense Multiple Access/Collision Detection (CSMA/CD) 9-7
9.5.2 CSMA/CD Procedure 9-8
9.5.3 CSMA/CA 9-9
9.6 Controlled Access 9-9
9.6.1 Reservation Systems 9-10
9.6.2 Polling 9-10
9.6.3 Token Passing 9-11
9.7 Channelization 9-11
9.7.1 FDMA 9-12
9.7.2 TDMA 9-12
9.7.3 Code Division Multiple Access (CDMA) 9-12
9.7.4 Comparison of FDMA, TDMA and CDMA 9-13
9.8 Link Layer Addressing 9-13
9.9 ARP (Address Resolution Protocol) 9-14
9.9.1 Mapping of IP Address into a MAC Address 9-15
9.9.2 ARP Operation 9-15
9.9.3 ARP Cache Memory 9-16
9.9.4 ARP Packet Format 9-16
9.9.5 Encapsulation 9-16
9.9.6 Operation of ARP on Internet 9-16
9.9.7 Four Different Cases 9-17
9.9.8 Proxy ARP 9-17
9.9.9 The Reverse Address Resolution (RARP) Protocol 9-17
9.10 Wired LANs Ethernet Protocol 9-17
9.11 Ethernet 9-18
9.11.1 Traditional Ethernet 9-18
9.11.2 Bridged Ethernet 9-19
9.11.3 Switched Ethernet 9-19
9.11.4 Full Duplex Ethernet 9-19
9.11.5 Fast Ethernet 9-19
9.11.6 Gigabit Ethernet 9-19
9.12 IEEE Standards 9-19
9.13 Traditional Ethernet 9-20
9.13.1 Traditional Ethernet Frame 9-20
9.13.2 Frame Length 9-20
9.13.3 Addressing 9-21
9.13.4 Types of Addresses 9-21
9.13.5 Physical Properties of Ethernet 9-21
9.14 Physical Layer Implementation of Standard Ethernet 9-21

9.15 Fast Ethernet 9-22
9.15.1 MAC Sublayer and Topology 9-22
9.15.2 Autonegotiation 9-22
9.15.3 Physical Layer Implementation 9-23
9.16 Gigabit Ethernet 9-23
9.16.1 MAC Sublayer 9-23
9.16.2 Physical Layer 9-24
9.16.3 Physical Layer Implementation 9-24
9.16.4 Ten Gigabit Ethernet 9-25
9.17 Virtual LANs 9-25
9.17.1 VLAN Configuration 9-25
9.17.2 Membership 9-26
9.17.3 Configurations 9-26
9.17.4 Communication between Switches 9-26
9.17.5 Advantages of VLANs 9-27
• **Review Questions** 9-27

Module V

Chapter 10 : Other Wired Networks 10-1 to 10-30

Syllabus : Point to point networks, SONET, Switched network : ATM, Connecting devices : Repeaters or hubs, Link layer switches, Routers, Sliding window compression.

10.1 Other Wired Networks 10-1
10.1.1 Point-to-point Networks 10-1
10.1.1.1 Dial-up Connection / Network 10-1
10.1.1.2 DSL (Digital Subscriber Line) 10-2
10.1.1.3 Cable TV 10-3
10.2 Synchronous Optical Network (SONET) 10-6
10.2.1 Architecture 10-6
10.2.2 Synchronous Transport Signals 10-6
10.2.3 SONET Devices 10-6
10.2.4 Terminals 10-7
10.3 Connections 10-7
10.4 SONET Layers 10-7
10.4.1 Path Layer 10-7
10.4.2 Line Layer 10-7
10.4.3 Section Layer 10-7
10.4.4 Photonic Layer 10-7
10.4.5 Relationship between Devices and Layers 10-7
10.5 SONET Frames 10-8
10.5.1 Frame, Byte and Bit Transmission 10-8
10.5.2 STS-1 Frame Format 10-8
10.6 Overheads 10-9
10.6.1 Section Overheads 10-9
10.6.2 Line Overheads 10-10
10.6.3 Synchronous Payload Envelope (SPE) 10-10
10.6.4 Encapsulation 10-11
10.7 Frame Transmission 10-11
10.7.1 STS-1 10-11
10.7.2 Virtual Tributaries 10-11
10.8 SONET Networks 10-11
10.9 Applications of SONET 10-12
10.10 High Bit Rate Services (STS Multiplexing) 10-12
10.11 Asynchronous Transfer Mode (ATM) 10-14
10.11.1 Overview of ATM 10-14
10.11.2 Packet Size 10-15
10.12 ATM Protocol Architecture (ATM Reference Model) 10-15
10.12.1 ATM Logical Connections 10-16
10.12.2 Control Signaling 10-16
10.12.3 ATM Cells 10-17
10.12.4 ATM Service Categories 10-17
10.12.5 ATM Adaptation Layer 10-17
10.12.6 ATM Adaptation Layer (AAL) Services 10-18
10.13 AAL Protocols 10-18
10.13.1 Conversion Sublayer (CS) 10-18
10.13.2 Segmentation and Reassembly (SAR) Sublayer 10-18
10.14 AAL Type 1 10-19
10.14.1 Format of SAR PDU 10-20
10.14.2 Features of AAL 3/4 10-21
10.14.3 AAL Type 5 10-21
10.15 Network Connecting Devices 10-21
10.16 Hubs 10-21
10.16.1 Passive Hubs 10-22
10.17 Repeaters 10-22
10.17.1 Active Hubs 10-22
10.17.2 Intelligent Hubs 10-23
10.18 Bridges 10-23
10.18.1 802 Bridges 10-24
10.18.2 Transparent Bridges 10-24

Scanned by CamScanner

10.18.3 Source Routing Bridges 10-25
10.18.4 Comparison of Transparent and Source Routing Bridge 10-26
10.18.5 Remote Bridges 10-26
10.19 Routers 10-27
10.20 Gateways 10-27
10.21 Switches 10-28
10.21.1 Two Layer Switch 10-28
10.21.2 Three Layer Switch 10-28
10.21.3 Comparison of Hub and Switch 10-29
10.21.4 Media Converters 10-29
10.21.5 Comparison of Router and Bridge 10-29
10.21.6 Comparison of Bridge, Switch and Hub 10-29
• **Review Questions** 10-30

Module VI

Chapter 11 : Data and Signal 11-1 to 11-16

Syllabus : Analog and digital, Transmission impairment, Data rate limits, Performance.

11.1 Analog and Digital Signals 11-1
11.1.1 Analog and Digital Data 11-1
11.1.2 Sources of Digital Signal 11-1
11.1.3 Advantages of Digital Signals 11-1
11.1.4 Comparison of Digital and Analog Signals 11-1
11.1.5 Classification of Signals 11-1
11.1.6 Periodic and Non-periodic Signals 11-2
11.1.7 Signal Propagation 11-2
11.2 Analog Signals 11-2
11.2.1 Simple Analog Signal 11-2
11.2.2 Composite Analog Signal 11-2
11.2.3 Sinewaves 11-2
11.3 Time and Frequency Domain 11-3
11.3.1 Time Domain Display of Analog Signals 11-3
11.3.2 Frequency Domain Display of a Signal 11-4
11.4 Composite Signals 11-4
11.5 Composite Signal and Transmission Medium 11-4
11.5.1 Medium 11-4
11.6 Channel Bandwidth 11-4
11.7 Digital Signals 11-5
11.7.1 Bit Interval (T_b) 11-5
11.7.2 Bit Rate (Data Rate) 11-5
11.7.3 Bauds (or Baud Rate) 11-5
11.7.4 Bit Length 11-6
11.8 Digital Signal as a Composite Analog Signal 11-6
11.9 Digital Versus Analog Bandwidth 11-7
11.9.1 Analog Bandwidth 11-7
11.9.2 Digital Bandwidth 11-7
11.9.3 Types of Channels (Mediums) 11-7
11.9.4 Low-pass Channel 11-7
11.9.5 Bandpass Channel 11-7
11.10 Transmission of Digital Signals 11-7
11.10.1 Baseband Transmission 11-7
11.10.2 Broadband Transmission (with modulation) 11-8
11.10.3 Relation between Required Bandwidth and Bit Rate 11-8
11.11 Some Important Definitions 11-8
11.12 Transmission Impairments 11-8
11.12.1 Attenuation 11-9
11.12.2 Delay Distortion 11-9
11.12.3 Harmonic Distortion 11-9
11.12.4 Noise 11-10
11.12.5 Signal to Noise Ratio 11-11
11.13 Data Rate Limits 11-11
11.13.1 Noiseless Channel : Nyquist Bit Rate 11-11
11.13.2 Noisy Channel : Shannon's Channel Capacity 11-11
11.13.3 Solved Examples 11-12
11.14 Performance 11-14
11.15 Bandwidth 11-14
11.15.1 Signal and Channel Bandwidths 11-14
11.16 Throughput (T) 11-14
11.17 Latency (Delay) 11-15
11.18 Jitter 11-15
11.18.1 Difference between Delay and Jitter 11-16
11.19 Bandwidth Delay Product 11-16
• **Review Questions** 11-16

Module VI

Chapter 12 : Digital and Analog Transmission 12-1 to 12-24

Syllabus : Digital to digital conversion, Analog to digital conversion, Analog transmission : Digital to analog conversion, Analog to analog conversion.

12.1 Digital Transmission 12-1
12.2 Digital to Digital Conversion 12-1
12.2.1 Definition of Line Coding 12-1
12.2.2 Some Important Characteristics of Line Coding 12-1
12.2.3 Signal Level and Data Level 12-1
12.2.4 Pulse Rate and Bit Rate 12-2
12.2.5 DC Component 12-2
12.2.6 Self Synchronization 12-2
12.2.7 Built in Error Detection 12-3
12.2.8 Immunity to Noise Interference 12-3
12.2.9 Complexity 12-3
12.2.10 Bandwidth 12-3
12.3 Classification of Line Codes 12-3
12.4 Unipolar Line Codes 12-4
12.4.1 Unipolar RZ Format 12-4
12.4.2 Unipolar NRZ Format 12-4
12.5 Polar Line Codes 12-4
12.5.1 Polar RZ Format 12-4
12.5.2 Polar NRZ Format 12-4
12.5.3 Split Phase Manchester Format 12-4
12.5.4 Differential Manchester Code 12-5
12.6 Bipolar Line Codes 12-5
12.6.1 Bipolar NRZ Format (AMI) 12-5
12.7 Some other Line Codes 12-5
12.7.1 2 B1Q (Two Binary, One Quaternary) 12-6
12.7.2 MLT-3 (Multi Line Transmission, Three Level) 12-6
12.7.3 NRZ-L (Non Return to Zero Level) 12-6
12.7.4 NRZ-M (Non Return to Zero Mark) 12-6
12.7.5 NRZ-S (Non Return to Zero Space) 12-6
12.7.6 Biphase-M Code 12-6
12.7.7 Biphase-S Code 12-6
12.7.8 Polar Quaternary NRZ Format 12-6
12.7.9 Gray Code 12-7
12.7.10 Differential Encoding 12-7
12.7.11 Comparison of Line Codes 12-7
12.7.12 Block Coding 12-9
12.7.13 Scrambling 12-9
12.8 Analog to Digital Conversion 12-10
12.9 Sampling Process 12-10
12.10 Pulse Code Modulation (PCM) 12-10
12.10.1 PCM Transmitter (Encoder) 12-10
12.10.2 Shape of the PCM Signal 12-11
12.10.3 PCM Receiver (Decoder) 12-11
12.10.4 Quantization Process 12-12
12.10.5 Quantization Error or Quantization Noise e 12-12
12.10.6 Effect of Noise on the PCM System 12-13
12.11 Advantages, Disadvantages and Applications of PCM 12-13
12.11.1 Advantages of PCM 12-13
12.11.2 Disadvantages of PCM 12-13
12.11.3 Applications of PCM 12-13
12.12 Linear Delta Modulation (D.M.) 12-13
12.13 Analog Transmission 12-14
12.14 Digital to Analog Conversion 12-14
12.14.1 Need of Digital Continuous Wave Modulation 12-14
12.14.2 Types of Digital Carrier Modulation 12-15
12.14.3 Advantages and Disadvantages of CW Modulation 12-15
12.15 Amplitude Shift Keying (ASK) or Digital Amplitude Modulation 12-15
12.15.1 Baud Rate (N_b) 12-16
12.15.2 Transmission Bandwidth of the ASK Signal 12-16
12.15.3 Multilevel ASK 12-16
12.16 Frequency Shift Keying (FSK) 12-16
12.16.1 FSK Generation 12-16
12.16.2 Frequency Spectrum of Binary FSK Signal 12-17
12.16.3 Bandwidth of FSK Signal 12-17
12.16.4 Bandwidth for FSK in terms of Baud Rate 12-17
12.16.5 Multilevel FSK (MFSK) 12-17
12.16.6 Advantages of FSK 12-18
12.16.7 Disadvantages of FSK 12-18

Scanned by CamScanner

12.17 Phase Shift Keying (PSK) 12-18
12.17.1 BPSK Generation 12-18
12.17.2 Spectrum of BPSK 12-18
12.17.3 Bandwidth of BPSK 12-19
12.17.4 Advantages of BPSK 12-19
12.17.5 Disadvantage of BPSK 12-19
12.17.6 Applications 12-19
12.17.7 Comparison of Binary Modulation Systems 12-19
12.18 Constellation Diagram 12-20
12.18.1 Constellation Diagram of ASK 12-20
12.18.2 Constellation Diagram of BPSK 12-20
12.19 Quadrature Amplitude Shift Keying (QASK) or QAM 12-21
12.19.1 Types of QAM 12-21
12.19.2 4 QAM and 8 QAM Systems 12-21
12.19.3 Comparison of QASK and QPSK 12-22
12.19.4 Bandwidth of QAM 12-22
12.20 Analog to Analog Conversion 12-22
12.20.1 Types of Analog to Analog Conversion 12-22
12.20.2 Amplitude Modulation (AM) 12-22
12.20.3 Frequency Modulation (FM) 12-23
12.20.4 Phase Modulation (PM) 12-23
12.20.5 Bandwidth of PM 12-24
• **Review Questions** **12-24**

Module VI

Chapter 13 : Bandwidth Utilization **13-1 to 13-22**

Syllabus : Bandwidth utilization, Multiplexing, Spread spectrum.

13.1 Bandwidth Utilization 13-1
13.2 Introduction to Multiplexing 13-1
13.3 Concept of Multiplexing and Demultiplexing 13-1
13.3.1 Types of Multiplexing 13-2
13.4 Frequency Division Multiplexing (FDM) 13-2
13.4.1 FDM Transmitter (Multiplexing Process) 13-2
13.4.2 FDM Receiver (Demultiplexing Process) 13-4
13.4.3 The Analog Carrier System 13-4
13.5 Advantages, Disadvantages and Applications of FDM 13-5
13.5.1 Advantages of FDM 13-5
13.5.2 Disadvantages of FDM 13-5
13.5.3 Applications of FDM 13-5
13.6 Wavelength Division Multiplexing (WDM) 13-5
13.6.1 Application of WDM 13-6
13.6.2 DWDM (Dense WDM) 13-6
13.7 Synchronous Time Division Multiplexing 13-6
13.7.1 PAM - TDM System 13-7
13.7.2 Signaling Rate (r) 13-9
13.7.3 Transmission Bandwidth of a TDM Channel 13-9
13.7.4 Empty Slots 13-9
13.7.5 Data Rate Management 13-10
13.7.6 Frame Synchronization 13-10
13.7.7 Advantages of TDM 13-11
13.7.8 Disadvantages of TDM 13-11
13.7.9 Applications of TDM 13-11
13.8 Comparison of FDM and TDM Systems 13-11
13.9 Digital Signal (DS) Service 13-11
13.9.1 T Lines 13-12
13.9.2 E Lines 13-12
13.9.3 Applications of Synchronous TDM 13-12
13.10 Statistical TDM 13-12
13.10.1 Data Rate of Statistical TDM 13-13
13.10.2 Slot Size 13-13
13.10.3 No Synchronization Bit 13-13
13.10.4 Bandwidth 13-13
13.10.5 Frame Format for Statistical TDM 13-13
13.10.6 Comparison of FDM, Synchronous TDM and Statistical TDM 13-14
13.11 Introduction to Spread Spectrum 13-14
13.11.1 How is the SS Signal Different from the Normal Signal ? 13-14
13.12 Applications of Spread Spectrum Modulation 13-14
13.13 Classification of the Spread Spectrum Modulation Techniques 13-14
13.14 Model of Spread Spectrum Digital Communication System 13-15
13.15 Direct Sequence Spread Spectrum (DS-SS) 13-16

13.15.1 Operation of the Encoder (Transmitter) 13-16
13.15.2 Receiver 13-16
13.15.3 Features of DSSS 13-17
13.15.4 Applications of DS-SS System 13-17
13.16 Frequency Hop Spread Spectrum (FH-SS) Signals 13-17
13.16.1 Types of Frequency Hopping 13-18
13.17 Slow Frequency Hopping 13-18
13.17.1 Operation of the FH/MFSK Transmitter 13-18
13.17.2 FH/MFSK Receiver 13-19
13.18 Fast Frequency Hopping 13-19
13.19 Advantages and Disadvantages of DS-SS and FH-SS Systems 13-21
13.19.1 Advantages and Disadvantages of the DS-SS System 13-21
13.19.2 Advantages and Disadvantages of FH-SS System 13-21
13.20 Comparisons 13-21
13.20.1 Comparison of Slow and Fast Frequency Hopping 13-21
13.20.2 Comparison of DS-SS and FH-SS Systems 13-21
• **Review Questions** **13-22**

Module VI

Chapter 14 : Transmission Media **14-1 to 14-32**

Syllabus : Guided madia, Unguided media, Wireless, Real time interactive protocols ; Rationale for new protocols RTP, Session Initialization Protocol (SIP), H.323, SCTP.

14.1 Transmission Media 14-1
14.1.1 Classification of Transmission Media 14-1
14.1.2 Comparison of Wired and Wireless Media 14-2
14.1.3 Types of Wired Media 14-2
14.1.4 Transmission Media and Physical Layer 14-2
14.2 Twisted Pair Cables 14-2
14.2.1 Types of Twisted Pair Cables 14-3
14.2.2 Applications of Twisted Pair Cables 14-3
14.2.3 Comparison of Twisted Pair Cables 14-3
14.3 Co-axial Cables 14-3
14.3.1 Characteristics of a Co-Axial Cable 14-4
14.3.2 Co-axial Cable Standards 14-4
14.3.3 Applications of Co-axial Cables 14-4
14.4 Optical Fiber Cables 14-4
14.4.1 Light Sources for Fiber 14-5
14.4.2 Principle of Light Propagation in a Fiber 14-5
14.4.3 Relation between Incident Angle and Emerging Angle 14-6
14.4.4 Modes of Propagation 14-6
14.4.5 Single Mode Fibers 14-6
14.4.6 Multimode Fibers 14-6
14.4.7 Characteristics of Optical Fiber Cables 14-8
14.4.8 Comparison of Optical Fiber with Coaxial and Twisted Pair Cables 14-8
14.5 Advantages and Disadvantages of Fiber Optical Fibers 14-9
14.5.1 Advantages of Optical Fibers 14-9
14.5.2 Disadvantages of Optical Fibers 14-9
14.5.3 Applications 14-9
14.6 Unguided (Wireless) Media 14-9
14.6.1 Unguided Media Wireless 14-9
14.6.2 Bands 14-10
14.6.3 EM Spectrum and Communication Applications 14-10
14.6.4 Infrared Signals 14-10
14.6.5 Visible Light 14-11
14.7 Wireless Media 14-11
14.7.1 Radio Wave Transmission Systems 14-11
14.7.2 Modes of Propagation of EM Waves 14-12
14.7.3 Microwave Transmission System 14-13
14.8 Infrared Light Used for Transmission 14-14
14.8.1 Applications and Standards 14-14
14.8.2 Comparison of Point to Point and Broadcast Infrared System 14-15
14.8.3 Applications of Infrared 14-15
14.9 Real Time Interactive Protocols 14-15
14.9.1 Rationale for New Protocols 14-16
14.9.2 Requirements of Transport Layer for Interactive Real Time Multimedia 14-16

Scanned by CamScanner

14.9.3 Whether to use TCP or UDP to Handle Real – Time Multimedia 14-17
14.10 RTP [Real Time Transport Protocol] 14-18
14.10.1 RTP Packet Format 14-18
14.10.2 UDP Port 14-19
14.11 RTCP [RTP Control Protocol] 14-19
14.12 Voice Over IP 14-20
14.13 SIP (Session Initiation Protocol) 14-20
14.13.1 SIP Messages 14-20
14.13.2 SIP Addresses 14-20
14.13.3 Simple SIP Session 14-20
14.13.4 Tracking the Callee 14-21
14.14 H.323 14-21
14.14.1 Protocol 14-22
14.14.2 Comparison of H.323 and SIP 14-23
14.15 Stream Control Transmission Protocol (SCTP) 14-23
14.15.1 UDP Performance for Internet Applications 14-23
14.15.2 TCP Performance for Internet Applications 14-24
14.15.3 SCTP Performance for Internet Applications 14-24
14.16 SCTP Services 14-24
14.16.1 Process to Process Communication 14-24
14.16.2 Multiple Streams 14-24
14.16.3 Multihoming 14-24
14.16.4 Full Duplex Communication 14-25
14.16.5 Connection Oriented Service 14-25
14.16.6 Reliable Service 14-25
14.17 SCTP Features 14-25
14.17.1 Transmission Sequence Number (TSN) 14-25
14.17.2 Stream Identifier (SI) 14-25
14.17.3 Stream Sequence Number (SSN) 14-25
14.17.4 Packets 14-25
14.17.5 Acknowledgement Number 14-26
14.17.6 Flow Control 14-26
14.17.7 Error Control 14-26
14.17.8 Congestion Control 14-26
14.18 Packet Format 14-26
14.18.1 General Header 14-26
14.18.2 Chunks 14-27
14.18.3 DATA 14-27
14.18.4 INIT 14-28
14.18.5 INIT ACK 14-29
14.18.6 COOKIE ECHO 14-29
14.18.7 COOKIE ACK 14-29
14.18.8 SACK 14-29
14.18.9 HEARTBEAT and HEARTBEAT ACK 14-30
14.18.10 SHUTDOWN, SHUTDOWN ACK and SHUTDOWN COMPLETE 14-30
14.18.11 ERROR 14-31
14.18.12 ABORT 14-31
14.18.13 FORWARD TSN 14-31
14.19 University Questions and Answers 14-32
• **Review Questions** 14-31
• **Appendix-A : Von Neumann Model ..... A-1 to A-4**

❑❑❑

CHAPTER 1

Module 0

Pre-requisites

Syllabus :

Von Neumann Model, Modulation, Demodulation, Encoding, Decoding.

1.1 Introduction :

- 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.

1.2 Introduction to Data Communication :

- The data communication and networking allows the exchange of data between any points in world. The data can be audio, text, video or of some other form.
- The transfer of data takes place over a computer network. A network provides path over which the data can travel to the desired destination.

1.2.1 Definition of Data Communication :

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

1.2.2 Why Study Data Communication ?

- In the modern world data communications and networking play a huge role in deciding the way we live and the way we make business.
- In order to make business decision quickly and correctly we need to access latest and accurate information. Computer networks can provide such an information easily.
- Therefore knowledge of how these networks operate, the type of technologies available etc. is essential.
- New developments are taking place everyday in the field of data communication.
- The latest developments in the field of data communication, is that communication links (Such as telephone cables) are made to carry more data at faster speed.
- This has expended the capacity of the networks. As engineers we have to learn and understand all these new trends in the field of data communication and network.

1.2.3 Characteristics of Data Communication System :

The three important characteristics of a data communication system are :

1. Delivery 2. Accuracy 3. Timeliness

1. **Delivery :**

A Data Communication System (DCS) must deliver data only to the user who is intended to use it and not to any one else.

2. **Accuracy :**

- Due to noise the data may get altered or corrected when it is travelling over a communication medium. Errors will be introduced and the accuracy of the received data is adversely affected.
- The Data Communication System (DCS) must be designed in such a way that the delivered data is accurate and free from any errors.

Scanned by CamScanner

CHAPTER 2

Introduction

Module I

Syllabus :

Network criteria, Physical structures, Network types : LAN, WAN, Switching, OSI reference model, TCP/IP suite, Comparison of OSI and TCP/IP, Network devices.

2.1 Computer Networks :

MU : May 14, Dec. 15

University Questions

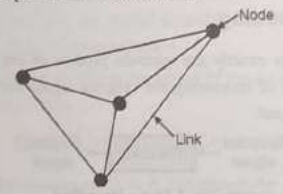
Q. 1 What is a network ? What are its goals and applications ? **(May 14, Dec. 15, 5 Marks)**

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. 2.1.1.
- 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. 2.1.1 : A simple communication network**

2.1.1 Introduction to Computer Networks :

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

Distributed System :

- A system with one control unit (master computer) and many slaves, or a large computer with remote printers and terminals is not called a **computer network, it is called a Distributed System.**
- In distributed system the existence of multiple autonomous computers is not visible to the user.
- With a computer network, the user has to 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 has to be done explicitly, it is all automatically done by the system 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 (sticking together) and transparency.

2.1.2 Computer Network Criteria :

- Network is a broad term similar to system. Network is a communication system which supports many users.
- In context with the computers we can say that, a "computer network" is a system which allows communication among the computers connected in the network.
- A network must be able to meet certain criteria. The most important of them are :
  1. Performance
  2. Reliability
  3. Security.

Performance :

- Performance can be measured in different ways. We can measure it in terms of transit time and response time.
- **Transit time** is defined as the time required for a message to travel from one device to the other.
- **Response time :** It is the time elapsed between the instant of enquiry and the instant of giving response.
- The other factors deciding the performance are as follows :
  1. Number of users.
  2. Type of transmission medium.
  3. The hardware used.
  4. The software used.

Reliability :

- The network reliability is important because it decides the frequency at which network failure takes place.
- It also decides the time taken by the network to recover and its robustness in the catastrophe.

Security :

The network security refers to protection of data from the unauthorized user or access. It also includes the data protection against damage and recovering it in the events of data losses.

2.2 Goals of Computer Networking :

MU : May 14, Dec. 15

University Questions

Q. 1 What is a network ? What are its goals and applications ? **(May 14, Dec. 15, 5 Marks)**

Some of the important goals of computer networks are as follows :

1. Sharing information.
2. Sharing resourses.
3. To facilitate centralized management of resources, softwares, data back up and network security.
4. To increase speed of communication.
5. To reduce cost.
6. To improve security.
7. To provide access to remote information.
8. To facilitate person to person communication (E-mail)
9. To provide interactive communication (gaming, video on demand etc.).

2.3 Uses of Computer Networks :

MU : May 14, Dec. 15

University Questions

Q. 1 What is a network ? What are its goals and applications ? **(May 14, Dec. 15, 5 Marks)**

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

2.3.1 Service Provided by the Network for Companies :

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

1. Resource sharing :

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

2. High reliability due to alternative sources of data :

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

Scanned by CamScanner

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.

2.3.2 Networks for 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 newgroups 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.

2.4 Physical Structures :

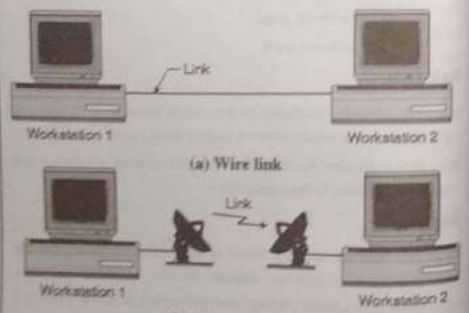
Two characteristics which can be used as the basis of distinguishing various data link configurations are topology and whether the link is half duplex or full duplex.

2.4.1 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.

2.4.2 Point-to-Point Connection :

- A point to point connection provides a dedicated link between two devices as shown in Fig. 2.4.1. 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. 2.4.1(a)) or using a microwave or satellite link (wireless link) as shown in Fig. 2.4.1(b).



(a) Wire link

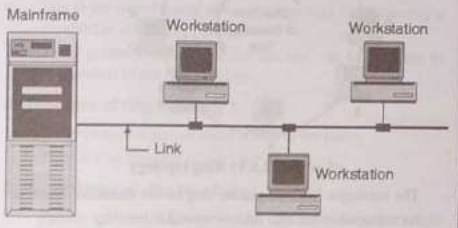
(b) Microwave link

(G-4) Fig. 2.4.1 : Point to point connection

2.4.3 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. 2.4.2.
- 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. 2.4.2 : Multipoint configuration

2.5 Network Topology Types :

MU : May 12, Dec. 14, Dec. 15, May 17

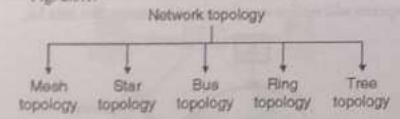
University Questions

Q. 1 Write short notes on : Network topology. **(May 12, Dec. 14, 5 Marks)**

Q. 2 Explain : Network topologies. **(Dec. 15, 5 Marks)**

Q. 3 Write short note network topologies. **(May 17, 5 Marks)**

- 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. 2.5.1.

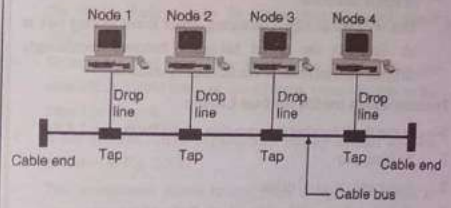


(G-14) Fig. 2.5.1 : Classification of network topology

- These topologies can be classified into two types :
  1. Peer to peer
  2. Primary – secondary
- Peer to peer is the relationship where the devices share the link equally. The examples are ring and mesh topologies.
- In Primary – secondary relationship, one device controls and the other devices have to transmit through it. For example star and tree topology.

2.5.1 Bus Topology :

- The bus topology is usually used when a network under consideration is small, simple or temporary as shown in Fig. 2.5.2.



(G-15) Fig. 2.5.2 : 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.

Scanned by CamScanner

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

Adequate Signal to Noise Ratio (SNR) should be maintained for better quality reception.

The signal should not be too strong. This is necessary to avoid the overloading of transmitter and hence the possibility of signal distortion.

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.

ransmission media for bus LANs :

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

. Twisted pair

. Baseband co-axial cable

. Broadband co-axial cable 4. Optical fibre

dvantages of bus topology :

. The bus topology is easy to understand, install, and use for small networks.

. The cabling cost is less as the bus topology requires a small length of cable to connect the computers.

. The bus topology is easy to expand by joining two cables with a BNC barrel connector.

. In the expansion of a bus topology repeaters can be used to boost the signal and increase the distance.

isadvantages of bus topology :

. 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.

. The BNC connectors used for expansion of the bus attenuates the signal considerably.

. A cable break or loose BNC connector will cause reflections and bring down the whole network causing all network activity to stop.

ote :

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.

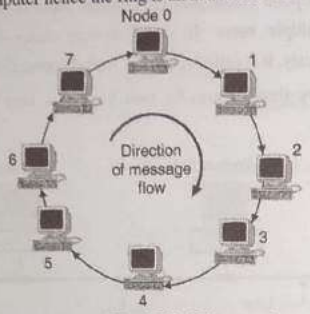
Token bus networks are defined by the IEEE 802.4 standard.

.5.2 Ring Topology :

In a ring topology, each computer is connected to the next computer, with the last one connected to the first as shown in Fig. 2.5.3.

Rings are used in high-performance networks where large bandwidth is necessary e.g. time sensitive features such as video and audio.

- Every computer is connected to the next computer in the ring and each retransmits what it receives from the previous computer hence the ring is an active network.

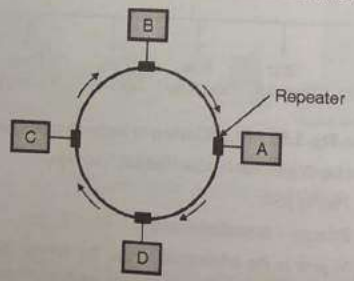


(G-16) **Fig. 2.5.3 : Ring topology**

- The messages flow around the ring in one direction. There is no termination because there is no end to the ring.
- Some ring networks do token passing. A short message called a token is passed around the ring until a computer wishes to send information to another computer.
- That computer modifies the token, adds an electronic address and data and sends it around the ring.
- Each computer in sequence receives the token and the information and passes them to the next computer until either the electronic address matches the address of a computer or the token returns to its origin.
- The receiving computer returns a message to the originator indicating that the message has been received.
- The sending computer then creates another token and places it on the network, allowing another station to capture the token and begin transmitting.
- The token circulates until a station is ready to send and capture the token. Faster networks circulate several tokens at once.
- Some ring networks have two counter-rotating rings that help them recover from network faults.

Characteristics of ring LANs :

- The basic ring LAN is shown in Fig. 2.5.4, 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. 2.5.4 : 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.

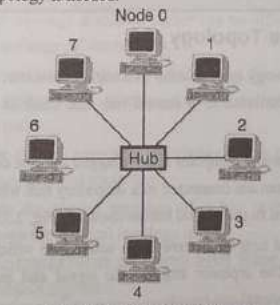
Note : Token ring networks are defined by the IEEE 802.5 standard.

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

2.5.3 Star Topology :

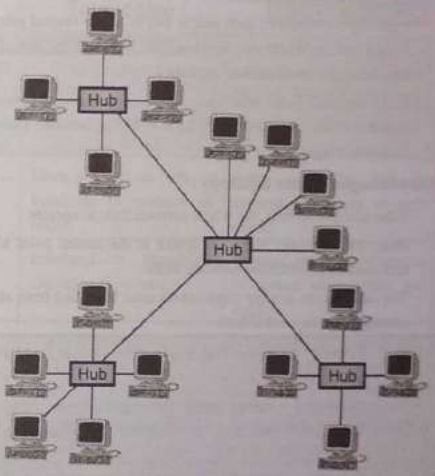
In a star topology all the computers are connected via cables to a central location where they are all connected by a device called a hub as shown in Fig. 2.5.5. There is no direct connections among the computers. All the connections are made via the central hub.

- Stars are used in concentrated networks, where the endpoints are directly reachable from a central location; when network expansion is expected and when the greater reliability of a star topology is needed.



(G-18) **Fig. 2.5.5 : Star topology**

- Each computer on a star network communicates with a central hub. The hub then resends the message to all the computers in a broadcast star network. It will resend the message only to the destination computer in a switched star network.
- The hub in a broadcast star network can be active or passive. An active hub generates the electrical signal and sends it to all the computers connected to it.
- This type of hub is usually called a multiport repeater. Active hubs require external power supply.
- A passive hub is a wiring panel or punch down block which acts as a connection point. It does not amplify or regenerate the signal. Passive hubs do not require electrical power supply.
- Several types of cables can be used to implement a star network. A hybrid hub can use different types of cable in the same star network.
- A star network can be expanded by placing another star hub as shown in Fig. 2.5.6.
- This arrangement allows several more computers or hubs to be connected to that hub. This creates a hybrid star network.



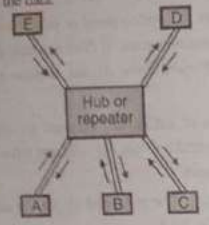
(G-19) **Fig. 2.5.6 : Expansion of star topology**

2.5.4 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.
- The basic star topology is as shown in Fig. 2.5.7. This is called as a single level star topology.

Scanned by CamScanner

- As shown in Fig. 2.5.7, 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.



(G-20) **Fig. 2.5.7 : Single level star topology**

- When a single station transmits, the hub repeats the signal and sends it to each station.
- Typically the length of each link is 100 m. If the twisted pair is used and the length may increase upto 500 m if the optical fibre is used as transmission medium.
- It is important to note that if two stations transmit simultaneously, then there will be a collision between their transmitted signals.

Disadvantages of star topology :

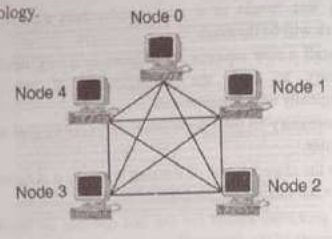
1. If the central hub fails, the whole network fails to operate.
2. Many star networks require a device at the central point to rebroadcast or switch the network traffic.
3. The cabling cost is more since cables must be pulled from all computers to the central hub.

> **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.

2.5.5 Mesh Topology :

In a mesh topology every device is physically connected to every other device with a point to point dedicated link as shown in Fig. 2.5.8.

- The term dedicated means that the link carries data only between two devices connected on it.
- A fully connected mesh network therefore has $n(n-1)/2$ physical cables to connect n devices. To accommodate that many links every device on the network must have n-1 input/output ports.
- So too many cables are required to be used for the mesh topology.



(G-21) **Fig. 2.5.8 : 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.

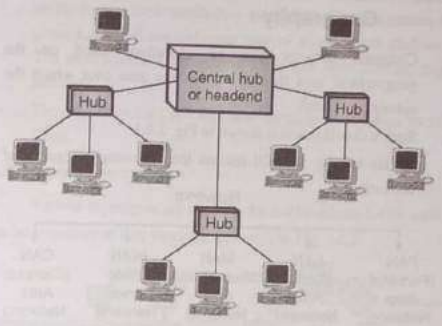
Disadvantages :

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.

2.5.6 Tree Topology :

- A tree topology is a variation of a star. As in a star, nodes in a tree are connected to a central hub that controls the entire network.
- However, every computer is not plugged into the central hub. Most of them are connected to a secondary hub which in turn is connected to the central hub as shown in Fig. 2.5.9.
- 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.



(G-22) **Fig. 2.5.9 : Tree topology**

Advantages :

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

Disadvantages :

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

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

2.5.7 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, eventhough the physical topology is bus.

2.5.8 Comparison of Ring and Star Topologies :

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.

2.5.9 Comparison of Bus and Star Topologies : MU : Dec. 12, May 13

University Questions

Q. 1 Differentiate between star topology and bus topology. **(Dec. 12, May 13, 5 Marks)**

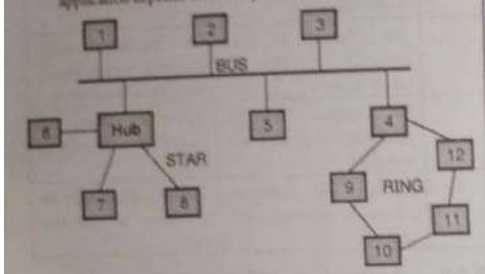
Sr. No.	Bus	Star
1.	Uses a cable as bus or backbone to connect all nodes.	Uses a central hub to connect the nodes to each other.
2.	Baseband or broadband coaxial cable is used.	Twisted pair, coaxial cables or optical fiber cables are used.
3.	If a part of bus fails, the whole network fails.	Failure of 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.

2.5.10 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. 2.5.10 shows the hybrid topology in which bus, star and ring topologies are used simultaneously.
- In Fig. 2.5.10, 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.

Scanned by CamScanner

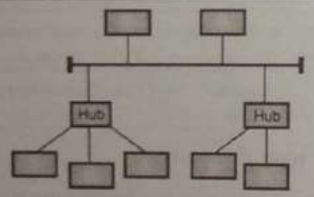
- The practical networks generally make use of hybrid topology. Many complex networks can be reduced to some form of hybrid topology.
- The hybrid topology which is to be used for a particular application depends on the requirements of that application.



(G-23) Fig. 2.5.10 : Hybrid topology

2.5.11 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

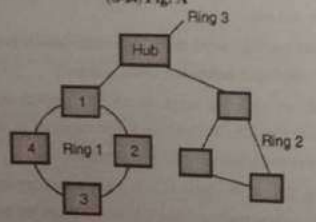
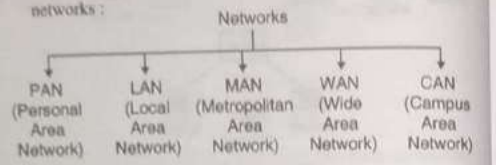


Fig. B

2.6 Network Classification by their Geography :

- Computer network can be classified based on the geographical area they cover, i.e. the area over which the network is spread.
- Such a classification is shown in Fig. 2.6.1.
- In this section, we will discuss the following categories of networks :



(G-1400) Fig. 2.6.1 : Network categories

2.6.1 Local Area Networks (LAN) :

MU : May 05, May 14, Dec. 16

University Questions

Q. 1 Design a LAN network for your institute. **(May 05, 6 Marks)**

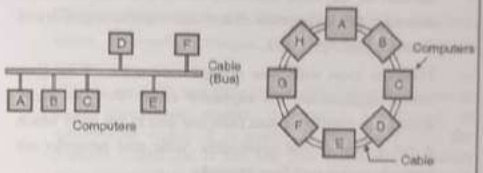
Q. 2 Discuss and compare various types of networks. **(May 14, Dec. 16, 5 Marks)**

- 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. 2.6.1.
- 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. 2.6.2.



(a) Bus topology (b) Ring topology

(G-32) Fig. 2.6.2 : LAN topologies

Static and dynamic broadcast networks :

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

LAN components :

Some of the important LAN components are as follows :

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

Workstation :

Workstation refers to the individual, single computer.

A communication capability is added to enable it for networking.

File server :

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

Gateway :

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

Network Interfacing Unit (NIU) :

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

LAN cables or communication channel :

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

Advantages of LAN :

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

Applications of LAN :

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

2.6.2 Metropolitan Area Network (MAN) :

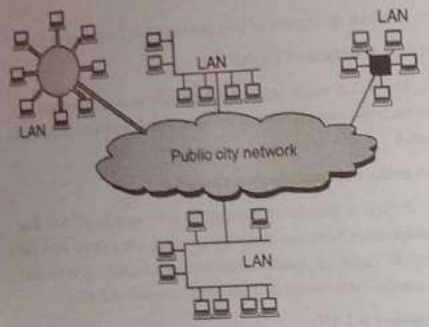
MU : May 14, Dec. 16

University Questions

Q. 1 Discuss and compare various types of networks. **(May 14, Dec. 16, 5 Marks)**

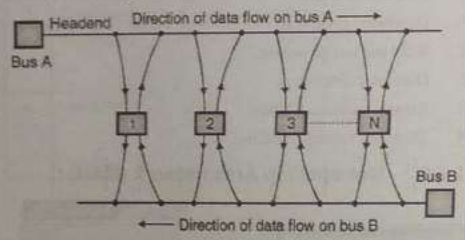
- A MAN is basically a bigger version of a LAN and normally uses similar technology. It is designed to extend over a larger area such as an entire city.
- The MAN can be in the form of a single network such as a cable network or it can be a combination of multiple LANs as shown in Fig. 2.6.3.
- A MAN may be wholly owned and operated by a private company or it may be a service provided by a public company, such as a local telephone company (telco).

Scanned by CamScanner



(G-33)Fig. 2.6.3 : Metropolitan area network

- 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. 2.6.4.
- 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. 2.6.4.



(G-34)Fig. 2.6.4 : Distributed queue dual bus architecture (DQDB)

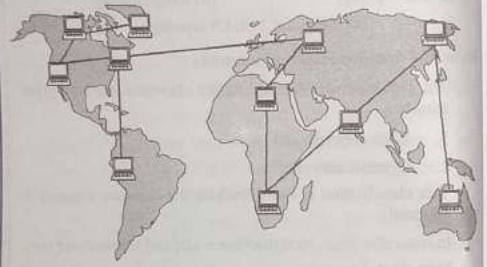
2.6.3 Wide Area Network (WAN) :

MU : May 14, Dec. 16

University Questions

Q. 1 Discuss and compare various types of networks. **(May 14, Dec. 16, 5 Marks)**

- 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.



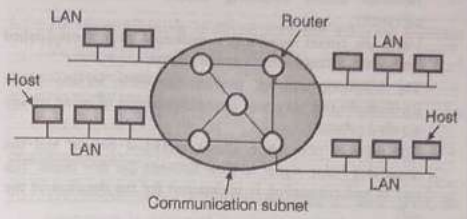
(G-35)Fig. 2.6.5 : Wide area network

- 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. 2.6.5.

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. 2.6.6.
- The function of the subnet is to carry messages from host to host. The subnet consists of two important components; transmission lines and switching elements.
- Transmission lines move bits from one machine to another. The switching elements are specialised computers used to connect two or more transmission lines. When data arrive on an incoming line, the switching element has to choose an outgoing line on which it is to be forwarded.

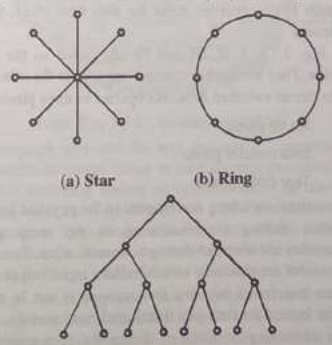


(G-36)Fig. 2.6.6 : Communication subnet and hosts

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

Router interconnection topologies :

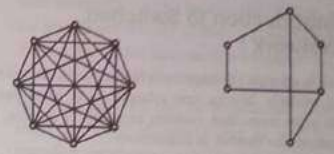
- Fig. 2.6.7 shows some of the possible router interconnection topologies in a point to point subnet.
- The LANs have a symmetric topology while WANs have irregular topologies.
- The WANs can also be formed using satellite or ground radio system. Satellite networks are inherently broadcast type so they are useful when the broadcast property is important.



(a) Star (b) Ring

(c) Tree

(G-37)Fig. 2.6.7



(d) Complete (e) Irregular ring

(G-38)Fig. 2.6.7 : Router interconnection topologies

2.6.4 Comparison of LAN, WAN and MAN :

MU : May 13, May 14, Dec. 15, May 16, Dec. 16

University Questions

Q. 1 Write differences between LAN, MAN and WAN. **(May 13, 5 Marks)**

Q. 2 Discuss and compare various types of networks. **(May 14, Dec. 16, 5 Marks)**

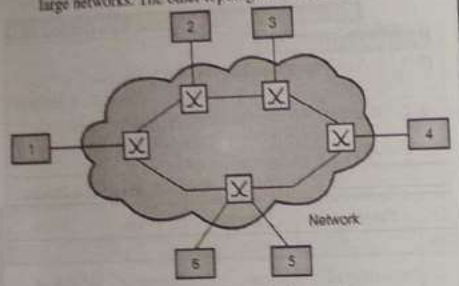
Q. 3 Compare LAN, WAN, MAN. **(Dec. 15, May 16, 5 Marks)**

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

Scanned by CamScanner

2.7 Introduction to Switched Network :

- 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.

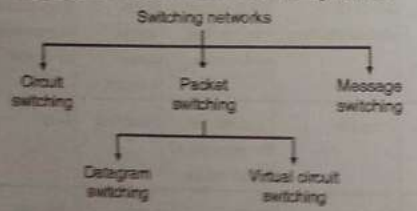


(L-616) **Fig. 2.7.1 : Switched network**

- 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. 2.7.1 shows a switched network.

2.7.1 Switching Methods :

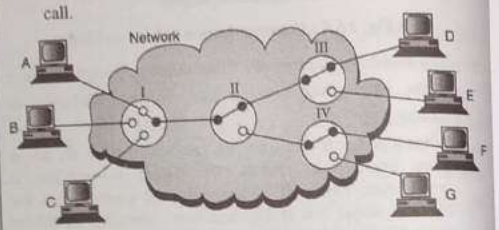
- The three basic methods of switching are :
  1. Circuit switching
  2. Packet switching
  3. Message switching
- Out of these, the circuit and packet switching are commonly used today but the message switching has been phased out in general communication but is still used in the networking applications.
- Fig. 2.7.2 shows the classification of switching methods.



(L-617) **Fig. 2.7.2 : Classification of switching methods**

2.7.2 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.
- The network connection allows electrical current and the associated voice signal to flow between the two users. The end to end connection is maintained for the duration of the call.



(L-618) **Fig. 2.7.3 : Circuit-switched network**

- The telephone networks are connection oriented because they require the setting up of a connection before the actual transfer of information can take place.
- The transfer mode of a network that involves setting up a dedicated end to end connection is called circuit switching.
- In circuit switching the routing decision is made when the path is set up across the network. After the link has been set between the sender and receiver, the information is forwarded continuously over the link. After the link has been set up no additional address information about the receiver or destination machine is required.
- In circuit switching a dedicated path is established between the sender and the receiver which is maintained for the entire duration of conversation, as shown in Fig. 2.7.3.
- 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. 2.7.3, 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).

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.

Disadvantages :

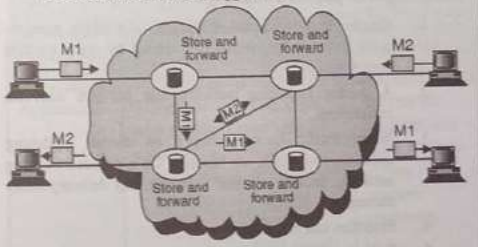
1. The disadvantage of circuit switching is that, since the connection is dedicated it cannot be used to transmit any other data even if the channel is free.
2. Dedicated channels require more bandwidth.
3. It takes long time to establish connection.

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.

2.7.3 Telegraph networks and message switching :

- In telegraphy the text message is encoded using the Morse code into sequences of dots and dashes. Each dot or dash is communicated by transmitting short and long pulses of electrical current over a copper wire.



(L-620) **Fig. 2.7.4 : Message switching**

- In telegraph networks the text message is transmitted from the source telegraph office to the telegraph switching station. At this switching station an operator takes the decision of routing the message based on the destination address information. The operator will either forward the message if a communication line to the destination is free or store the message still the communication line becomes free.
- Message switching does not establish a dedicated path between two communicating devices. In message switching, each message is treated as an independent unit and includes its own destination and source address.
- Each complete message is then transmitted from device to device through the internetwork as shown in Fig. 2.7.4.
- Each intermediate device receives the message, stores it, until the next device is ready to receive it and then forwards it to the next device. For this reason, a message switching network is sometimes called as a store and forward network.
- Messages switches can be programmed with information about the most efficient routes as well as information regarding neighbouring switches that can be used to forward messages to their ultimate destination.

Advantages :

1. It provides efficient traffic management by assigning priorities to the messages to be switched.
2. It reduces network traffic congestion because it is able to store message until a communication channel becomes available.
3. With message switching, the network devices share the data channels.
4. It provides asynchronous communication across time zones.

Disadvantages :

1. The storing and forwarding introduces delay hence cannot be used for real time applications like voice and video.
2. The intermediate devices require a large storing capacity since it has to store the message unless a free path is available.

2.7.4 Packet Switching :

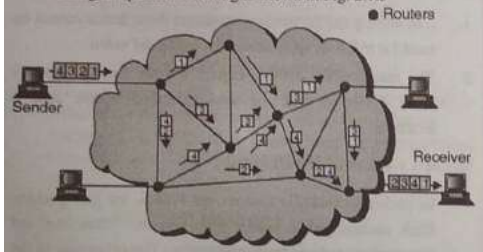
- In packet switching, messages are broken up into packets. Each packets has a header with source, destination and intermediate node address information. The other part of the packet includes data load.
- Individual packets can take different routes to reach the destination. Independent routing of packets 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.

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.

Scanned by CamScanner

- 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. 2.7.5

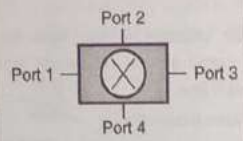


(L-623) **Fig. 2.7.5 : Datagram packet switching**

- 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. 2.7.5 may travel different paths to reach the destination. Due to this the packets may arrive out of order at the destination.
- The delay associated with each packet will be different as a result of the different paths followed by them. The datagrams may get lost 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.

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 are 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. 2.7.6.



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

(L-624) **Fig. 2.7.6 : 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. 2.7.6, if the destination address on the received packet is 4360 then it will be forwarded through port 2.

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.

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.

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.

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.

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.

2.7.5 Comparison of Message, Circuit and Packet Switching : MU : May 17

University Questions

Q. 1 Compare circuit switched and packet switched networks. **(May 17, 5 Marks)**

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

2.8 Network Models :

- This chapter is the base for the remaining book. In this chapter the idea of network model has been discussed first and then the TCP/IP protocol suite has been discussed in detail.
- In order to define the computer network operations, two models have been derived. They are as follows :
  1. TCP/IP protocol suite. 2. OSI model.
- The International Standards Organisation (ISO) covers all aspects of network communication in the Open Systems Interconnection (OSI) model.
- An OSI model is a layered framework for the design of network systems that allows for communication across all types of computer systems.
- The purpose of each layer is to offer certain services to the higher layers.
- Layer n on one machine (source) will communicate with layer n on another machine (destination).
- The rules and conventions used in this communication are collectively known as the layer n protocol.
- Basically a protocol is an agreement between the two communicating machines about how the communication link should be established, maintained and released.

2.9 Protocol Layering :

Protocol :

A protocol in data communication and networking is designed to define certain rules which are to be followed by both sender and the receiver and all the intermediate devices, so as to make the communication effective.

Protocol layering :

- For a simple type of communication, we need to use only one simple protocol.
- However for a complex type of communication, we need to divide the tasks among various layers. At each layer we need to use a protocol to carry out a specific task. This is known as **protocol layering.**

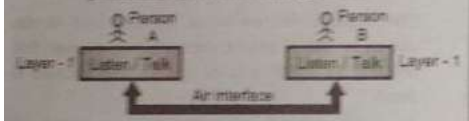
Scanned by CamScanner

2.9.1 Scenarios :

Need of protocol layering :

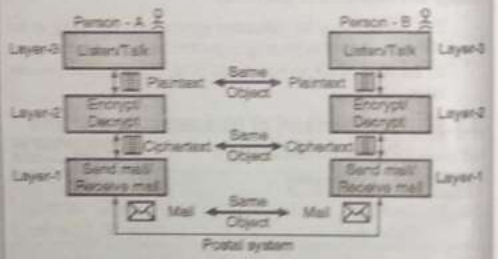
In order to understand the need of protocol layering, let us develop two simple scenarios as follows :

1. **First scenario :**
   - In the first scenario, the communication between the source and destination is very very simple. Therefore only **one layer** will be sufficient to carry it out successfully.
   - Assume that A and B are neighbours staying next to each other in the same building. They speak the same language and can talk face to face very easily and frequently.
   - Therefore the communication between A and B can take place in one layer as shown in Fig. 2.9.1(a).



(G-2062) **Fig. 2.9.1(a) : A single layer protocol**

   - Even in the simple single layer scenario, a set of rules must be followed. The set of rules which should be followed by both A and B are as follows :
     1. Both A and B should greet each other.
     2. They must choose proper words for communication.
     3. If A is speaking, B should remain silent and listen to A and vice versa.
     4. Both know that the communication should be bidirectional (dialog) and not unidirectional (monolog).
     5. They should say goodbye while leaving.
2. **Second scenario :**
   - Now let us discuss the second scenario, in which person A has been offered a high-level position in his company and therefore he needs to relocate himself to company's another branch which is located in a city which is far away from person B.
   - But A and B being very good friends wish to continue their communication about an innovative project to start a new business after their retirement.
   - They choose the conventional mail through post office as their way of communication. But they do not want to reveal their ideas to anyone in case their mails are intercepted. Therefore both of them agree upon using the technique of **encryption and decryption.**
   - Thus the sender encrypts the letter so that any intruder won't be able to read and understand the contents of the letter.
   - Only the receiver knows how to decrypt it. So he will decrypt the received letter and understand its contents.
   - From this discussion we conclude that the communication between A and B takes place in three layers as shown in Fig. 2.9.1(b). Let us assume that both persons A and B have three different machines or robots to perform the tasks specified at each layer.
   - Refer Fig. 2.9.1(b) and imagine that person A sends the first letter to B. For this A talks to the robot at layer-3 as if it is person B.
   - The layer-3 robot (or machine) listens to what A says and converts it into the **plaintext** i.e. a letter written in English. This letter is then sent to the robot or machine present at layer-2.
   - This **plaintext** is encrypted by the machine at layer-2 to create the **ciphertext** which is sent to the machine present at layer-1.
   - The robot/machine present at layer-1 will take the ciphertext, puts it in an envelope, write the addresses of sender and receiver over it and mails the envelope.



(G-2063) **Fig. 2.9.1(b) : A three layer protocol**

   - At **person B's place,** the letter from the mailbox is picked up by the robot/machine at layer-1, the letter in the **ciphertext** is taken out of the envelope and gives it to the machine/robot at layer-2.
   - The machine at layer-2, decrypts the ciphertext to obtain the **plaintext** and hands it over to the machine at layer-3.
   - Finally the machine/robot present at layer-3 reads the plaintext as if person A is talking to person B.

Advantages of protocol layering :

1. It allows us to divide a complex task into many simpler tasks.
2. It allows us to separate the services from the implementation.
3. In practice, the communication does not always take place directly between the two end systems (A and B) but there are intermediate systems which need only some layers. Without the protocol layering the intermediate systems will be as complex as the two end system, thus making the entire system very complex and expensive.

4. It simplifies the design process as the function of each layer is well defined.
5. It provides flexibility to modify and develop network services.
6. Addition of new services and management of network infrastructure becomes easy.

Disadvantages of protocol layering :

1. We lose the touch with reality.
2. Sometimes the protocol layering can result in poor performance of protocol.

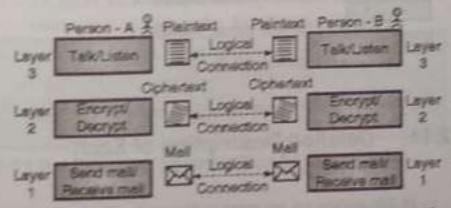
2.9.2 Principles of Protocol Layering :

There are two different principles of protocol layering. We will discuss them one by one.

1. **First principle :**
   - According to the first principle, in order to have a successful bidirectional communication, each layer should be able to perform two opposite tasks one in each direction.
   - For example layer-1 performs send and receive mail functions or layer-2 performs the encryption and decryption and so on.
2. **Second principle :**
   - According to the second principle, in protocol layering the two objects under each layer at both the ends should be the same.
   - For example in Fig. 2.9.1(b), the object under the second layer at A as well as B is cipher text.

2.9.3 Logical Connections :

- We can think of the logical connection between each layer as shown in Fig. 2.9.2. This is after following the two principles of protocol layering.
- Fig. 2.9.2 shows that there is a logical (imaginary) connection from a layer at A to the corresponding layer at B.
- The logical connection between each layer implies that there is a layer to layer communication.
- Due to logical connections, persons A and B can think that it is possible to send the object created from layer to the corresponding layer at the other end.



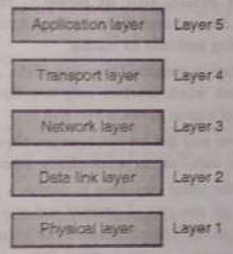
(G-2064) **Fig. 2.9.2 : Concept of logical connections between the peer layers**

2.10 TCP/IP Protocol Suite : MU : May 14

University Questions

Q. 1 What are the goals of TCP/IP model ? **(May 14, 5 Marks)**

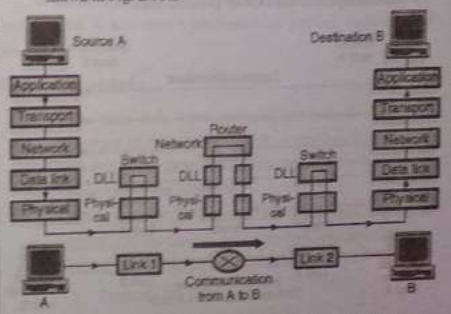
- After discussing about the concept of protocol layering and about the logical communication taking place between layers, now it is time to introduce the **TCP/IP protocol suite.**
- TCP/IP is the short form of two important protocols namely Transmission Control Protocol/Internet Protocol.
- A **protocol 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. 2.10.1.



(G-2065) **Fig. 2.10.1 : Layers in TCP/IP protocol suite**

2.10.1 Layered Architecture :

- In order to understand how the communication takes place between various layers of TCP/IP protocol suite, we have considered a small internetwork consisting of three LANs (links) with all LANs connected to each other via a router as shown in Fig. 2.10.2.



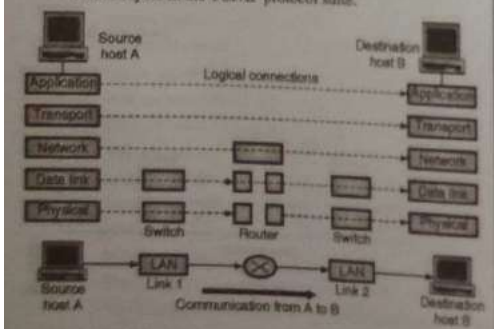
(G-2176) **Fig. 2.10.2 : Communication through an Internet**

Scanned by CamScanner

- In Fig. 2.10.2, 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. 2.10.2.
- 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. 2.10.2 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. 2.10.2.
- 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. 2.10.2 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.

2.10.2 Layers in the TCP/IP Protocol Suite :

- Now we are going to discuss the functions and duties of various layers in the TCP/IP protocol suite.



(G-2177) **Fig. 2.10.3 : Logical connections between the layers of TCP/IP suite**

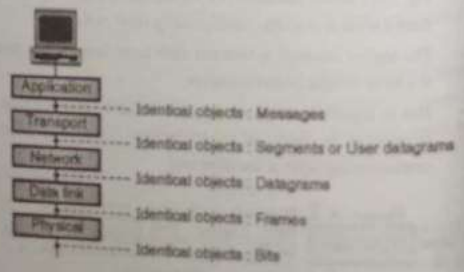
- In this section, we will think about the logical connections between various layers, so as to clearly understand the duties of each layer.
- The logical connections in a simple internetwork have been shown in Fig. 2.10.3.
- Each layer has some specific duties and we can use the logical connections to think about them easily.
- From Fig. 2.10.3 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.
- However the data unit created at the lower two levels can be changed only by the router. The link layer switches cannot modify it.
- The second principle that we discussed for the protocol layering has been shown in Fig. 2.10.4. Note that the objects shown below each layer related to each device are identical.



(G-2178) **Fig. 2.10.4 : Identical objects in the TCP/IP suite**

2.11 Detailed Description of Each Layer :

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

2.11.1 Detailed Introduction to Physical Layer :

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

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.

2.11.2 Detailed Introduction to Data Link Layer :

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

Following are the functions of data link layer :

1. **Framing :**

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

2. **Flow control :**

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

3. **Physical addressing :**

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

4. **Error control :**

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

5. **Access control :**

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

Scanned by CamScanner

11.3 Detailed Introduction to Network Layer :

The primary responsibility of the network layer is to create a connection between the source and destination computers. The communication at the network layer level is called as host to host communication.

The several routers present between the source and destination hosts choose the best route for each travelling packet.

Therefore the two responsibilities of the network layer are : host to host communication and routing of the packet through the possible routers.

The main protocol in the network layer of the Internet is IP (Internet Protocol). The format of the packet (datagram) at network layer is decided by IP.

The routing of datagrams from their source to destination is also the responsibility of IP. It achieves this by making each router forward the datagrams to the next router in its path towards the destination.

IP is a **connectionless** protocol. It does not provide services like **flow control, error control** or even the **congestion control.**

Therefore it is dependent on the transport layer in case if an application needs these services.

The routing protocols included in the network layer are of unicast (one-to-one) and multicast (one-to-many) nature.

These routing protocols have a responsibility of creating the forwarding tables for the routers to help them in the process of routing.

There are some auxiliary protocols at the network layer, that are designed to assist IP in its delivery and routing tasks. The examples of such protocols are ICMP, IGMP, DHCP, ARP etc.

The functioning of these protocols is as follows :

. 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.

unctions of the network layer :

It translates logical network address into physical machine addresses i.e. the numbers used as destination IDs in the physical network cards.

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.

It breaks the larger packets into smaller packets if the packet is larger than the largest data frame the data link will accept.

4. It is concerned with the circuit, message or packet switching.
5. It provides connection oriented services, including network layer flow control, network layer error control and packet sequence control.
6. Routers and gateways operate in the network layer.

2.11.4 Detailed Introduction to Transport Layer :

- The primary responsibility of the transport layer is also to provide an end to end connection.
- At the source host, the application layer sends a message to the transport layer which **encapsulates** it into a transport layer packet (which is also called as a **segment** or **user datagram**) and sends it through the logical connection (which is imaginary) to the transport layer of the destination host.
- In short the transport layer takes message from the application layer of source host and via the transport layer at the destination host delivers the message to the application layer at the destination.
- For the Internet applications, there are number of transport layer protocols designed to give specific service to various application programs.
- The main protocol in the transport layer is TCP (Transmission Control Protocol) which is a connection oriented protocol.
- The main task of TCP is to establish a logical connection between the transport layers of the source and destination hosts before actually transferring the data.
- Being connection oriented, the TCP is a reliable protocol which provides the following services to an application layer program :
  1. Flow control 2. Error control and
  3. Congestion control
- The other commonly used transport layer protocol is UDP (User Datagram Protocol). 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.

2.11.5 Detailed Introduction to Application Layer :

- The logical connection between the application layers of source and destination hosts is **end-to-end** type.
- The communication between the application layers of source and destination hosts takes place through all the layers.
- The application layer communication is between **two processes.** A process is nothing but a program running at the application layer.
- Thus the primary responsibility of the application layer is the **process to process communication.**
- There are many predefined protocols at the application layer in the Internet. Some of these protocols are HTTP, WWW, SMTP, FTP, TELNET, SNMP etc. These protocols and their functions are shown in Table 2.11.1.

Table 2.11.1

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 :

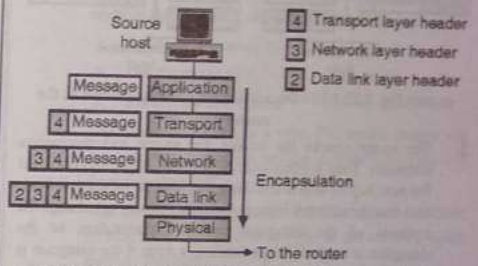
1. The application layer allows the creation of a virtual terminal which is the software version of a physical terminal. The user can log on to the remote host due to this arrangement.
2. The application layer provides File Transfer Access and Management (FTAM) which allows a user to access, retrieve,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

2.12 Encapsulation and Decapsulation :

- The encapsulation / decapsulation is one of the most important concepts in the protocol layering in Internet.
- This concept applied to a small Internet has been illustrated in Fig. 2.12.1.
- In this figure, the layers of data link switches have not been shown because encapsulation or decapsulation does not take place in the data link layer switches.
- In Fig. 2.12.1, the encapsulation takes place at the source host, decapsulation takes place at the destination host while both encapsulation and decapsulation takes place at the router.

2.12.1 Encapsulation at the Source Host :

Refer Fig. 2.12.1(a) to understand the process of encapsulation at the source host.



(G-2066) **Fig. 2.12.1(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. 2.12.1(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.

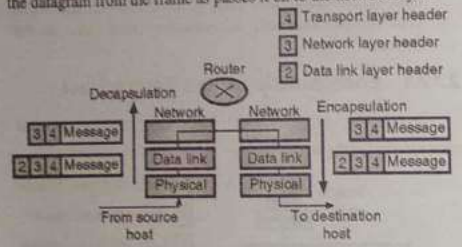
Scanned by CamScanner

2.12.2 Decapsulation and Encapsulation at the Router :

Refer Fig. 2.12.1(b) which illustrates the processes of decapsulation and then encapsulation occurring at a router connected to two or more links.

1. Decapsulation :

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

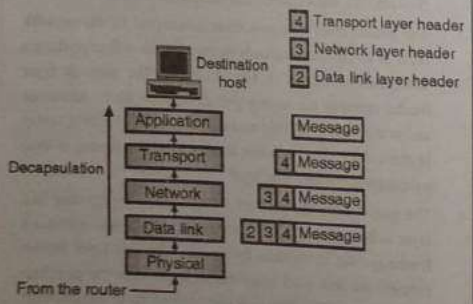


(G-2067) **Fig. 2.12.1(b) : Decapsulation / Encapsulation at the router**

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.

2.12.3 Decapsulation at the Destination Host :

- At the destination host, only the decapsulation process is carried out at each layer, as shown in Fig. 2.12.1(c).



(G-2068) **Fig. 2.12.1(c) : Decapsulation at the destination host**

- At each layer, the payload is removed from the packet and the payload is delivered to the higher layer, by removing the headers at each stage.
- Finally after removing all the headers, the message is delivered to the application layer.
- It is important to note that the **error checking** is involved in the process of decapsulation at the destination host.

2.13 Addressing :

- 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. 2.13.1 shows the addressing at each layer.

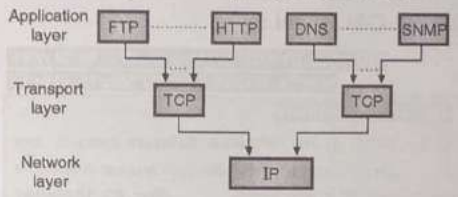
Packet name	Layers	Address
Message	Application	Names
Segment/User datagram	Transport	Port numbers
Datagram	Network	Logical addresses
Frame	Data link	Link layer addresses
Bits	Physical	No address needed

(G-2069) **Fig. 2.13.1 : Addressing in TCP/IP protocol suite**

- Fig. 2.13.1 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.

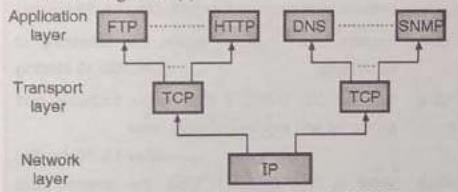
2.14 Multiplexing and Demultiplexing :

- In TCP/IP protocol, many protocols are being used at the same layer. Therefore multiplexing is needed at the source and demultiplexing is needed at the destination.
- In the process of **multiplexing** as shown in Fig. 2.14.1(a), a protocol at one layer in TCP/IP can encapsulate a packet (one at a time) from several protocols corresponding to the next higher layer in TCP/IP suite.



(G-2070) **Fig. 2.14.1(a) : Multiplexing in TCP/IP**

- In the process of demultiplexing, a protocol will decapsulate and deliver a packet one at a time to several protocols belonging to the next higher layer in TCP/IP protocol suite as shown in Fig. 2.14.1(b).



(G-2071) **Fig. 2.14.1(b) : Demultiplexing in TCP/IP**

- As shown in Fig. 2.14.1(a), at the transport layer two protocols TCP and UDP are capable of multiplexing the messages coming from various protocols at the application layer.
- Next the segments from TCP or user datagrams from UDP are accepted and multiplexed by IP at the network layer.
- IP can also multiplex the packets from some other protocols such as ICMP or IGMP etc.
- The frames at the data link layer level can carry the payload coming from the network layer protocols such as IP or ARP etc.

2.15 Connection Oriented and Connectionless Services :

MU : Dec. 03, May 04, Dec. 09, May 14

University Questions

Q. 1 Write advantages and disadvantages of connection oriented service with connectionless 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)**

Q. 3 Compare connection oriented and connectionless network. **(Dec. 09, 5 Marks)**

Q. 4 Write short notes on : Connection oriented and connectionless service. **(May 14, 5 Marks)**

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

1. Connection oriented service :

- 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.

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.

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.

Scanned by CamScanner

- 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 2.15.1 lists various types of services and their examples.

Table 2.15.1 : 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.

2.16 Relationship of Services to Protocols :

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

2.16.1 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.

2.16.2 Protocol :

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

2.17 OSI Model :

MU : Dec. 03, Dec. 07, May 09, Dec. 09, May 11, May 14, May 15, Dec. 15, May 16, May 17

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, 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 Explain OSI model and compare it with TCP/IP reference model. **(May 09, May 11, 10 Marks)**

Q. 4 Explain OSI reference model and functions of each layer. **(Dec. 09, 10 Marks)**

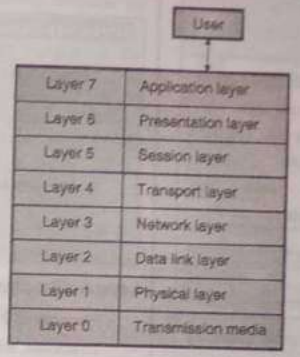
Q. 5 What is OSI model ? Explain the functions and protocols and services of each layer. **(May 14, 10 Marks)**

Q. 6 What is OSI model ? Give the function and services of each layer. **(May 15, Dec. 15, May 16, 10 Marks)**

Q. 7 What is OSI model ? Give the function and services of each layer. **(May 17, 10 Marks)**

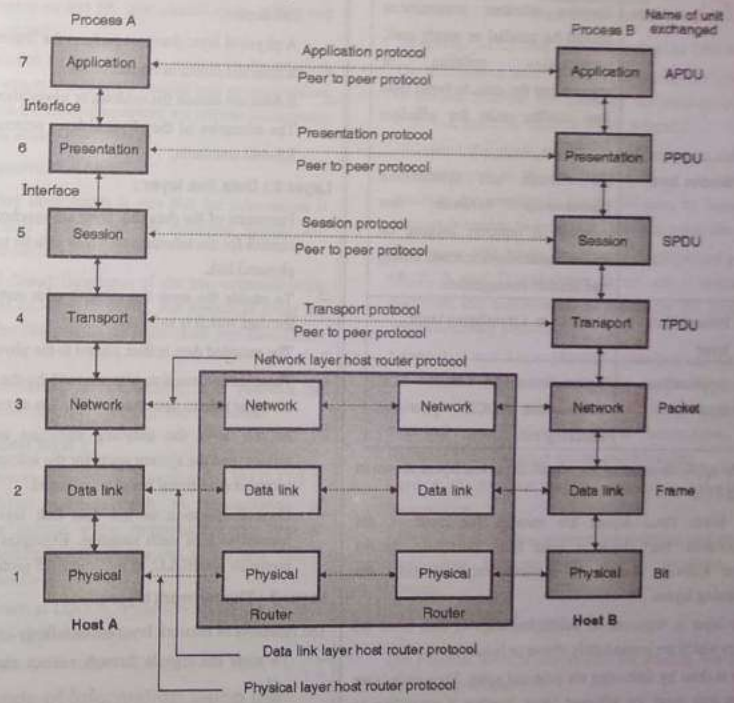
- The users of a computer network are located over a wide physical range i.e. all over the world.
- Therefore to ensure that nationwide and worldwide data communication systems can be developed and are compatible to each other, an international group of standards has been developed.
- These standards 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. 2.17.1 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. 2.17.2.

- The OSI model shown in Fig. 2.17.2 does not contain the physical medium.
- This model is based on a proposal developed by the International Standards Organization (ISO).



(G-59) **Fig. 2.17.1 : A seven layer ISO-OSI reference model**

- It is called as ISO-OSI (Open System Interconnection) reference model because it is designed to deal with open systems i.e. th systems which are open for communication with other systems.



(G-60) **Fig. 2.17.2 : The OSI reference model**

Scanned by CamScanner

– Table 2.17.1 shows various layers and its functions.

Table 2.17.1 : 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. 2.17.2.

– 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.

2.17.1 Functions of Different Layers :

MU : Dec. 09, May 14, May 15, Dec. 15, May 16, May 17

University Questions

Q. 1 Explain OSI reference model and functions of each layer. **(Dec. 09, 10 Marks)**

Q. 2 What is OSI model ? Explain the functions and protocols and services of each layer. **(May 14, 10 Marks)**

Q. 3 What is OSI model ? Give the function and services of each layer. **(May 15, Dec. 15, May 16, 10 Marks)**

Q. 4 What is OSI model ? Give the function and services of each layer. **(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.

– 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. 2.17.2. 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.

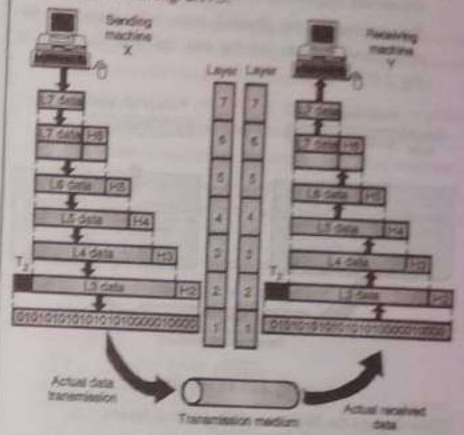
– The functions such as LOGIN, or password checking are also performed by the application layer.

– Let us now go into the details of each and every layer.

2.17.2 Exchange of Information using the OSI Model :

– At the physical layer, communication is direct i.e. machine X sends a stream of bits to machine Y.

– At higher layers, each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it as shown in Fig. 2.17.3.



(G-43) **Fig. 2.17.3 : An exchange using the OSI model**

– The information added by each layer is in the form of headers or trailers. Headers are added to the message at the layers 6, 5, 4, 3, and 2. A trailer is added at layer 2.

– At layer 1 the entire package is converted to a form that can be transferred to the receiving machine. At the receiving machine, the message is unwrapped layer by layer with each process receiving and removing the data meant for it.

– The upper OSI layers are always implemented in software (4, 5, 6 and 7) and lower layers are a combination of hardware and software (2, 3) except for the physical layer which is mostly hardware.

– Layers 1, 2 and 3 (i.e. physical , data link and network) are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical connections, physical addressing and transport timing and reliability.

– Layer 4, the transport layer ensures end to end reliable data transmission.

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

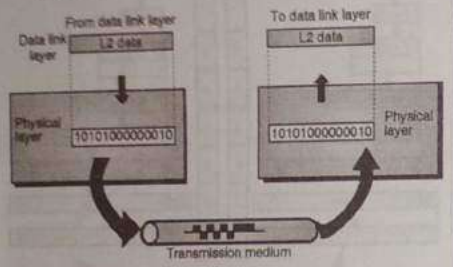
2.17.3 Physical Layer :

– 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.

Scanned by CamScanner

- The physical layer is used to define physical and electrical details such as what will represent a 1 or a 0, how many pins a network will have, how data will be synchronized and when the network adapter may or may not transmit the data.
- The position of the physical layer with respect to the transmission medium and the data link layer is shown in Fig. 2.17.4.



(G-62) **Fig. 2.17.4 : Physical layer**

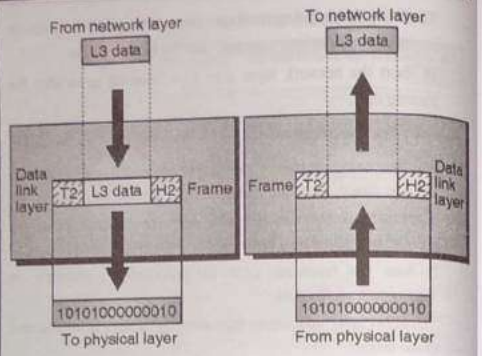
Following are the functions of the physical layer :

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.

2.17.4 Data Link Layer :

- It is responsible for reliable node to node delivery of the data. It accepts packets from the network layer and forms frames and gives it to the physical layer as shown in Fig. 2.17.5.



(G-63) **Fig. 2.17.5 : Data link layer**

Following are the functions of data link layer :

1. **Framing :**

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

2. **Flow control :**

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

3. **Physical addressing :**

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

4. **Error control :**

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

5. **Access control :**

   - The data link layer protocol 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 :

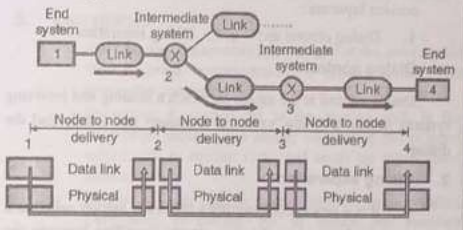
   1. **Logical Link Control (LLC) :**

      It establishes and maintains links between the communicating devices.

   2. **Media Access Control (MAC) :**

   - It controls the way multiple devices share the same media channel.
   - The logical link control sub-layer provides Service Access Points (SAPs) that the other computers can refer to and use to transfer information from LLC to the network layer.

- The MAC sub-layer provides for shared access to the network adapter and communicates directly with the network interface cards.
- Network Interface Cards (NIC) have a unique 12-digit hexadecimal MAC address assigned before they leave the factory where they are manufactured.
- The MAC addresses are used to establish logical link between two computers on the same LAN.
- Bridges, intelligent hubs and network interface cards are devices associated with the data link layer.
- The data link layer is responsible for moving frames from one hop (node) to the next.
- Fig. 2.17.6 shows the node delivery by the data link layer.

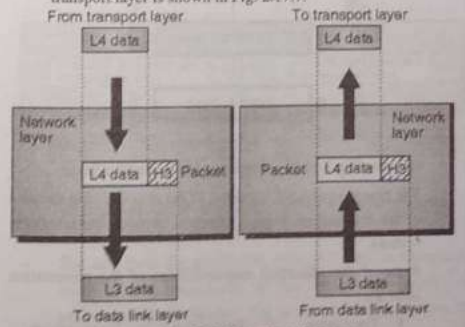


(G-64) **Fig. 2.17.6 : Node to node delivery**

- Fig. 2.17.6 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.

2.17.5 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. 2.17.7.

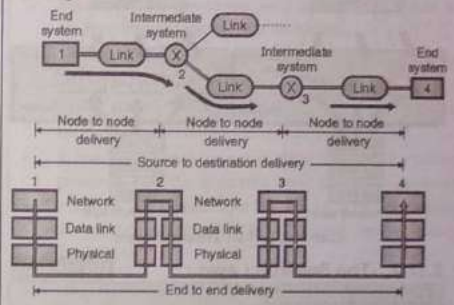


(G-65) **Fig. 2.17.7 : Network layer**

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. 2.17.8.



(G-66) **Fig. 2.17.8**

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

2.17.6 Transport Layer :

- The function of the transport layer is the process to process delivery of the entire message.
- It ensures that the whole message reaches the destination intact and in order, with both error control and flow control incorporated at the source and destination.

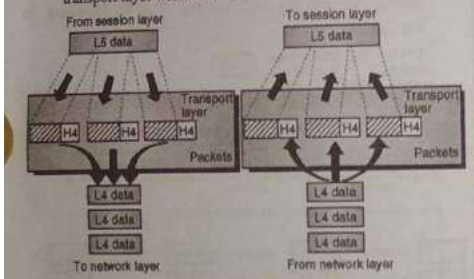
Scanned by CamScanner

- Fig. 2.17.9 shows the relationship of the transport layer to the network layer and session layer.

Functions of transport layer :

The transport layer performs the following functions :

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



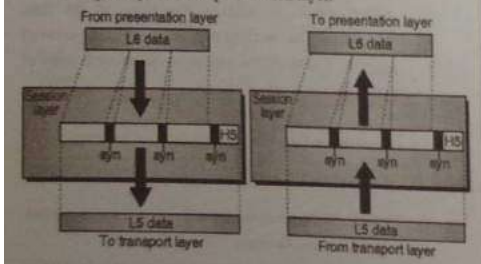
(G-67) **Fig. 2.17.9 : Transport layer**

2.17.7 The Session Layer : MU : May 04

University Questions

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

- The main function of this layer is to establishe, maintain and synchronise the communication between interested systems.
- Fig. 2.17.10 shows the relationship of the session layer to the transport layer and the presentation layer.



(G-68) **Fig. 2.17.10 : 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 :

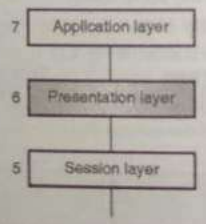
Dialog control is the means by which a sending and receiving systems initiate a dialog, exchange messages and finally end the dialog.

2. Dialog separation :

- It is a process of inserting a reference marker called as a checkpoint into the data stream travelling between the sending and receiving systems.
- This allows the checking of status of both the machines at the same point in time.
- This will avoid any possible confusion and collision situation.

2.17.8 Presentation Layer :

- The presentation layer is the 6th layer the OSI model as shown in Fig. 2.17.11.
- Above it there is the application layer and below it there is the sessions layer.



(G-707) **Fig. 2.17.11 : 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 :

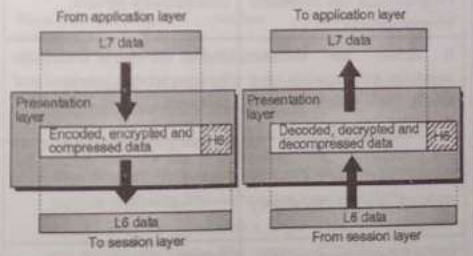
- For ensuring the security and privacy of the information that is being communicated, a process called data encryption is essential.
- Encryption is carried out at the sending end. In the encryption process, the sender transforms the original information to another form, and sends the transformed information.
- 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. 2.17.12.



(G-69) **Fig. 2.17.12 : 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. 2.17.12.
- 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 :

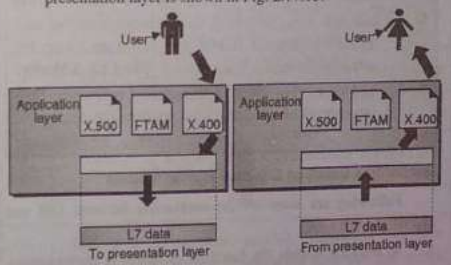
The presentation layer performs the following function :

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.
3. For security and privacy purpose it carries out encryption at the transmitter and decryption at the receiver.
4. It carries out data compression to reduce the bandwidth of the data to be transmitted.

- Unlike the session layer, which provides many different functions, the presentation layer has only one function.
- It basically functions as a pass through device. It receives primitives from the application layer and issues duplicate primitives to the session layer below it, using the Presentation Service Access Point (PSAP) and Session Service Access Point (SSAP).

2.17.9 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. 2.17.13.



(G-70) **Fig. 2.17.13 : Application layer**

Scanned by CamScanner

The application layer performs the following functions :

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

2.17.10 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.

2.17.11 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.

2.18 Comparison of OSI and TCP/IP Models :

MU : May 04, Dec. 07, May 09, May 10, May 11, May 13

University Questions

Q. 1 List two ways in which the OSI reference model and TCP/IP reference model are the same and two ways in which they are different ? **(May 04, 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 Explain OSI model and compare it with TCP/IP reference model. **(May 09, May 11, 10 Marks)**

Q. 4 List two ways in which OSI reference model and TCP/IP reference model are same and also list two ways in which they differ ? **(May 10, 5 Marks)**

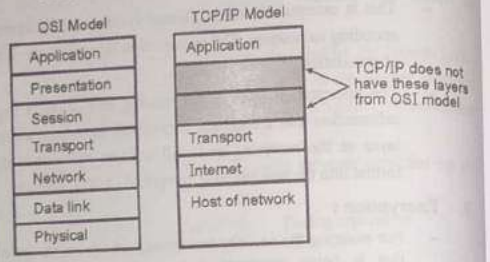
Q. 5 List the five key differences between TCP references model and OSI reference model. **(May 13, 5 Marks)**

Similarities between OSI and TCP/IP Models :

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

1. In both the models the functions of layers is approximately same.
   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 Fig. 2.18.1 and Table 2.18.1 for the comparison of the two reference models.



(G-73) **Fig. 2.18.1 : Relationship between OSI and TCP/IP models**

Table 2.18.1 : 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 connectionless 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.

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.

Hybrid (Internet) reference model :

– Inspite of many problems associated with the OSI model, it has proved to be very useful one practically.
– But the OSI protocols have not become popular.
– On the other hand the TCP/IP model is practically non existing but the TCP/IP protocols are used widely.
– So sometimes a modified OSI model with primary concentration on TCP/IP is used which is called as the hybrid model.
– The hybrid model is shown in Fig. 2.18.2. It is also called as the Internet model.

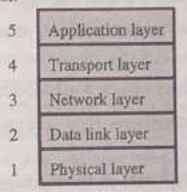
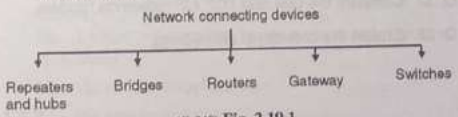


Fig. 2.18.2 : Hybrid model

2.19 Network Connecting Devices :

– Different types of network connecting devices are as shown in Fig. 2.19.1.

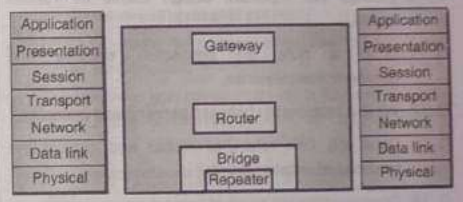


(G-348) **Fig. 2.19.1**

– The relation between OSI reference model and various connecting devices is shown in Fig. 2.19.2.

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. 2.19.2.



(G-896(a)) **Fig. 2.19.2 : Connecting devices and OSI model**

Categories of connecting devices :

Fig. 2.19.2 shows the relationship between the connecting devices and various layers of the internet model.

Table 2.19.1 : 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.

Scanned by CamScanner

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.

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.

□□□

CHAPTER 3

Module II

Application Layer

Syllabus :

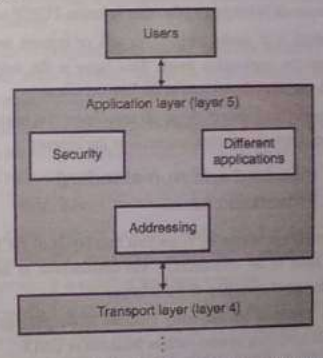
Introduction, Providing services, Application layer paradigm, Client-server paradigm : Application programming interface, Using services of transport layer, Standard client server applications : World wide web and HTTP, FTP, Electronic mail, Telnet, Secure shell (SSH) and Domain Name System (DNS).

3.1 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.

3.1.1 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. 3.1.1 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. 3.1.1 : 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.

Scanned by CamScanner

- 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.

3.2 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.

3.2.1 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.

3.2.2 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.

3.2.3 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.

3.3 Application Layer Paradigms :

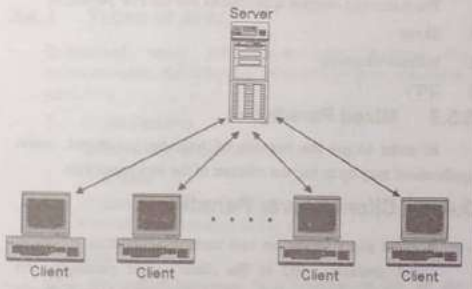
During the life time of the Internet, two different paradigms have been developed. They are as follows :

1. Client-server paradigm.
2. Peer to peer paradigm.

3.3.1 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 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. 3.3.1 shows client-server network relationship. The server provides security and administration of the network.



(G-41) **Fig. 3.3.1 : 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.

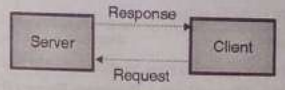
Server :

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



(G-42) **Fig. 3.3.2 : Client/server communication**

- The server responds to this request and sends the signal accordingly to the client as shown in Fig. 3.3.2.
- 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.

Scanned by CamScanner

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.

plications :

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. email

Some of these protocols have been discussed in this chapter.

.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.

f the file requested by a client to server is a large file such as music or video file, then it puts a lot of load on the server machine.

n such situations the **P2P** paradigm becomes attractive. The 2P paradigm is also attractive in a situation in which two eers want to exchange files without involving the server.

owever it should be noted that the **P2P** paradigm does not nore the client-server paradigm completely. Instead the P2P lows some users to share the duty of the server.

stead of sharing of a big file using client-server connection, P2P paradigm will let the server download a part of that e and then share it among themselves.

us in P2P paradigm the same computer has to sometimes ave like a client and at some other time like a server.

other words, the same computer will be a client for some lications for certain amount of time and server at other es. However such applications are not a part of the rnet, 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.

3.3.3 Mixed Paradigm :

In order to get the benefits of both the paradigms, some applications may try to use the mixture of the two paradigms.

3.4 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.**

3.4.1 Application Programming Interface (API) :

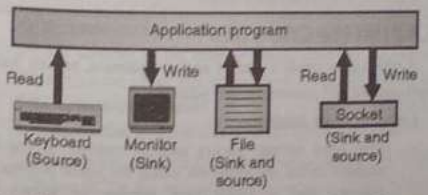
- We need to now understand that how a client process communicates with a server process.
- A client process is basically a computer program which like any other program, written in a computer language but with certain additional instructions.
- These new or additional set of instructions makes the client 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.

3.4.2 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 ?

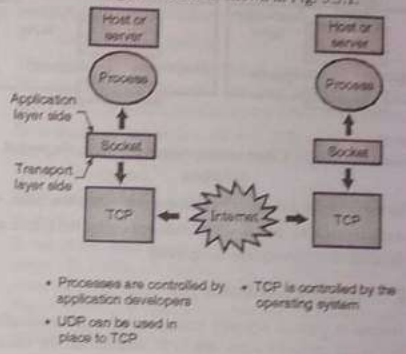
- With the **socket interface**, it is possible to use all the instructions that can read and write data in the programming languages like C, C++ and Java.
- All these preexisting instructions can be used to read and write data from the **sockets.**
- Thus **socket** is new source or sink of data which 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. 3.4.1.



(G-2209) **Fig. 3.4.1 : Sockets are like any other sinks and sources**

3.5 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. 3.5.1.



(G-436) **Fig. 3.5.1 : Socket**

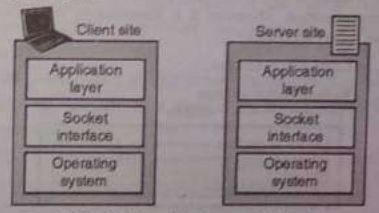
- Thus **socket** is defined as an interface between the application layer and the transport layer within a host.
- It is also called as the Application Programming Interface (API) between the application and the network.
- In Fig. 3.5.1 we have assumed that the transport protocol being used is TCP. But note that UDP can also be used.
- In the Internet, a socket is a software **data structure.**

3.5.1 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. 3.5.2 to understand the conceptual relationship between an operating system and TCP/IP suite.

Definition :

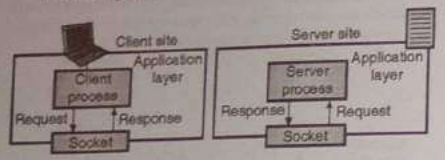
- We may define the **socket interface** as the set of instructions which helps an application access the services provided by the TCP/IP protocol suite. It is located between the application program and operating system.
- A socket is suppose to behave like a file or a terminal but it does not have a physical existence like them. It is basically a **data structure** which is created and used by the application layer program.



(G-2210) **Fig. 3.5.2 : Relation between application layer, socket interface and operating system**

Scanned by CamScanner

- 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. 3.5.3.

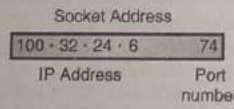


(G-2211) **Fig. 3.5.3 : Client server communication via socket interface**

- 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.

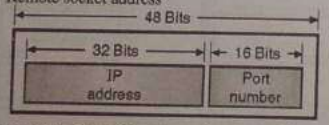
3.5.2 Socket Address :

- 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.
- The combination of IP address and port number is as shown in Fig. 3.5.4 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. 3.5.4 : 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. 3.5.5 : Structure of socket address**

3.5.3 Finding Socket Addresses :

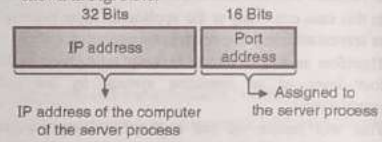
- Let us discuss now about how a client or a server find the two socket addresses mentioned above.
- The situation at the client site is completely different than that at the server site.
- Therefore we will consider them separately.

3.5.3.1 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. 3.5.6.



(G-2213) **Fig. 3.5.6 : 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.

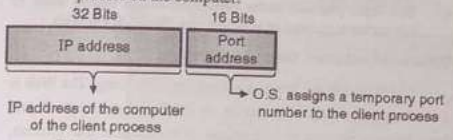
3.5.3.2 At the Client Site :

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. 3.5.7.

- 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. 3.5.7 : 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.

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.

3.6 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.

3.6.1 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.

3.6.2 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.

Scanned by CamScanner

3.6.3 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.

3.7 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
- 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.

3.8 World Wide Web (WWW) :

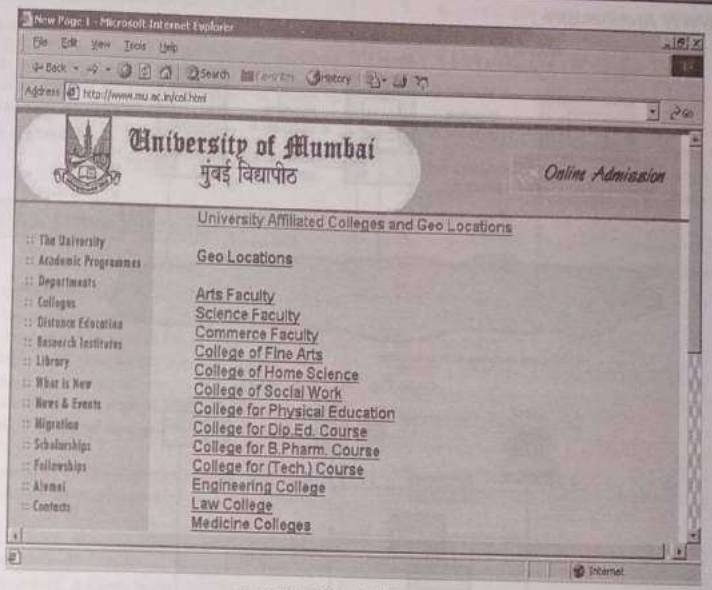
- People have become aware of the power of Internet through WWW. HTTP is a file transfer protocol which is specifically designed to facilitate access to the WWW.
- The World Wide Web is an architectural framework for accessing documents which are spread out over a number of machines over Internet.
- 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.

3.8.1 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. 3.8.1.
- 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.
-



(G-653) **Fig. 3.8.1 : 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 :

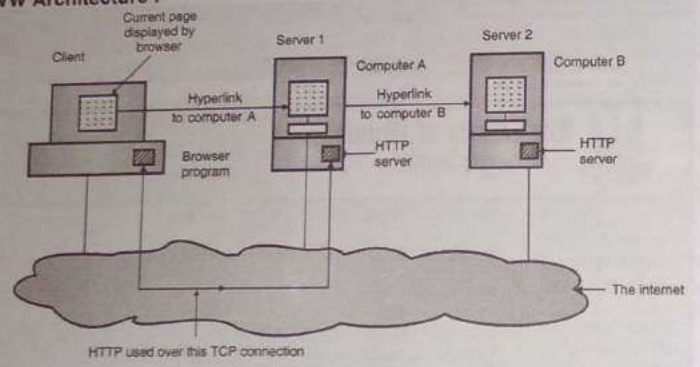
- All pages may not be viewable in the conventional way because some pages may contain audio tracks, video clips or both.
- If the hypertext pages are mixed with other media, the result of such a mixing is called as hypermedia.
- Some browsers are capable of displaying all kinds of hypermedia but others 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.

3.8.2 Web from the Servers Side :

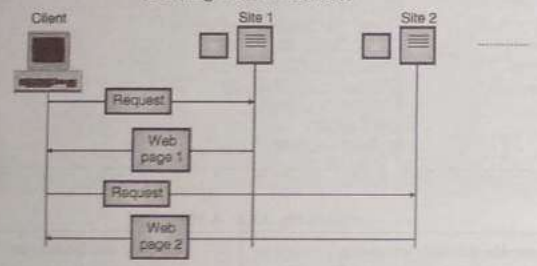
- Every website has a server process. It is listening to TCP port 80 on which incoming clients (browsers) are connected.
- Once a connection is established, the client sends a request and the server sends a reply for that. Then the connection is released.
- The protocol used for defining the legal request and replies is called HTTP.
- Fig. 3.8.2 shows various parts of the web model.

Scanned by CamScanner

3.8.3 WWW Architecture :



(G-654) Fig. 3.8.2 : Web model

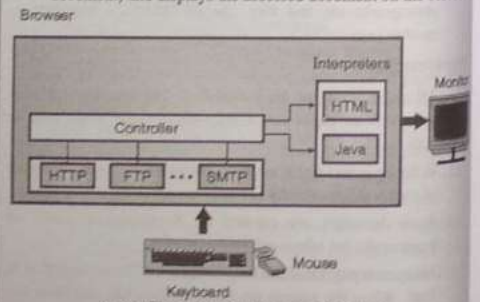


(G-655) Fig. 3.8.3 : WWW architecture

- 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. 3.8.3 shows the architecture of WWW.
- As shown in Fig. 3.8.3, 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.

3.8.4 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. 3.8.4 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.



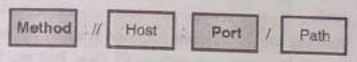
(G-445) Fig. 3.8.4 : Browser architecture

3.8.5 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.

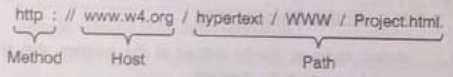
3.8.6 Uniform Resource Locator (URL) :

- 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. 3.8.5(a). They are as follows :
  1. Method or protocol
  2. Host computer
  3. Port
  4. Path.



(G-660) Fig. 3.8.5(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. 3.8.5(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. 3.8.5(b). Note that the port is not included.



(G-1969) Fig. 3.8.5(b) : Example of URL

3.8.7 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.

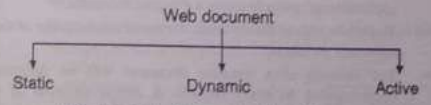
  For example the header line can be :

  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.

3.9 Web Documents :

- The web documents can be classified into three categories as shown in Fig. 3.9.1.



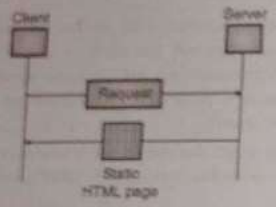
(G-668) Fig. 3.9.1 : Categories of web documents

3.9.1 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.

Scanned by CamScanner

- 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. 3.9.2.



(G-669) Fig. 3.9.2 : Static document

3.9.2 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.

3.9.3 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. 3.9.3 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.

3.9.4 Common Gateway Interface (CGI) :

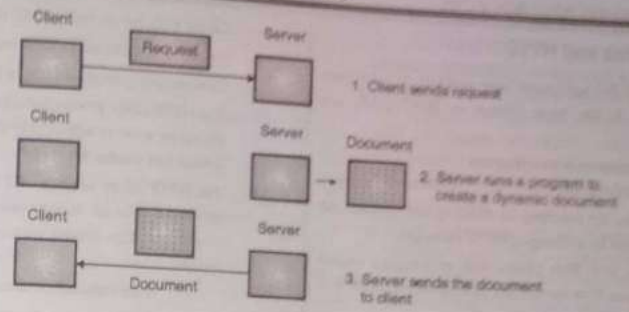
- CGI is the name of a technology which creates the dynamic documents and handles them too.
- CGI is in fact a set of standards. It defines the way in which a dynamic document should be written, the way in which input data be supplied to the program and how the output result be used.
- Note that CGI 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 :

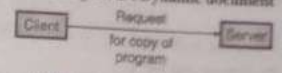
It is a code which is written in one of the languages that supports CGI (such as C, C ++, etc.).

3.9.5 Active Documents :

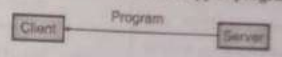
- Active document can be defined as the program, that is needed to be run at the client side.
- The examples of active documents are the programs creating animated graphics on the screen or the ones which help interaction with the user.
- Refer Fig. 3.9.4 to understand this concept. It shows that whenever 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.



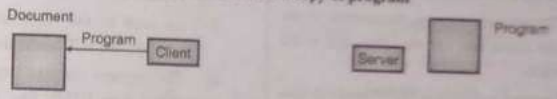
(G-670) Fig. 3.9.3 : Dynamic document



(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. 3.9.4 : Active document

Steps in creation of an active document :

Refer Fig. 3.9.4 to understand the creation, compilation and execution of an active document.

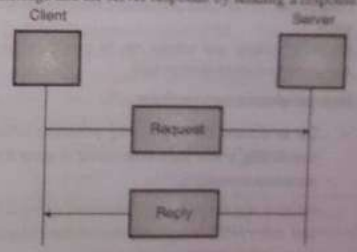
1. At the server, a program is written in source code and stored in a file.
2. Then the program is compiled and binary code is creates and stored in a file at the server's site.
3. A client (browser) requests for a copy of program as shown in Fig. 3.9.4(a). This program is transported from the server 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.

3.10 HTTP(Hypertext Transfer Protocol) :

- 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.

3.10.1 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. 3.10.1 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. 3.10.1 : HTTP transaction

Scanned by CamScanner

3.10.2 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.**

3.10.3 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) :

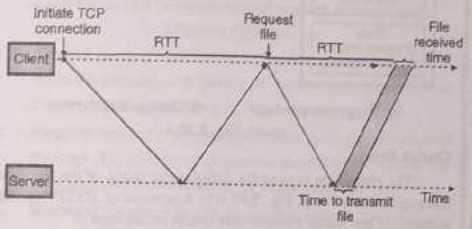
- The RTT is defined as the time taken by a small packet to travel from client to server and then back to the client.

  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. 3.10.2.
  1. The browser initiates a TCP connection between the browser and web server. This process makes use of a **three way handshake.**

  In the three way handshake, the client sends a small TCP segment to the web server. The server acknowledges and responds with another small TCP segment. Finally the client acknowledges back to the server.
  2. After completing the first two parts of the three way handshake the client sends the HTTP request message to the server.
  3. In response the server sends the HTML file to the client. The total response time as shown in Fig. 3.10.2 is equal to 2RTT plus the time taken by the server to transmit the file.



(G-658) **Fig. 3.10.2**

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.

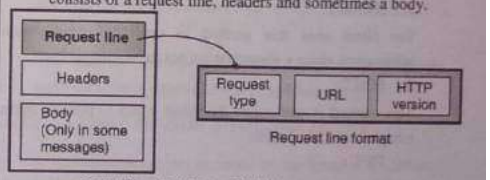
With pipelining only one RTT will be expended for all the referenced objects. Another advantage is that the pipelined TCP connection remains idle for a very short time.

3.10.4 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.

3.10.5 Request Message :

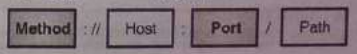
- Fig. 3.10.3(a) shows the format of the request message. It consists of a request line, headers and sometimes a body.



(G-659) **Fig. 3.10.3(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. 3.10.3(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. 3.10.3(b). They are as follows :
  1. Method 2. Host computer
  3. Port 4. Path.



(G-660) **Fig. 3.10.3(b) : URL**

Scanned by CamScanner

- Method is the protocol used such as FTP, HTTP. Host is the computer where the required information is located. The name of the computer begins with www but this is not mandatory.
- URL can optionally contain the server's port number. If the port is included then it should be inserted between host and path and it should be separated by a colon.
- Path is the name of the file where the information is located.
- **Version :** The latest version of HTTP is 1.1 but the versions 0.9 and 1 are also used.

The example of URL is shown in Fig. 3.10.3(c).

http : // www.w4.org / hypertext / WWW / Project.html.

Method Host Path

Fig. 3.10.3(c) : Example of URL

3.10.6 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 :

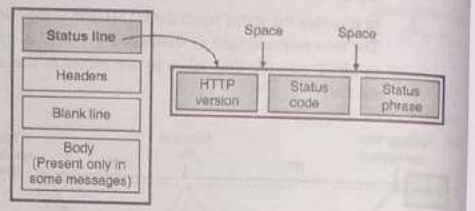
It is used for deleting the links created by the LINK method.

11. OPTION :

It is used by the client to ask the server about various options that are available.

3.10.7 Response Message :

Fig. 3.10.4(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. 3.10.4**

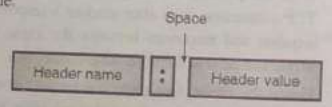
Status line :

The status line is used for defining the status of the response message. As shown in Fig. 3.10.4(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.

3.10.8 Headers :

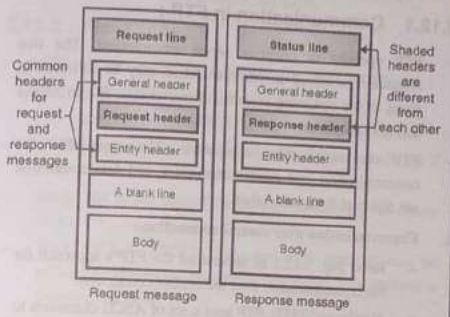
- Headers in the response message are used for exchanging additional information between the client and server.
- The header can be a one liner or multiple lines. The format of a header line is shown in Fig. 3.10.5 which shows that it consists of a header name, a colon, a space and a header value.



(G-663) **Fig. 3.10.5 : 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. 3.10.6. The common headers and different headers have been indicated clearly.

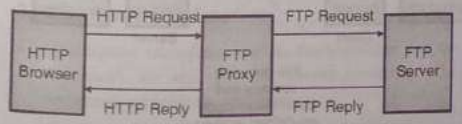


(G-664) **Fig. 3.10.6 : Comparison of request message and response message**

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. 3.10.6.
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. 3.10.6.

3.11 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. 3.11.1.



(G-656) **Fig. 3.11.1 : 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. 3.11.1.
- 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.

3.11.1 HTTP Security :

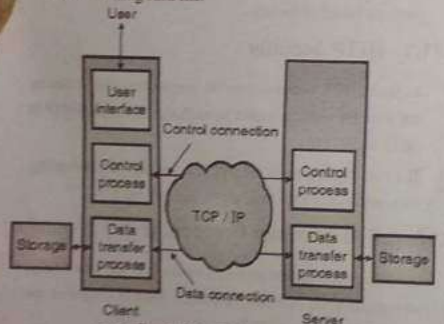
- As such HTTP does not provide any security. But it can be run over the secured socket layer (SSL). If so, the HTTP is called as HTTPS.
- The security features of HTTPS include confidentially, authentication of client and server and data integrity.

3.12 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. 3.12.1.
- 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.

Scanned by CamScanner

- The fact that FTP separates control and data makes it very efficient.
- The control connection uses simple rules of communication. Only one line of command or a line of response is transferred at a time.
- But the data connection uses more complex rules due to the variety of data types being transferred.
- FTP uses port 21 for the control connection and port 20 for the data connection. Both these are well known TCP ports.
- As shown in Fig. 3.12.1 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. 3.12.1.
- 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. 3.12.1 : 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 :

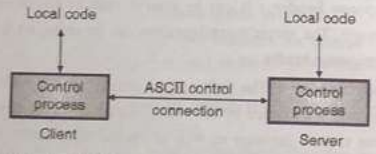
- Data connection uses the port 20 at the server site. This connection is opened when data to be transferred is ready and it is closed when transfer of data is over.
- The data connection does not remain open continuously like control connection. It is opened and closed many times as per requirement.

3.12.1 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 :

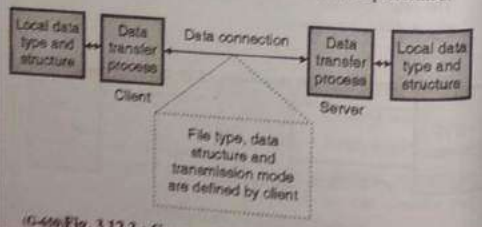
- Refer Fig. 3.12.2 to understand the FTP's approach for the communication over the control connection.
- Similar to SMTP, FTP uses a set of ASCII characters to communicate across the control connection.
- Communication is achieved through a process of commands and response. One command is sent at a 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. 3.12.2 : 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. 3.12.3 : Communication over the data connection

- Refer Fig. 3.12.3 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.

3.12.2 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.
- With ASCII or EBCDIC files one more attribute must be added for defining the printability of the file. This attribute is nonprint or TELNET.

3.12.3 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.

3.12.4 Transmission Mode :

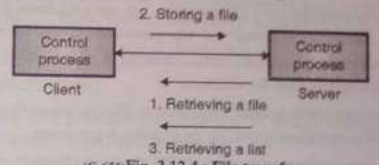
FTP uses one of the following modes to transfer a file :

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.

3.12.5 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. 3.12.4.



(G-651)Fig. 3.12.4 : File transfer

3.12.6 FTP Commands :

- The following commands are used for copying files using FTP.

Table 3.12.1 : 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 3.12.2.

Table 3.12.2 : 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 3.12.3.

Table 3.12.3 : 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.

3.12.7 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.

Scanned by CamScanner

- 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.

3.12.8 Security for FTP :

- In the early days of FTP its security was not a big issue. FTP is password protocol 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.

3.13 Electronic Mail :

- One of the most popular network services is electronic mail (e-mail).
- Simple Mail Transfer Protocol (SMTP) is the standard mechanism for electronic mail in the Internet.
- The first e-mail systems simply consisted by file transfer protocols.
- But some of the limitations of this system were as follows :
  1. It is difficult to send a message to a group of people.
  2. Message did not have any internal structure. So its computer processing was difficult.
  3. The sender never used to know if a message arrived or not.
  4. It was not easy to handover one's e-mails to someone else for the purpose of managing them when one is out of town or country for sometime.
  5. The user interface with the transmission system is poorly integrated.
  6. It was not possible to create and send messages containing a text, drawing, facsimile and voice together.
- So more elaborate e-mail systems were proposed. ARPANET e-mail proposals were published as RFC 821 (transmission protocol) and RFC 822 (message format).
- These are used in Internet.

3.13.1 E-mail Architecture and Services :

- An e-mail system consists of two subsystems :
  1. User agents and 2. Message transfer agents

User agents : They enable users to read and send e-mail.

Message transfer agents : They move the messages from the sender to the receiver.

Basic Functions :

- E-mail systems support five basic systems which are as follows :
  1. Composition 2. Transfer
  3. Reporting 4. Displaying and
  5. Disposition

1. **Composition :**

   The process of creating messages and to answer them is known as composition. The system can also provide assistance with addressing and a number of header fields attached to each message.

2. **Transfer :**
   - It is the process of moving messages from the sender to the recipient.
   - This includes establishment of a connection from sender to destination or some intermediate machine, transferring the message, and breaking the connection.

3. **Reporting :**

   The reporting system is designed to tell the sender about whether the message was delivered or rejected or lost.

4. **Displaying :**

   It is the process of displaying the incoming messages so that it can be read by the user. For this purpose simple conversions and formatting are required to be done.

5. **Disposition :**
   - This is concerned with what the recipient does with the received message. Disposition is the final step in e-mail system.
   - Some of the possibilities are as follows :
     1. Throw after reading
     2. Throw before reading
     3. Save messages
     4. Forward messages
     5. Process messages in some other way.

Advanced features of E-mail systems :

Some of the advanced features included in addition to the basic functions are as follows :

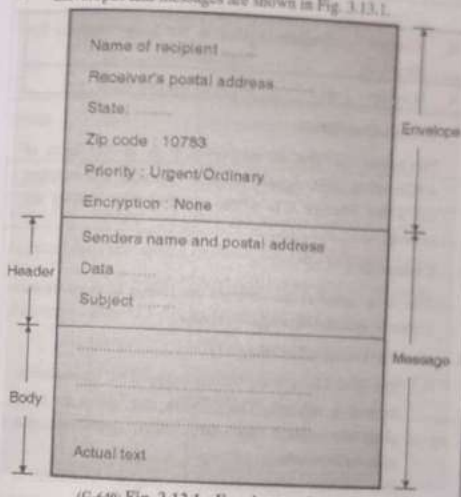
1. Forwarding an e-mail to a person away from his computer.
2. Creating and destroying mailboxes to store incoming e-mail.
3. Inspecting contents of mailbox, insert and delete messages from the mailboxes.
4. Sending a message to a large group of people using the idea of mail list.
5. To provide the facility of registered e-mail.
6. Automatic notification of undelivered e-mails.
7. Carbon copies.
8. High priority e-mail (setting the priority of e-mails).
9. Secret (encrypted e-mail).
10. Alternative recipient. This allows automatic forwarding of an e-mail to an alternate recipient if the main recipient is not available.

E-mail Envelope :

- In the modern e-mail systems, there is a distinction made between the e-mail and its contents.
- An e-mail envelope contains the message, destination address, priority, security level etc.
- The message transport agents such as SMTP use this envelope for routing.

Message :

- The actual message inside the envelope is made of two parts :
  1. Header and 2. Body
- Header carries the control information while body contains the message contents.
- Envelopes and messages are shown in Fig. 3.13.1.



(G-640) **Fig. 3.13.1 : Envelope and message**

3.13.2 Message Formats :

Let us now discuss the e-mail message formats.

RFC 822 :

- All the e-mail messages consist of an envelope, a few header fields, a blank line and then the message body.
- Each header field logically consists of a single line of ASCII text which consists of the field name, a colon and a field.
- Normally the user agent builds a message and passes it to the message transfer agent which uses some header fields for construction of an envelope.
- Table 3.13.1 shows the principle header fields related to the message transport. Let us discuss them one by one.

Table 3.13.1 : RFC 822 header fields related to message transport

Header Name	Meaning
To :	E-mail address of primary recipients
Cc :	E-mail address of secondary recipients (Carbon copy)
Bcc :	E-mail address for blind carbon copies
From :	Originator of the message
Sender :	E-mail address of the person sending the message
Received :	Line added by each transfer agent along the route
Return – Path :	Can be used to identify the path back to the sender

1. **The To : field :**

   This field gives the DNS address of the primary recipient. It is allowed to have multiple recipients.

2. **The Cc : field :**

   This field gives the addresses of any secondary recipients. Cc stands for carbon copy. Whatever message and attachments are sent to the primary recipient the same are sent to the secondary recipient as well.

3. **The Bcc : field :**
   - The long form of Bcc is blind carbon copy. This field is like Cc field, except that this is deleted from all the copies sent to the primary and secondary recipients.
   - Thus a sender can send copies to third parties without primary and secondary recipients knowing about it.

4. **From : and Sender : fields :**
   - These fields tell about who wrote the message and who actually sent the message respectively because the person who creates the message and the person who sends it can be different.
   - The From : Field is necessary but the Sender : field can be omitted, if it is same as the From : field.
   - These fields are required when the message cannot be delivered and is to be returned to the sender.

5. **Received : field :**
   - A line containing Received : is added by each message transfer agent along the way. This line carries the agent's identity, date and time at which the message was received.
   - It also contains some other information that can be used to find bugs in the routing system.

6. **The Return-Path : field :**
   - This field is added by the final message transfer agent and it is intended to tell how to get back to the sender.
   - This information can be obtained from all the received : headers.

Other header fields :

In addition to the fields of Table 3.13.2, RFC 822 messages may contain many other header fields. These are used by either the user agents or human recipients some of them are shown in Table 3.13.2.

Scanned by CamScanner

Table 3.13.2 : Some fields in RFC 822 message header

Header	Meaning
Date :	The date and time of the message.
Reply-To	E-mail address to which the reply is to be sent
Message-Id :	Message identifying number
In-Reply-To :	Message-Id of the message to which this is a reply
References :	Other relevant message identifying numbers
Keywords :	Keywords chosen by user
Subject :	Summary of the message for the one line display.

- The RFC 822 allows the users to invent new headers for their own private use but it is essential that these headers start with the string X-. For example X-Event of the week.

Message Body :

- The message body comes after the header. The users can include anything that they want to send, in the message body.
- It is possible to terminate the messages with ASCII cartoons, quotations, political statements etc.

3.14 MIME – Multipurpose Internet Mail Extensions :

- In the early days, the e-mail used to consist of only the text messages in English and expressed in ASCII.
- RS 822 was sufficient for this environment. But in the worldwide internet environment, this approach is not adequate.
- Some problems are encounter in sending and receiving the following types of messages :
  1. Messages in certain languages that have accents such as French or Germans.
  2. Messages which do not contain text e.g. audio and video.
  3. Messages in the languages which do not have alphabets (e.g. Chinese and Japanese).
  4. Messages which contain some non-Latin alphabets such as Russian or Hebrew.
- The solution to these problems was MIME i.e. Multipurpose Internet Mail Extensions. It was proposed in the standard RFC 1341 and then updated in RFC 1521.

3.14.1 Principle of MIME :

- MIME uses the same RFC 822 format but it adds structure to the message body (In RFC 822 there is no structure to the message body). In addition to this, MIME defines encoding rules for non ASCII messages. It is possible to send MIME messages using the existing mail programs and protocols.
- The sending and receiving programs need to be changed to achieve this, which users can do themselves.

New message headers :

Five new message headers are defined for MIME. They are listed in Table 3.14.1.

1. **MIME-Version :**

   It tells the user agent that this message is a MIME message and it also specifies the version of MIME being used.

Table 3.14.1 : New headers in MIME

Sr. No.	Header Name	Meaning
1.	MIME – Version :	Indicates the MIME version
2.	Content – Description :	Tells what is in the message
3.	Content – Id :	Identifier
4.	Content – Transfer – Encoding :	How is the body wrapped for transmission
5.	Content – Type :	Type of the message.

2. **Content-Description :**

   This header tells what the message is. It is in the form of ASCII string. This header is needed because the recipient will know whether it is worth decoding and reading the message.

3. **Content-Id :**

   This field identifies the contents. Its format is same as the format of standard Message- Id header.

4. **Content-Transfer-Encoding :**

   - This field tells how the body is wrapped for transmission through a network. The network can object to most characters except for the letters, numbers and punctuation marks.
   - Five schemes are provided for this purpose in addition to an escape to new schemes. These schemes are as follows :

   (a) The first scheme simply uses ASCII text. Each ASCII character uses 7-bits and can be carried directly if each line contains at the most 1000 characters.

   (b) The second scheme is similar to the first scheme except for one change. Instead of 7-bit characters, now 8-bit characters are used. The maximum line length remains unchanged.

   (c) Third is the messages using binary encoding. The problems with these messages are that they do not always use all the 8 bits and do not stick to the 1000 line per character limit. There is no guarantee that these messages arrive errorfree.

   (d) The fourth type is encoded binary messages using **base 64** encoding which is also called as ASCII armor.

   (e) The fifth type is the messages with a special type of encoding called **quoted-printable encoding.**

5. **Content-Type :**

   - This is last header in Table 3.14.1 and it is used to specify the type of the message body. RFC 1521 defines seven types with each one having one or more subtypes.
   - The type and subtype are separated by a slash such as,

     Content – Type : Video / mpeg.
   - The subtype must be given in the header. Table 3.14.2 gives the initial list of types and subtypes specified in RFC 1521.

Table 3.14.2 : The MIME types and subtypes in RFC 1521

Type	Subtype	Description
Text	Plain	Text in the unformatted way
	Richtext	Text includes simple formatting commands
Image	Gif	Still pictures in GIF format
	Jpeg	Still pictures in JPEG format
Audio	Basic	Audio or sound content
Video	Mpeg	Movie (video) in MPEG format
Applications	Octet-stream	Byte sequence in uninterpreted form
	Post script	A printable document in Post script
Message	Rfc 822	A MIME RFC 822 message
	Partial	Split message for transmission
	External body	Message itself should be fetched over the net
Multipart	Mixed	There are independent parts in the specified order
	Alternative	Same message in different formats
	Parallel	Parts must be viewed simultaneously
	Digest	Each part is a complete RFC 822 message

- Note that many new types have been added to the basic list of Table 3.14.2 and the addition is still being made. Let us discuss the content types listed in Table 3.14.2.

(a) **Text :**

- The text type is for straight text. There are two subtypes namely plain and richtext.
- The text / plain combination represents the original messages without any encoding or further processing.
- The text/richtext allows simple formatting in the text. It allows the text with boldface, italics, small and large point sizes, indentation, subscripts, page layout etc.

(b) **Image :**

- This MIME type is used for transmitting still pictures. There are many formats used for storing and transmitting images with or without compression.
- The two subtypes are GIF and JPEG.

(c) **Audio and Video :**

The audio type is for sound and video is for moving pictures. The video does not include any soundtrack. Only one video format defined is MPEG which is designed by the Moving Picture Experts Group (MPEG).

(d) **Applications :**

- This type is used for formats which require external processing and which is not covered by any other type.
- The octet stream is a sequence of uninterpreted bytes. When it is received a user agent should display it and suggest the user to copy it in a file for further processing.
- The other subtype is post script. It corresponds to the post script language produced by Adobe systems which is used for describing printed pages.

(e) **Message :**

- This type allows one message to be fully encapsulated inside the other message. This is useful in order to forward e-mails.
- The partial subtype allows to break an encapsulated message into pieces and send them separately.
- The external body subtype can be used for very long messages such as video films.

(f) **Multipart :**

- This is the last type of multipart. It allows a message to contain multiple parts in the same message. The beginning and end of each part is clearly demarked within a message.
- There are four subtypes. The mixed subtype allows each part to be different. In the alternative subtype each part should contain the same message expressed in a different medium or encoding.
- The alternative subtype can be used for multiple languages as well.
- The parallel subtype is used for viewing all parts simultaneously e.g. audio and video parts of a movie.
- The fourth subtype is digest. It is used when many messages are packed together to form a composite message.

3.15 Message Transfer Agent : SMTP :

- 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.

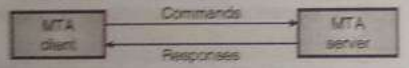
Scanned by CamScanner

(G-641) Fig. 3.15.2 : SMTP range

- As shown in Fig. 3.15.1, 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.

3.15.1 Commands and Responses :

- As shown in Fig. 3.15.2, SMTP the transfer of messages between MTA client and MTA server takes place using the command and response principle.



(G-642) Fig. 3.15.2 : 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.

3.15.2 SMTP (Simple Mail Transfer Protocol) :

- 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.

3.15.3 Components of E-mail System :

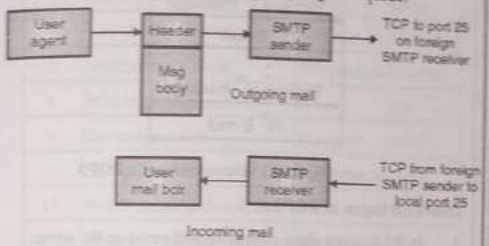
The three main components of internet mail system are :

1. User Agent (UA)
2. SMTP sender
3. SMTP receiver

They are shown in Fig. 3.15.3.

- The mail is created by a user agent program in response to user input. Each created message consists of a header which includes the recipient's E-mail address and other information and the message body containing the message to be sent.
- These messages are lined up to form a queue and provided as input to an SMTP sender program.

- The SMTP sender takes messages from the queue and transmits them to the proper destination host via SMTP connection over one or more TCP connections to port 25.
- The SMTP protocol is used to transfer a message from the SMTP sender to SMTP receiver and it uses TCP connection for the same.
- The SMTP receiver accepts each arriving message and stores it in the user mail box. If the mail is to be forwarded then the SMTP receiver copies it to the outgoing mail queue.



(G-643) Fig. 3.15.3 : SMTP mail flow

3.15.4 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 3.15.1 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 3.15.1 : 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.

3.15.5 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.

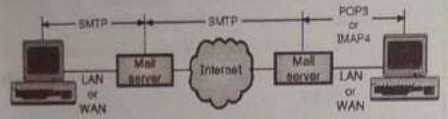
3.15.6 Comparison of HTTP and SMTP :

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.
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.

Scanned by CamScanner

3.16 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. 3.16.1 : Use of POP 3 or IMAP 4**

3.16.1 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. 3.16.1.
  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. 3.16.2.

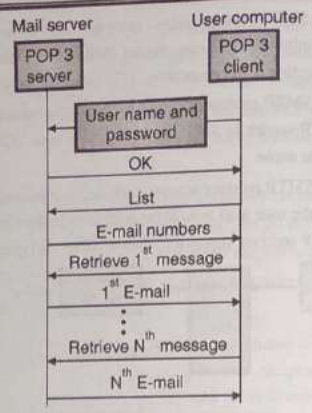
Modes of POP 3 :

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. 3.16.2 : 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.

3.16.2 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.
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.

3.16.3 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

3.17 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.

3.17.1 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.

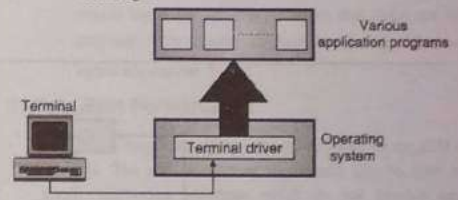
Time Sharing Environment :

- 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. 3.17.1 illustrates the principle of local login.



(G-1793) **Fig. 3.17.1 : 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. 3.17.2 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

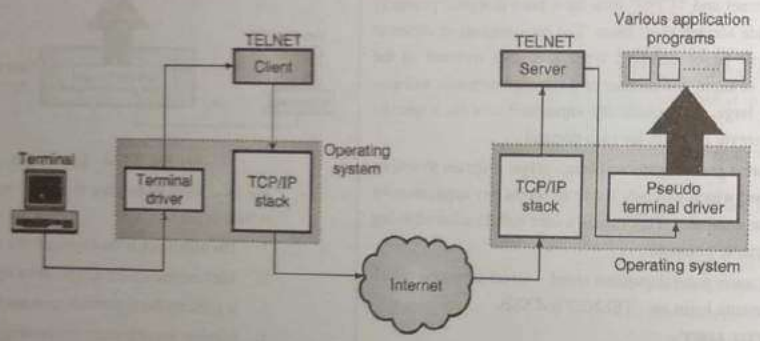
2. The terminal driver at local O.S. accepts the characters but sends them to TELNET client without interpreting them.
3. TELNET client converts them into NVT characters. NVT is Network Virtual Terminal. This is a universal character set.
4. NVT characters are delivered to TCP/IP stack (local).
5. The 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.

3.17.2 Network Virtual Terminal (NVT) :

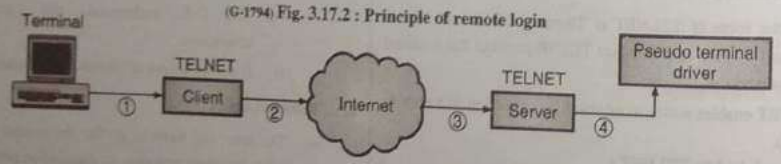
- NVT character set is a universal interface defined by TELNET in order to ensure that a user can access any remote computer in this world.
- Fig. 3.17.3 illustrates the concept of NVT.
- The local computer character set is used for the communication between the user terminal and TELNET client.
- Then 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. 3.17.3.
- NVT has two sets of characters. One set is for the data and the other set is for control. Both have 8 bit characters.

3.17.3 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. 3.17.2 : Principle of remote login**



① - Local computer character set
② and ③ - NVT character set
④ - Remote computer character set

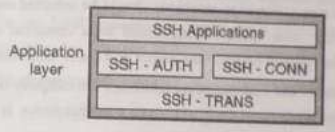
(G-1795) **Fig. 3.17.3 : Concept of NVT**

3.17.4 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. 3.17.4, it has four components.



(G-1796) **Fig. 3.17.4 : 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 :

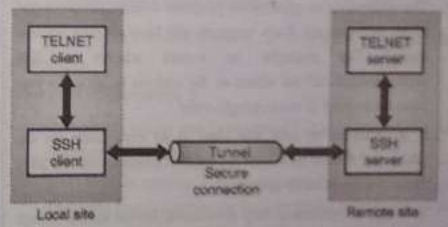
- The third component of SSH is SSH – CONN i.e. SSH connection protocol.
- This piece of software is called for by the SSH once a secure connections has been established and authentication done.
- SSH – CONN performs the multiplexing as one of its services. It allows the client to create multiple logical 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.

3.17.5 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. 3.17.5. 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. 3.17.5.

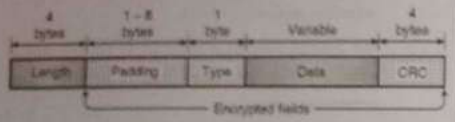


(G-1797) **Fig. 3.17.5 : Port forwarding**

Scanned by CamScanner

3.17.6 SSH Packet Format :

- The SSH packet format is as shown in Fig. 3.17.6.



(G-1798) **Fig. 3.17.6 : 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.

3.18 Domain Name System (DNS) :

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.

3.18.1 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.

3.18.2 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.

3.18.3 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.

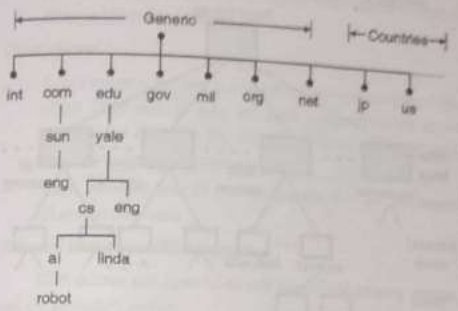
3.18.4 Hierarchical Name Space :

- 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.

3.19 Domain Name Space :

- 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. 3.19.1.

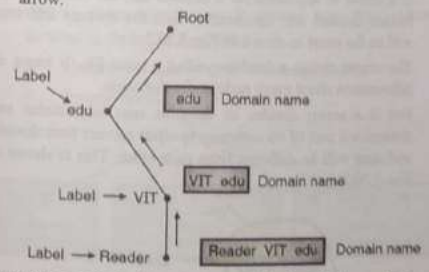


(G-631)**Fig. 3.19.1 : A portion of Internet domain name space**

- 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. 3.19.2. The upward followed path has been shown by an arrow.



(G-632)**Fig. 3.19.2 : 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 ?

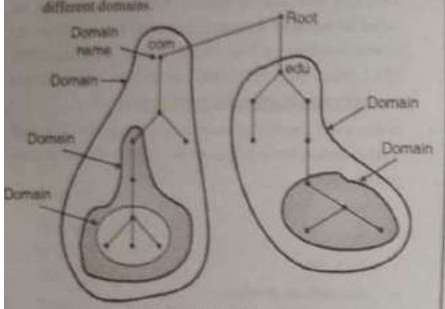
- Component names can have upto 63 characters and the full path name can at the most have 255 characters.
- Each domain controls how it allocates the domain under it. To create a new domain we have to take a permission of the domain in which it is to be included.

Domain :

- A domain can be defined as a subtree of the DNS name space as shown in Fig. 3.19.3. The name of the domain is the domain name of the node at the top of the subtree as shown in Fig. 3.19.3. e.g. com or edu.

Scanned by CamScanner

- A domain can be divided into subdomains as shown in Fig. 3.19.3.
- 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. 3.19.3 : Domains

3.20 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.

3.20.1 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.

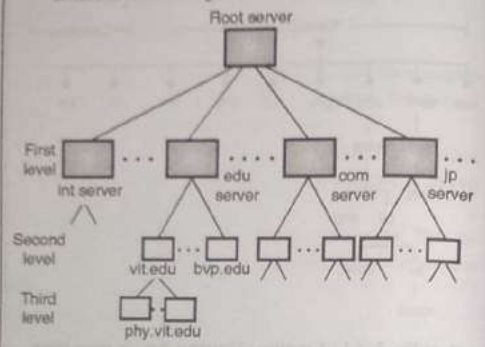
Such a server will be soon overloaded and be useless and worst thing is if it ever goes down the entire Internet will go down.

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. 3.20.1.

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. 3.20.1.

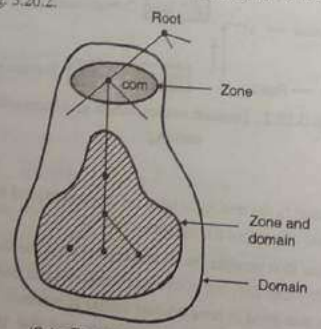


(G-634)Fig. 3.20.1 : Hierarchy of name servers

- 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. 3.20.2.
- 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. 3.20.2.



(G-635)Fig. 3.20.2 : Domains and zones

- The information about the nodes that belong to the subdomains is stored in the servers at the lower levels. The higher level and original server keeps some sort of reference of these lower level servers.

Root server :

- A root server is defined as a server whose zone consists of the whole DNS tree. It does not store any information about domains but delegates the authority to other servers. It only keeps the reference of these servers.
- There are more than 13 root servers and they are distributed all around the world.

Primary and secondary servers :

DNS defines two types of servers namely the primary servers and the secondary servers.

Primary server :

It is a server which stores a file about its zone. It is authorised to create, maintain and update the zone file. It stores the zone file on a local disk.

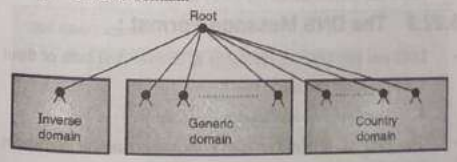
Secondary server :

- This server transfers complete information about a zone from another server which may be primary or secondary server. The transferred information is saved on the disc storage of the secondary server.
- The secondary server is not authorized to create or update a zone file. If its zone file is to be updated, then it is to be done by the primary server.

3.21 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. 3.21.1.

1. Generic domain 2. Country domain
3. Inverse domain.



(G-636)Fig. 3.21.1 : Use of DNS in Internet

3.21.1 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 3.21.1.

Table 3.21.1 : 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.

3.21.2 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.

3.21.3 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.

3.22 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.

Scanned by CamScanner

- 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 :

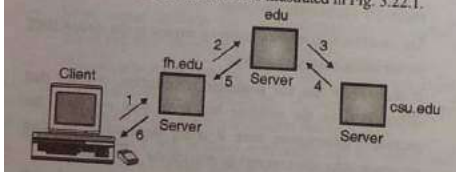
- Here, a client sends an IP address to a server and requests for its name. This type of query is called as PTR query.
- To answer the PTR query, the DNS uses the inverse domain.
- If the IP address is 142.36.48.118 then the resolver first inverts the address and adds two labels "in_addr" and "arpa" to it. So the domain name sent is :

  118.48.36.142.in_addr.arpa.

- This is received by the local DNS and resolved.

3.22.1 Recursive Resolution :

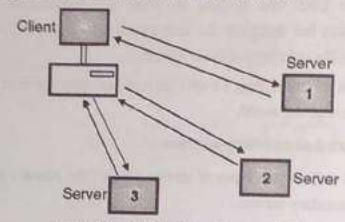
- Sometimes a client (resolver) requests for recursive or final answer from a name server.
- If this server is authorised for the domain name, it checks its database and sends a reply.
- But if this server is not authorised it diverts this request to another server (usually the parent server) and waits for the response.
- If the parent has the authority, then it sends the answer, otherwise it diverts the query to another server.
- When the query is solved, the response is returned back to the requesting client.
- Such a query is called as recursive query and the process is called recursive resolution. It is illustrated in Fig. 3.22.1.



(G-637)**Fig. 3.22.1 : Recursive resolution**

3.22.2 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. 3.22.2 illustrates the iterative resolution.



(G-638)**Fig. 3.22.2 : 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 :

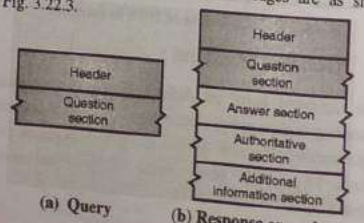
- www.yahoo.com - the world's best-known name
- www.mit.edu - a popular EDU name
- encarta.msn.com - a Web server that does not start with www
- www.bbc.co.uk - a name using four parts rather than three
- ftp.microsoft.com - an FTP server rather than a Web server
- www.spce.ac.in - Server in India 'in' 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.

3.22.3 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. 3.22.3.



(a) Query (b) Response or reply

(G-639)**Fig. 3.22.3**

- 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. 3.22.3.

3.22.4 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.

3.23 DNS Records :

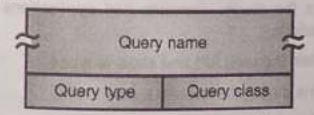
- There are two types of records used in DNS as follows :

  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.

3.23.1 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. 3.23.1.
- Various fields in the question record format are query types and query class.



(G-1791) **Fig. 3.23.1 : 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 :

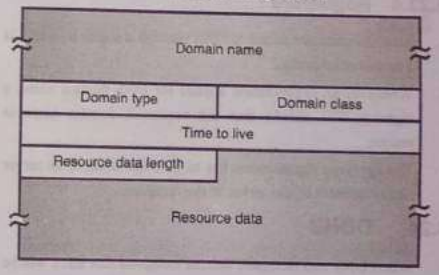
- This field also is 16-bit long. It defines the specific protocol using DNS. Table 3.23.1 has listed some of possible classes. However the most important class would be IN i.e. internet (class 1).

Table 3.23.1 : 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)

3.23.2 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. 3.23.2.



(G-1792) **Fig. 3.23.2 : 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.

Scanned by CamScanner

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. 3.23.2 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.

3.23.3 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.

3.23.4 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.

3.24 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. 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 unauthorized changes in DNS records.

3.24.1 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.

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. For more details on how TCP is used in FTP refer section 3.12.

□□□

Scanned by CamScanner

CHAPTER 4

Module II

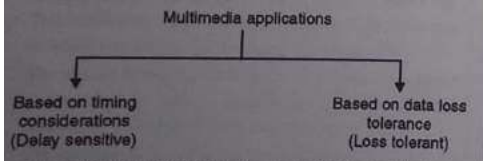
Multimedia

Syllabus :

Compression : Lossless compression, Lossy compression, Multimedia data : Text, Image, Video, Audio, Multimedia in Internet : Streaming stored Audio / Video, Streaming live audio / video, Real time interactive audio / video, Optimal compression algorithms, Huffman coding, Adaptive Huffman compression, Dictionary based compression, Speech compression, LZW, RLE, Image compression GIF, JPEG.

4.1 Multimedia :

- The meaning of multimedia is two or more media. But in practice when we use the word multimedia, it means the combination of two or more **continuous media.**
- Usually the two media are audio and video.
- Multimedia is a system, which is a combination of following components such as :
  1. Text 2. Images or Graphics
  3. Animation 4. Sound 5. Video
- In multimedia, all these five media are used to represent the information to the users via the computer.
- In practice, many multimedia packages comprise of only two or three medias of the above media, as sometimes the use of all media types may not be appropriate for the information exchange. Typically all computers have inbuilt sound cards. Playing of notes, music is possible.
- We can classify the multimedia applications in two major categories as shown in Fig. 4.1.1.



(G-724) **Fig. 4.1.1 : Classification of multimedia applications**

- **Delay sensitive :** These applications are sensitive to timing delays. Many multimedia applications are useless if the sender to receiver delay is more than a few hundred milliseconds.

Loss tolerant : Most of the multimedia applications are loss tolerant. That means they allow the loss of data to some extent without compromising with the quality.

So the multimedia applications are delay sensitive but loss tolerant, which are different from the elastic applications such as E-mail, FTP and Telnet.

4.2 Compression : MU : May 14, May 15, May 16

University Questions

Q. 1 What is compression ? List compression algorithms. **(May 14, May 15, 3/4 Marks)**

Q. 2 What is compression ? List different compression algorithm. Why adaptive Huffman coding is used ? **(May 15, 4 Marks)**

Q. 3 What is compression ? List different compression algorithm. **(May 16, 4 Marks)**

- Due to the large volume of data exchanged, compression plays an important role in multimedia communication.
- In compression the volume of data to be exchanged is reduced.
- Basically there are two forms of data compression :
  1. Lossless compression 2. Lossy compression.

4.2.1 Lossless Compression : MU : Dec. 15

University Questions

Q. 1 What is lossless compression ? **(Dec. 15, 5 Marks)**

- In lossless compression, the redundant information contained in the data is removed.
- Due to removal of such information, there is no loss of the data which contains information. Hence it is called as lossless compression.
- Lossless compression is also known as data compaction.
- Lossless compression is achieved using those techniques which generate an exact duplicate of the input data stream after following compression at transmitter and expansion at the receiver.

4.2.2 Lossy Compression : MU : Dec. 15

University Questions

Q. 1 Describe Lossy compression methods. Where we use Lossy compression methods ? **(Dec. 15, 6 Marks)**

- In this type of compression, there is a loss of information in a controlled manner.

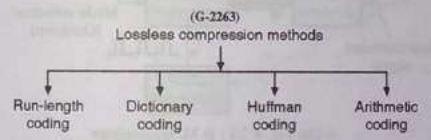
- The lossy compression is therefore not completely reversible. That means we can not reproduce the exact replica of the original picture at the receiver.
- But the advantage of this type is higher compression ratios than the lossless compression.
- The lossless compression is used for the digital data. The lampel - ziv algorithm is used for the same.
- For many applications, the lossy compression is preferred due to its higher compression without a significant loss of important information.
- Lossy compression can be applied to graphical images and digitized voice.
- By their very nature, these digitized representations of analog phenomenon are not perfect and so a small loss of information due to compression does not matter much.

4.2.3 Lossless Compression :

- Data integrity is preserved in lossless compression.
- The compression and decompression algorithms are exactly opposite to each other. In this process there is no loss of the data which contains information.
- Lossless compression is used when we cannot afford any data loss.
- In some lossy compression processes for further reduction of data size, lossless compression is applied as the last step.

Lossless compression methods :

- Lossless compression methods are as follows :



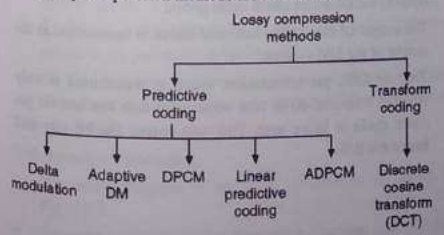
We have discussed all these topics at the end of this chapter.

4.2.4 Lossy Compression :

- There is limit on the amount of compression in lossless compression methods.
- In the following subsections we will discuss some lossy compression methods.

Lossy compression methods :

- Lossy compression methods are as follows :



(G-2264) **Fig. 4.2.1**

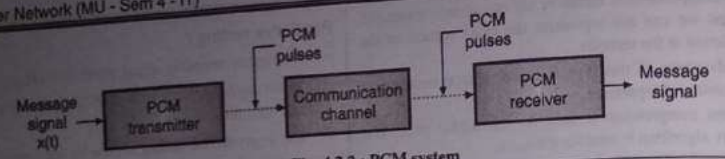
Predictive coding :

- To digitize an analog signal, predictive coding is used.
- In the digital systems such as PCM, each sample is quantized and encoded.
- But in **predictive coding** we use the similarity in the adjacent samples. So instead of quantizing and encoding each sample, the difference between the adjacent samples is quantized and encoded.
- This will reduce the number of bits required for encoding.
- Some of the examples of predictive coding are :
  1. Delta modulation
  2. Adaptive delta modulation
  3. Differential PCM (DPCM)
  4. Adaptive DPCM (ADPCM)

4.2.5 Pulse Code Modulation (PCM) :

- PCM is a "digital" pulse modulation system.
- That means the PCM output is in the coded digital form. It is in the form of digital pulses of constant amplitude, width and position.
- The information is transmitted in the form of "code words". A PCM system consists of a PCM encoder (transmitter) and a PCM decoder (receiver).
- The essential operations in the PCM transmitter are sampling, quantizing and encoding.
- All these operations are usually performed in the same circuit called as analog-to-digital (A to D) converter.
- It should be understood that the PCM is not modulation in the conventional sense.
- Because in modulation, one of the characteristics of the carrier is varied in proportion with the amplitude of the modulating signal. Nothing of that sort happen in PCM.
- Fig. 4.2.2 shows the simplified block diagram of a PCM system. It consists of a transmitter and receiver.
- The transmitter converts the message signal x (t) into a series of coded pulses and sends it over the communication channel.
- The transmitter is also called as an encoder.
- The receiver performs exactly in the reverse way as compared to the transmitter. It will convert the received encoded PCM pulses back into the message signal.

Scanned by CamScanner



(D-771) Fig. 4.2.2 : PCM system

4.2.6 Delta Modulation (D.M.) :

In PCM system, N number of binary digits are transmitted per quantized sample. Hence the signaling rate and transmission channel bandwidth of the PCM system are very large.

- These disadvantages can be overcome by using the delta modulation.

Principle of operation :

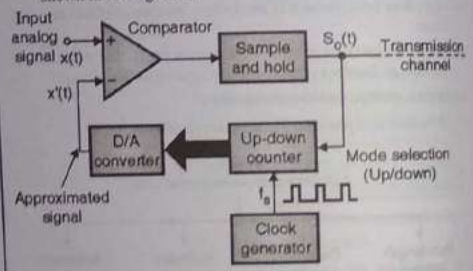
- Delta modulation transmits only one bit per sample instead of N bits transmitted in PCM. This reduces its signaling rate and bandwidth requirement to a great extent.
- In the basic or linear D.M., a staircase approximated version of the sampled input signal is produced as shown in Fig. 4.2.3.
- The original signal and its staircase representation are then compared to produce a difference signal.
- And this difference signal is quantized into only two levels namely ± δ corresponding to positive and negative difference respectively.
- That means if the approximated signal x′ (t) lies below x (t) at the sampling instant, then the approximated signal is increased by "δ". (See instants 1, 2, 3, 4, 5 and 6 in Fig. 4.2.3)
- Whereas if x′ (t) is greater than x (t) at the sampling instant, then x′ (t) is decreased by "δ" (see instants 7, 9 and 10 in Fig. 4.2.3.)

D.M. output :

- As shown in Fig. 4.2.3, the D.M. output is 1 if the staircase signal x′ (t) is increased by "δ" i.e. at sampling instants 1, 2, 3, 4, 5 and 6.
- Whereas D.M. output is 0 if x′ (t) is decreased by "δ" i.e. at sampling instants 7, 9 and 10.
- In delta modulation, the present sample value x (t) is compared with the approximate value x′ (t) and the result of this comparison is transmitted.
- Thus we are sending the information of whether the present sample value is higher than or lower than the approximate value. Note that the actual sampled value is not being transmitted.

Delta modulator transmitter (encoder) :

- The block diagram of a delta modulator transmitter is as shown in the Fig. 4.2.4.

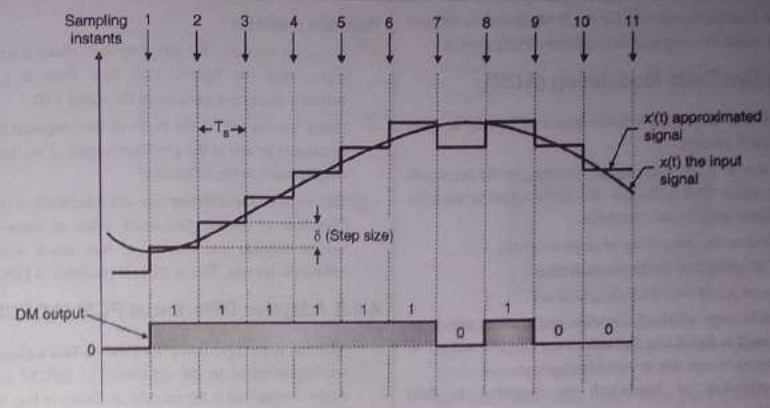


(L-236) Fig. 4.2.4 : D.M. transmitter

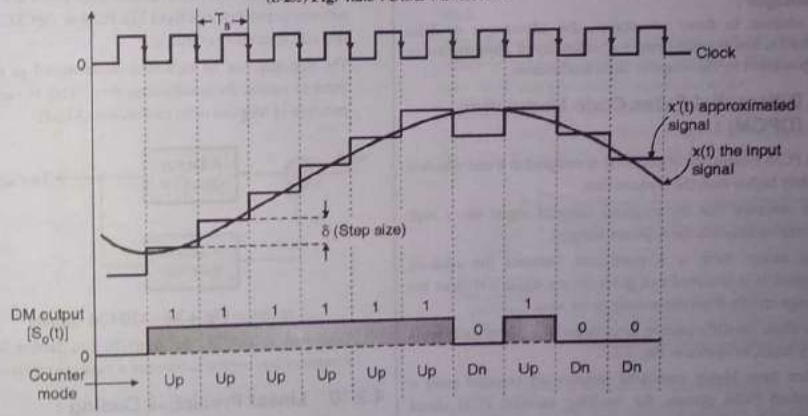
Operation

The operation of the D.M. transmitter is as follows :

- x (t) is the analog input signal and x′ (t) is the quantized (approximated) version of x (t). Both these signals are applied to a comparator.
- The comparator output goes high if x (t) > x′ (t) and it goes low if x (t) < x′ (t). Thus the comparator output is either 1 or 0. The sample and hold circuit will hold this level (0 or 1) for the entire clock cycle period.
- The output of the sample and hold circuit is transmitted as the output of the DM system.
- Thus in DM, the information which is transmitted is only whether x (t) > x′ (t) or vice versa. Also note that one bit per clock cycle is being sent. This will reduce the bit rate and hence the BW.



(L-235) Fig. 4.2.3 : D.M. waveforms

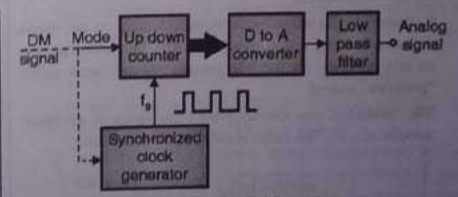


(L-237) Fig. 4.2.5 : D.M. waveforms

- The transmitted signal is also used to decide the mode of operation of an up/down counter. The counter output increments by 1 if S_o (t) = 1 and it decrements by 1 if S_o (t) = 0, at the falling edge of each clock pulse. This is as shown in the waveform in the Fig. 4.2.5.
- The counter output is converted into analog signal by a D to A converter. Thus we get the approximated signal x′ (t) at the output of the D to A converter.

D.M. receiver (decoder) :

- The block diagram of the D.M. receiver is as shown in Fig. 4.2.6.
- Compare it with the transmitter block diagram, you will find that it is identical to the chain of blocks producing the signal x′ (t) i.e. the approximated signal.
- The original modulating signal can be recovered back by passing this signal through a low pass filter.



(L-238) Fig. 4.2.6 : D.M. receiver

D.M. bit rate (Signaling rate) :

- D.M. bit rate (r) = Number of bits transmitted / second

$$= \text{Number of samples/sec} \times \text{Number of bits/sample}$$

$$= f_s \times 1 = f_s \quad \text{...(4.2.1)}$$

- Thus the D.M. bit rate is (1/N) times the bit rate of a PCM system, where N is the number of bits per transmitted PCM codeword.

Scanned by CamScanner

- Hence the channel bandwidth for the D.M. system is reduced to a great extent as compared to that for the PCM system.

4.2.7 Adaptive Delta Modulation (ADM) :

- It is possible to improve the performance of DM by keeping the step size δ variable.
- The step size in ADM is changed according to the amplitude of analog signal. This will allow the ADM signal to track the original signal quickly and faithfully.
- This will reduce the possibility of slope overload.

Advantages of adaptive delta modulation :

The advantages of ADM over DM are as follows :

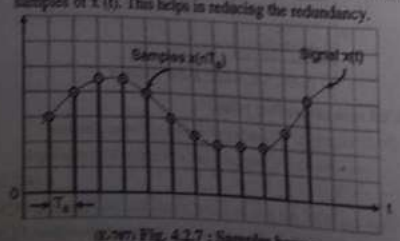
1. Reduction in slope overload distortion and granular noise.
2. Improvement in signal to noise ratio.
3. Wide dynamic range due to variable step size.
4. Better utilization of bandwidth as compared to delta modulation.

Disadvantages :

In addition to these advantages, the advantages of delta modulation i.e. low signaling rate and simplicity of implementation are also possessed by the adaptive delta modulation.

4.2.8 Differential Pulse Code Modulation (DPCM) :

- In a PCM system, the signal x (t) is sampled at a rate which is slightly higher than the Nyquist rate.
- It is observed that the resulting sampled signal has a high correlation between the adjacent samples.
- That means there is a correlation between the adjacent samples. It is observed that generally the signal x (t) does not change rapidly from one sample to the next.
- Therefore the difference in amplitudes of adjacent samples is very small, as shown in Fig. 4.2.7.
- When these highly correlated samples are encoded using a standard PCM system, the resulting encoded PCM signal contains redundant information. Redundant bits do not contain any new information.
- By removing this redundancy before encoding, we can obtain a more efficiently coded signal. The DPCM system operates on this principle. In DPCM system a special circuit called "predictor" is used.
- The "predictor" can actually predict the values of the future samples of x (t). This helps in reducing the redundancy.



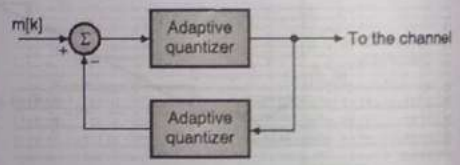
(E-707) Fig. 4.2.7 : Samples have a correlation between them

Role of a predictor :

- It is observed that if the sampling takes place at a rate which is higher than the Nyquist rate, then there is a correlation between successive samples of the signal x (t).
- Hence we can predict the range of next required increment or decrement in x(t) at the predictor output, if we know the past sample value or the difference.
- This reduces the difference or error between x (t) and $\bar{x}$ (t). Therefore to encode this small value of error the DPCM system requires less number of bits which will ultimately reduce the bit rate. This is the role predictor in DPCM system.

4.2.9 Adaptive Differential PCM (ADPCM) :

- ADPCM is the next step after DPCM. This technique is used for improvement in the efficiency of DPCM by using an adaptive equalizer at the encoder as shown in Fig. 4.2.8.
- In ADPCM the number of quantization levels are fixed. The step size is however not fixed like PCM or DPCM. Instead the step size is adaptive (variable).
- The step size can be increased or decreased as required in order to reduce the quantization error. This is similar to the principle of adaptive delta modulation (ADM).



(E-1010(a)) Fig. 4.2.8 : ADPCM encoder

- Compared to DPCM, the ADPCM can further reduce the number of bits needed to transmit a message signal.

4.2.10 Linear Predictive Coding :

- Linear predictive coding (LPC) is a new and completely different method of representing an analog signal digitally.
- The analog signal at the input is first synthesized. The parameters of the waveform synthesizer are then encoded and transmitted instead of transmitting the original signal. LPC is particularly well suited for speech synthesis and transmission.
- This method uses a transversal filter or its digital equivalent alongwith some auxiliary components to synthesize the required waveform.
- The parameters of the waveform synthesizer are then encoded for transmission (note that the actual signal is not transmitted).

4.3 Transform Coding :

- In transform coding to generate the output signal, a mathematical transformation is applied to the input signal.
- To allow the recovery of the original signal, the transformation is required to be invertible.

- In encoding, there is reduction in the number of bits. This is because transformation changes the representation of signal from one domain to other domain (e.g. time domain to frequency domain).
- The quantization step is added to the operation to achieve the compression goals.

We have discussed this topic at the end of this chapter.

4.3.1 Difference between Lossless and Lossy Compression :

Table 4.3.1 shows comparison between lossless and lossy compression.

Table 4.3.1

Sr. No.	Parameter	Lossless compression	Lossy compression
1.	Preserving information	Yes	No
2.	Compression Ratio	Low	High
3.	Examples	RLE, LZW	JPEG, MPEG
4.	Used in	Text file compression	Image compression

4.4 Multimedia Data :

Multimedia data consists of :

1. Text
2. Images
3. Video
4. Audio

4.4.1 Text :

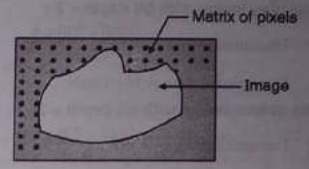
- The Internet accumulate a huge amount of text which can be used and downloaded.
- In textual data, it always refers to plaintext as a linear form and hypertext as a non linear form.
- For representation of symbols in the underlying language, text store in the Internet uses a character set such as Unicode.
- One of the lossless compression method discussed earlier is used to compress text for storage of large amount of textual data.
- At the time of decompression, we can't afford loss of any piece of information. Due to this reason we need to use lossless compression.

4.4.2 Images :

In a moving picture, an image is the representation of a photography, a frame or a fax page.

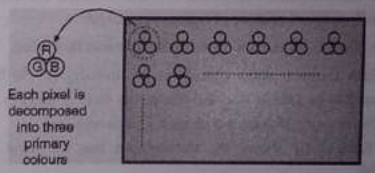
Digital image :

- To use an image, first it should be digitized. To represent an image as a two dimensional array of dots (pixels) is called as **digitization.**
- Each pixel is in the form of number of bits which is referred to as the **bit depth.**
- The basic principle is as follows. An image is divided into a matrix of pixels (pixel means picture element).
- Each pixel is in the form of a small dot as shown in Fig. 4.4.1. We can use a large number of pixels for better resolution.
- Higher resolution ensures better quality of picture.



(G-5) Fig. 4.4.1

- After dividing the image into pixels, each pixel is represented by a unique bit pattern.
- For black and white image 1 bit per pattern is sufficient to represent a pixel. 1 will represent white and 0 will represent black.
- If the gray shades are to be included then we can use 2 bit pattern to represent each pixel. Then 00 is black, 01 is dark gray, 10 is light gray and 11 represents white.
- If a coloured image is to be represented, then each coloured pixel is decomposed into three primary colours namely Red, Green and Blue (RGB), as shown in Fig. 4.4.2.



(G-6) Fig. 4.4.2 : Pixels for coloured images

- The intensity of each colour at each pixel is then converted into an 8 bit pattern. Thus colour image representation needs more number of bits. Thus the intensity information corresponding to each pixel is to be converted into a unique binary bit pattern.
- In a black and white image bit depth = 1. e.g. fax page
- In a colour image, bit depth = 24 (8 bits for each column)
- In a gray image, bit depth = 8 with 256 levels.
- To represent the background, some representations use a separate channel known as α (alpha)-channel. For black and white image this results in two α-channels. In a color image this results in 4 channels.

Ex. 4.4.1 : Calculate the time required to transmit an image of 1280 × 720 pixels if transmission rate of 100 kbps using :

1. Black and white image
2. Gray image
3. Colour image

Scanned by CamScanner

oln. :

. **Using a black and white image with bit depth = 1 :**

$\therefore$ Transmission time $= \frac{1280 \times 720 \times 1}{1,00,000}$

$\therefore$ Transmission time = 9 seconds

. **Using gray image with bit depth = 8 :**

$\therefore$ Transmission time $= \frac{1280 \times 720 \times 8}{1,00,000}$

$\therefore$ Transmission time = 74 seconds

Using colour image with bit depth = 24 :

$\therefore$ Transmission time $= \frac{1280 \times 720 \times 24}{1,00,000}$

$\therefore$ Transmission time = 221 seconds

4.3 Video :

Video is composition of multiple frames where each frame is e image. That means, a high transmission rate is required for leo file.

gitizing video :

A video consists of a sequence of frames. We get impression of motion if the frames are displayed fastly on the screen.

The reason behind this is that our eyes cannot differentiate the quickly flashing frames.

25 frames/second is common in North America. There is no as such standard number of frames per second.

A frame is required to be refreshed to avoid **flickering.**

Each frame repaints twicely in TV industry i.e. 50 frames need to be sent or if at the sender site there is memory, from the memory 25 frames with each frames repainted.

Table 4.4.1 shows the transmission rate for some video nnel.

Table 4.4.1

Video standard	Resolution	Number of frames / sec.	Bits/ Colour	Transmission rate
Colour Broadcast television	720 × 480	30	24	720 × 480 × 30 × 24 = 248,832,000 bps = 249 Mbps
High broadcast colour television	1920 × 1080	30	24	1920 × 1080 × 3 × 24 = 1,492,992,00 bps = 1.5 Gbps

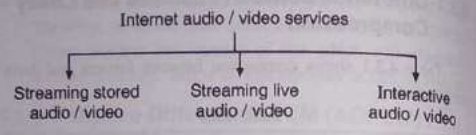
.4 Audio :

The nature of sound (audio) signal is analog which requires a medium to travel. Audio signal cannot travel through a vaccum.

In the air, speed of light is about 330 m/s. For normal human hearing the range of audible frequency is about 20 Hz to 20 kHz with maximum audibility is about 3300 Hz.

4.5 Multimedia in Internet :

- Fig. 4.5.1 shows the classification of audio and video services. It shows that audio and video services can be classifield into three categories namely :
  1. Streaming stored audio / video.
  2. Streaming live audio / video.
  3. Interactive audio / video.



(O-261) Fig. 4.5.1 : Classification of internet audio and video services

4.5.1 Streaming :

Streaming is the process in which the user can listen or watch an audio or video file after the downloading has begun.

Streaming stored audio / video :

- In this type of internet service the audio / video files are stored on a server in the compressed form. A user (client) uses Internet to download these stored files, onto his machine.
- The examples of this service are : stored songs, books, educational lectures, movies, TV shows, video clips etc.
- Streamed stored audio / video service is also known as on demand audio / video.

4.5.2 Streaming Live Audio / Video :

- In this category the audio / video information is being streamed live on the Internet and the user is listening / watching the broadcast live.
- The examples of this service are : Internet radio and Internet TV (live cricket match broadcast).
- Note that in the live streaming there is no need to download the stored audio / video files from a server.

4.5.3 Interactive Audio / Video :

- This service enables the users to interactively communicate with each other via Internet. The examples of this service are Internet telephony and internet teleconferencing.
- For all these applications the audio and video information has to be in the digital form. Hence it is necessary to first digitize the sound and video information and then it should be compressed to reduce the bandwidth required to transmit it.

4.5.4 Problems for Multimedia in Today's Internet :

- The protocol used by the Internet is IP. Recall that IP provides the **best effort service** to all the datagrams it carries.
- That means the Internet makes best effort to move each datagram from sender to receiver as quickly as possible.

- But the Internet does not make any promise about end to end delay for an individual packet.
- Same is true for TCP and UDP as they operate on IP.
- As there is no guarantee of delivering the packets in time, it is an extremely challenging problem to develop successful multimedia networking applications for the Internet.
- So multimedia on Internet has not achieved the success that it is expected to get.

4.5.5 Expectations of Multimedia from the Internet :

Different multimedia types have different expectations from the Internet. Some of the important expectations are as follows :

1. Real time characteristics.
2. High bandwidth
3. Multicasting support
4. Error characteristics of the medium
5. Session individuality
6. Security
7. Mobility.

1. Real time characteristics :

- Most multimedia applications have real time traffic requirements. For example, audio and video data must be played back continuously at the rate at which they are sampled.
- If the data does not arrive in time, the playing back process will stop and human ears and eyes can easily pick up the artifact.
- In Internet telephony, human beings can tolerate a latency of ~200 msec. If the latency exceeds this limit, the voice will sound like a call routed over a long satellite circuit and users will complain about the quality of the call.
- Thus a real time traffic requires strict bounds on end-to-end delay and jitter. The time taken by the packet to travel from the source to the destination is the end-to-end delay, while the variability in the inter-packet delay at the receiver is the jitter.
- Performance improves with decrease in both these quantities.

2. High bandwidth requirements :

- Most multimedia applications demand significantly higher bandwidth. For e.g. a PCM encoded voice grade telephone conversation requires a bandwidth of 64 kbps, which is greater than any of the currently available modem speeds.
- Similarly un-encoded video conferencing with a picture size of 1024 × 1024 pixels at 30 frames/sec will require a bandwidth of ~1 Gbps.
- Of course, there are compression techniques that take advantage of spatial and temporal locality present in voice and video, but they still require significantly higher bandwidth than what we have been using in the past.
- The best effort Internet model neither provides any mechanism to demand such high bandwidths nor prevents any one from sending at such high rates. If everyone starts sending at a high rate there will be heavy congestion in the network leading to a congestion collapse that can completely halt the Internet.
- There is no mechanism in the best-effort Internet to prevent this from happening (except using a brute force technique of disconnecting the source of such congestion).
- It is left to the discretion of the application to dynamically adapt to network congestions. Elastic applications do utilize a closed-loop feedback mechanism (built into TCP) to prevent congestion, but RTI and RTT applications cannot use the same feedback techniques, as the resulting delay will significantly degrade performance.
- Thus such applications have the capability to create a congestion collapse. The enhanced Internet service models prevent this by employing admission control mechanisms.
- The application must first get permission from some authority to send traffic at a given rate and with some given characteristics.
- If the authority allows the admission, then the application can send data limited at that rate only. The newer service models employ traffic policing mechanisms to ensure that applications do not violate this contract.

Compression techniques :

There are two kinds of compression techniques :

- Those that loose some information (or lossy compression) and those that do not loose any information (Lossless Compression).
- In lossless compression, the data received by the user are identical to the original data. With lossy compression, some distortion is introduced.
- Lossy compression usually yields significantly higher compression ratios than lossless compression.
- However lossy compression might not be acceptable to all sections of the society (viz. medical specialist).
- Also compression of such huge data sets will increase the packet processing delay.

3. Multicasting support :

- Many multimedia applications, like video/audio conferencing will require the communication network to provide a strong multicasting support.
- The best-effort Internet is sufficiently equipped to handle multicasting, however we wish to make a point that any enhancements to the Internet must also support multicasting.
- In the best-effort Internet, multicasting is achieved by sending packets to a multicast IP address (Class D IP addresses are multicast IP addresses).
- All those receivers that desire to receive the multicast have to register with appropriate routers, which forward any packets that are sent to that address.

Scanned by CamScanner

for the enhanced Internet service models, we expect that the problem of multicasting to be solved along similar principles.

Error characteristics of the medium :

From a receiver's point of view, error occurs when a packet is lost or when it arrives with some bits turned the other way.

Both these events are treated as lost packets in most multimedia applications and suitable actions are taken to overcome them.

Many algorithms are now available that allow such applications to interpolate lost information. In case of wired networks the probability of packet loss is less, while unfortunately the same cannot be said about wireless networks.

So the entire equation of handling lost packets in wireless networks changes. Interesting and complex scenario arise when a multimedia streaming session occurs between a wired host and a mobile host.

Often, the schemes applied to one may not be the optimum choice for the other. For e.g. FEC is most widely used to detect and correct errors in packets. However, FEC requires overhead bits in each packets, which wastes bandwidth. The choice of FEC might seem to be optimum for wireless networks, as this will prevent unnecessary retransmission in case of lost packets (which happen relatively more frequently).

However FEC might not be an optimum choice for wired networks, as the lesser probability of loss does not justify the added overhead.

The best-effort Internet does not provide any information regarding the path over which the packets might travel and their error characteristics. Hence without this feedback, the sender application has no knowledge of the error characteristics of the medium and ends up using error correction/detection mechanism that may not be optimum.

For the newer Internet Service models, as discussed earlier, the sender application has to go through admission control. At that time, the sender can specify the maximum error that it can tolerate.

If the network is unable to find a path that can satisfy this requirement (assuming some QoS based routing is in use), it will just reject the connection or make a counter offer to the sender specifying the error rate at which it is willing to accept the connection. In other words, the sender is made aware of the error characteristics of the medium.

Session Individuality :

A multimedia session might consist of multiple streams that need to be clearly identified. For e.g. the sender might choose to send the audio and video as two separate streams, which the receiver needs to decode synchronously.

Another option might be that the sender might bunch the audio and video streams together, but divide quality into a base layer and some enhancement layers, so that low-bandwidth receivers might be able to receive only the base layer, which high-bandwidth receivers might also receive the enhancement layers.

- In the best-effort Internet, every session can be identified using the tuple <Src Ip, Src Port, Dst IP, Dst Port, Protocol>.
- Thus individual transport layer sockets have to be established for every session. However, if there ever arises a need to bunch sessions together (for cutting costs, say) there is no available mechanism.
- Hence there is clearly a need to multiplex different streams into the same transport layer socket.
- This can be accomplished by having a visible "Session Layer" between the Application and the transport layer (as in the 7-layer OSI model), which has been notably absent in the best effort Internet.
- Apart from identifying the individual streams, the session layer might even insert timing and sequencing information into the stream that facilitates playout at the receiver. RTP and RTCP are two protocols that are most widely used for this purpose.
- While RTP is concerned with identifying individual streams and inserting time stamps, RTCP is used for exchange of commands and responses between the client and the server.
- Note that this is not a major issue, as introducing such a session layer in the best-effort Internet is also a trivial task.

6. Security :

- The security issue has been neglected in almost all discussions of multimedia communication. However, it is now apparent that security needs to be incorporated.
- Security provides the following three aspects to multimedia data: Integrity (data cannot be changed in mid-flight), Authenticity (Data comes from the right source) and Encryption (Data cannot be deciphered by any third party).
- For example, public broadcasts require data integrity and data authenticity, while private communication requires data encryption. All the above aspects can be provided using cryptographic techniques.

7. Mobility :

- Mobility aspect has added another dimension of complexity to multimedia networks. It opens up questions on a host of complex issues like: routing to mobile terminals, maintaining the Quality of Service (QoS) when the host is in motion, inter-networking between wireless and wired networks etc.
- The 3rd generation cellular systems, now offers data communication in addition to voice at rates approaching 384 kbps and it is quite possible to view a low-quality streaming video or listen to a low quality streaming audio file on your cell phone.
- Cellular systems have a large coverage area and hence permit higher mobility.
- Another emerging option is IEEE 802.11b wireless LAN, which can operate at speeds exceeding 54 Mbps. Wireless LANs typically cover a smaller area and hence limit mobility.

- However the main advantage of wireless LANs is that they work in the ISM band, which does not require licensing.
- This eliminates the need to invest significant amounts of money for obtaining a license. Hence wireless LANs can be easily operated by any startup company.
- Also because of its simplicity and availability of cheap products in the market the end cost to the user is lower. It remains to be seen, which system, 3G or wireless LANs will win the race for providing wireless data service.
- Interesting scenarios arise when we think about the internetworking between wireless LANs and cellular systems.
- Due to the vastly different environments on the wired and wireless Internet, application performance degrades and some proxy agents need to be introduced.
- Many projects are researching into extending the newer Internet Service models to be extended to cover wireless networks. It remains to be seen how effective will this models will be.

4.6 Streaming Stored Audio and Video :

- This is the class of applications which allows the clients to request for compressed audio or video files which are stored on the servers.
- Stored audio files may contain educational lectures, songs and other recorded audio stuff.
- Stored video files may contain movies, TV shows, documentaries, cartoons or music video clips.
- This class of applications has three distinguishing factors as follows :
  1. Stored media
  2. Streaming
  3. Continuous playout.

1. Stored media :

- The multimedia content has been prerecorded and stored at the server.
- So it is possible for the user to make following operations on the stored contents :
  1. Pause
  2. Rewind
  3. Fast forward
  4. Index through.

2. Streaming :

- In a streaming stored audio/video applications, a client starts playout of the audio/video a few seconds after receiving the file from the server.
- So the client plays out audio/video from one location in the file when it is receiving later parts of the same file from the server. This technique is called as **streaming.**
- This avoids need to download the entire file before beginning playout.

3. Continuous playout :

- Once the playout of the multimedia content begins, it is necessary to proceed as per the original timing of recording.
- This requirement puts critical delay constraints on data delivery.
- In the recent years audio/video streaming has become a significant user of network bandwidth due to its popularity.
- This popularity is due to many reasons such as :
  1. Cost of disk storage continues to decrease.
  2. Improvement in Internet infrastructure.
  3. Increased demand for high quality video on demand.
- In audio/video streaming, clients request compressed audio/video files which have been stored on servers.
- Such servers can be the ordinary web servers or special streaming servers.
- When the server receives clients request, it directs an audio/video file to the client by sending the file into a socket. Both TCP and UDP socket connections are used in practice.
- Before sending the audio/video files into the network, they are segmented. The segments are then encapsulated with special headers.
- The **real time protocol (RTP)** is the standard used for such an encapsulation.
- The user interactivity also needs a protocol for client/server interaction. The **real time streaming protocol (RTSP)** is used for this purpose.
- The users generally request the audio/video streaming through a browser. But audio/video playout is not integrated directly into today's browser.
- Hence we need to use a separate **helper application** to playout the audio/video.
- Helper applications are also called as **media players.**

4.6.1 Functions Performed by Media Players :

Some of the functions performed by media players are :

1. Decompression
2. Jitter removal
3. Error correction.

1. Decompression :

- Audio/video content are always in the compressed form so as to save the disc space and network bandwidth.
- A media player being on the receiving side should decompress the audio/video.

2. Jitter removal :

- Audio/video are sensitive to the jitter as discussed earlier.
- So the media player must provide a receiver with buffer to remove the jitter.

3. Error correction :

- Due to unpredictable congestion in Internet a part of packet stream may get lost.
- The quality of received audio/video can be seriously affected if the part lost is of large size.
- The errors can be corrected by using the following steps :
  1. By reconstructing lost packets by transmission of

Scanned by CamScanner

redundant packets.

2. By requesting retransmission of lost packets.
3. By interpolating the missing data from the received data.

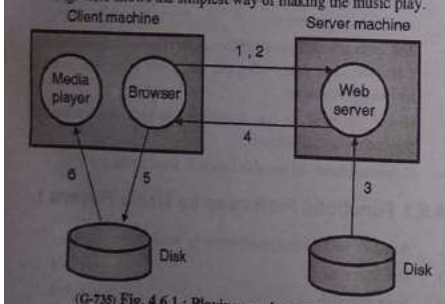
- The media player has a graphical user interface with a control knob. It includes following controls :
  1. Volume controls
  2. Pause/resume buttons
  3. Sliders for making temporal jumps in audio/video stream.

4.6.2 Accessing Audio and Video Through a Web Server :

Stored audio/video is on a web server. It delivers this stored audio/video to the client over HTTP or on an audio/video streaming server.

Streaming Audio :

- Streaming audio means listening to sound over the Internet. This is also called as music on demand.
- The internet consists of many music web sites. Some of them are free sites whereas others require payment.
- Fig. 4.6.1 shows the simplest way of making the music play.



(G-735) **Fig. 4.6.1 : Playing music on a web page**

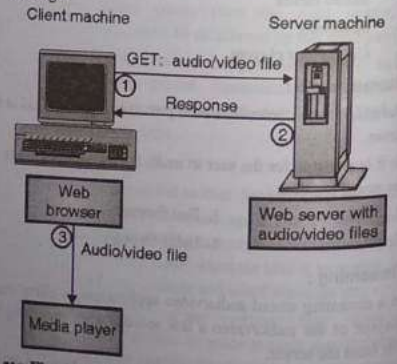
- The steps followed to play the required song is as follows :
  1. Establish TCP connection to the web server.
  2. Send a GET request in HTTP to request the song.
  3. The server fetches the desired song from the disc.
  4. The fetched song is sent back to the browser.
  5. This entire song will be stored on the clients disk as a scratch file.
  6. The media players starts fetching and playing the music block by block.
- Principally there is nothing wrong about the process but practically some problems do arise.
- The main problem is the time required to download a song can be as long as 10 minutes.
- This problem is sorted out by transferring the music line by line and pushing the browser out of the loop.

4.7 Streaming Stored Audio / Video :

- In this type of Internet service the audio / video files are stored on a server in the compressed form. A user (client) uses Internet to download these stored files, onto his machine.
- The examples of this service are : stored songs, books, educational lectures, movies, TV shows, video clips etc.
- Streamed stored audio / video service is also known as on demand audio / video.
- Downloading such types of files from web server may be different from other types of files.
- To know the concept, let us discuss following four approaches with different complexity :
  1. Using a web server.
  2. Using a web server with a metafile.
  3. Using a media server.
  4. Using a media server and RTSP.

4.7.1 Using a Web Server :

- Let us assume that audio and video are contained in one file. The architecture for audio/video streaming is shown in Fig. 4.7.1.
- The client uses the services of HTTP and sends a GET message to download the file.
- The web server sends the compressed file to the client machine (browser) the browser can then use a help application normally "media player" to play the file.
- The browser establishes a TCP connection with a web server and requests the audio/video file with an HTTP request message.



(G-736) **Fig. 4.7.1 : Audio/video streaming using a web server**

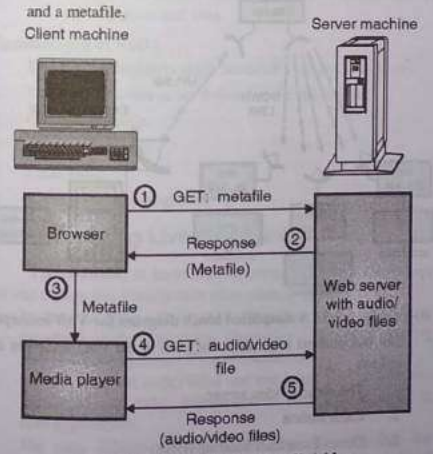
- The web server sends the requested audio/video file to the browser using an HTTP response message.
- The client browser examines the content type of the response message, launches the associated media player and passes the file to the media player.
- The media player then renders the audio/video file.

Drawbacks :

- This is a simple approach but the drawback is that the media player has to interact through the web browser with the web server.
- So the entire object must be downloaded before the browser passes it to the media player.
- This results in an unacceptable amount of delay before playout can begin.
- So the audio/video file should be sent directly to the media player. For this a direct socket connection is made between the server and media player.
- This is done by making use of a **metafile** as shown in Fig. 4.7.1. A **metafile** is the file that provides information about the audio/video file that is to be streamed.

4.7.2 Using a Web Server with a Metafile :

- Refer Fig. 4.7.2.
- A metafile is the file that stores information about the audio and video files.
- In this approach the media player is directly connected to the web server for downloading the audio/video file.
- The web server stores two files. The actual audio/video file and a metafile.



(G-737) **Fig. 4.7.2 : Streamed audio/video using metafiles**

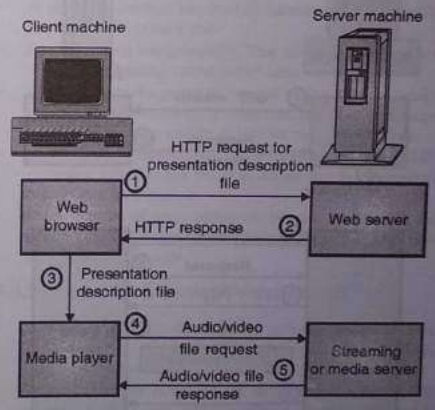
Steps followed :

1. The HTTP client uses the GET message to access the web server.
2. In response we get information about metafiles.
3. The metafile is passed from browser to media player.
4. The URL in the metafile is used by the media player to access the audio/video files.
5. The web server responds and sends the audio/video files directly to the media player.

- Many companies which sell products for audio/video streaming do not recommend the architecture that uses metafiles.
- This is because here, the media player communicates with the server over HTTP and hence also over TCP.
- The interaction with the server using HTTP is not sufficiently rich. It does not allow a user to send pause / resume, fast-forward and temporal jump commands to the server.

4.7.3 Using a Media Server :

- In order to overcome the problem associated with HTTP and TCP the audio/video can be stored on and sent from a streaming server to the media player as shown in Fig. 4.7.3.
- With an additional streaming server the audio/video can be sent over UDP rather than TCP.
- The architecture of Fig. 4.7.3 provides two servers. One is HTTP server and the other is streaming server. The HTTP server serves the web pages (including metafiles) and the second server called streaming server serves the audio/video files.



(G-738) **Fig. 4.7.3 : Audio/Video streaming using media server**

Steps followed :

1. The HTTP client accesses the web server using an HTTP request message.
2. The information about the metafile comes back in the HTTP response.

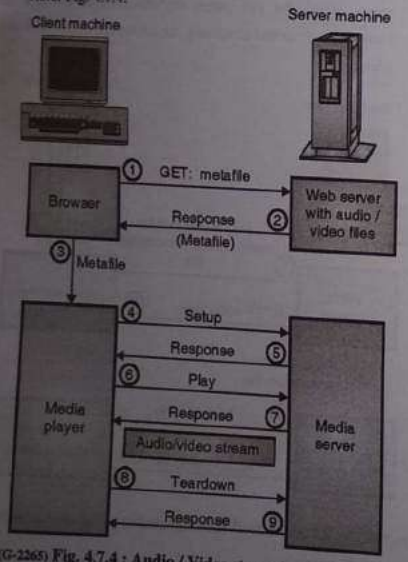
Scanned by CamScanner

3. The metafile is passed to the media player from the web browser.
4. The media player uses the URL in the metafile and accesses the media server to download the file. This downloading can be done with the help of any protocol that uses UDP.
5. The media server responds by sending the audio / video file.

- We needed a media server as we know HTTP is designed to run over TCP and TCP retransmits a lost or damaged segment. Hence we need to avoid TCP and its error control so we need to use UDP.
- However HTTP, which accesses the web server and the web server itself are designed for TCP. So we need another server "Media server".

4.7.4 Using a Media Server and RTSP :

- To add more functionalities to the streaming process, a control protocol RTSP (Real time streaming protocol) is designed.
- With the help of RTSP, the playing of audio/video can be controlled.
- Similar to the second connection in FTP, RTSP is an out of band control protocol.
- Refer Fig. 4.7.4.



(G-2265) **Fig. 4.7.4 : Audio / Video streaming using media server and RTSP**

Steps followed :

The HTTP client uses the GET message to access the web server.

In response we get information about metafiles.

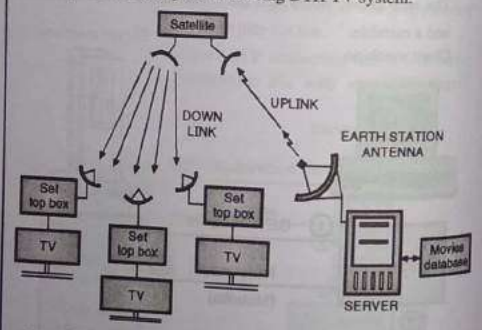
The metafile is passed from browser to media player.

4. To establish connection with the media server, the media player sends **setup** message to media server.
5. The media server responds to media player.
6. To start downloading (playing), the media player sends **play** message to media server.
7. Downloading of audio / video file can be done with the help of any protocol that uses UDP.
8. Media player sends **Teardown** message to breakdown the connection.
9. The media server responds to the media player.

- The media player can send other type of messages such as **pause** to stop the downloading temporarily and **play** to resume the downloading.
- **Video on demand (VOD)** is an example of steaming stored audio/video.

4.7.5 Example : Video on Demand (VOD) :

- Video on Demand (VoD) or movie on demand is basically an interactive multimedia system. VoD works with the DTH TV system and allows the subscriber to select a movie of his choice from a large collection of videos (movies).
- In this system, different subscribers in an area can watch different movies at the same time. Thus the VoD system is analogous to a video retail shop.
- Fig. 4.7.5 shows a simplified block diagram which will explain the concept of VoD using DTH TV system.



(O-132) **Fig. 4.7.5 : A simplified block diagram for VoD concept**

- The components required to be used in the VoD setup are as follows :
  1. The audio / video server.
  2. Earth station
  3. Direct Broadcast Satellite (DBS)
  4. Set to boxes at the subscriber's place
  5. TV receivers

Operation :

- As shown in Fig. 4.7.5 an audio / video server has a database containing the pre recorded videos which are stored in the digitized format.

- Whenever a video is asked for it is first coded and compressed and then transmitted with the help of an earth station parabolic dish antenna to the direct broadcast satellite (DBS). A video is ordered either via interactive voice response or through the call centre of the DTH service provider.
- The DBS simply relays the video content after down converting it to its downlink frequency.
- The set top box will decompress and decode the received video and applies it to the TV receiver for reproduction. The quality of VoD is as good as that of a standard DVD.
- The digital audio / video can be stored on a hard disk of the server by compressing the signal. The DTH network will advertise about the available videos / movies on the DTH network.
- There can be multiple archive servers which contain different data bases present simultaneously in the system. Based on the request made by the subscriber, videos / movies will be accessed at a predetermined time by the DTH service provider.
- VoD can operate on the DTH TV network or on the cable TV network with the help of set top boxes.
- The audio / video servers used in the system should have the following important characteristics :
  1. They should be capable of storing a huge data.
  2. They should allow a simultaneous access to a number of subscribers in real time.

Applications of VoD :

Some of the important applications of VoD are as follows :

1. To provide movies as per demand to the subscribers.
2. Games and music.
3. Weather forecasts.
4. Local news.
5. Remote learning programs.

4.8 Streaming Live Audio and Video :

This is similar to traditional broadcast radio and TV, except for one change that transmission takes place over the Internet.

- In this category, through the Internet a user listens to broadcast audio and video. Examples of streaming live audio/video are Internet TV and Internet radio.
- Streaming stored audio/video and streaming live audio/video are sensitive to delay. Retransmission cannot be accepted in both applications.
- The main difference between both applications is that, the communication is on-demand and unicast in streaming stored audio/video whereas in streaming live audio/video the communication is live and multicast.
- Live streaming use the protocols such as RTP and UDP and they are suitable for the multicast services of Internet protocol (IP).
- Currently instead of multicasting live streaming still uses multiple unicasting and TCP.
- In live streaming there is no need to download the stored audio/video files from a server.
- The examples of streaming live audio/video are discussed as follows.

4.8.1 Example : Internet Radio / Web Radio :

- After it became possible to stream audio over the Internet, commercial radio stations started broadcasting their contents over the Internet.
- There are two general approaches followed. In the first one, the programs are prerecorded and stored on disk.
- Listeners can download any of these programs for listening.
- The other approach is to broadcast live over the Internet. With this technique, buffering on the users side is necessary to smooth out jitter.
- The Internet radio should use multicasting with RTP/RTSP protocols.
- The streaming live audio/video is not stored. Hence a client cannot fast forward through the media.
- Internet radio offers sports, talk and music through the Internet.
- However local storage is always possible, which makes the other interactive applications possible.
- Distribution of live audio/video to many receivers can be accomplished using the IP multicasting technique or using separate unicast streams.
- Internet radio offers sports, talk and music through the Internet.
- A streaming medium involved in Internet radio is accessible from anywhere in the world.
- Internet radio is non-interactive. That means it cannot pause or replay like streaming stored audio/video.
- Over the Internet a group of Internet radio providers consists of radio stations which at the same time broadcast their output traditionally. It also consists of Internet only radio stations.
- In web radio, compression of audio sound takes place by MP3 or similar software and the compressed bits are transported over TCP or UDP packets.
- For prevention of jitter, before the bits are reassembled and played they are buffered and delayed for some time (few second) on the user side.

4.8.2 Example : Internet Television (ITV) :

- Internet TV which is also called as online TV or web TV is the application in which digital TV contents are distributed via the public Internet which is also carrying other type of data.
- The dedicated terrestrial TV or cable TV or satellite TV systems do not carry anything else except the video/audio contents related to television.
- In Internet television, from a library of shows user can choose the show he/she want to watch.

4.8.3 Example : IPTV (Internet Protocol Television) :

- An IPTV (Internet Protocol TV) is a system which is used for delivering the TV services through Internet protocol suite. The TV signal is transferred in the packet form over a packet switched network such as a LAN or the Internet.

Scanned by CamScanner

- This is an alternative way of delivering the TV contents to the user instead of using the means such as the terrestrial TV, satellite or cable TV.
- IPTV allows to stream the contents in small batches directly from the source. This is different from downloading the media.
- The sources of IPTV are classified as follows :
  1. Live TV 2. Time shifted television
  3. Video on Demand (VoD)

The official definition of IPTV according to ITU is, "IPTV is a multimedia service including TV/video/audio /text/graphics/data delivered over IP based networks that are managed to provide the required level of quality of service, experience, safety, interactivity and reliability".

- IPTV is operational in a number of countries including India and the global IPTV subscribers are well over 100 million.
- IPTV is the natural extension of the pay-per view and video on demand concepts. IPTV services are being offered in hotels more than homes.
- In IPTV, audio and video signals are transmitted in the form of IP packets over the IP network such as LAN or Internet.
- The audio and video information is converted into IP packets and routing information is added before transferring the packets onto the Internet or some other data network.
- We can watch IPTV on NTSC or PAL TV set, a multimedia computer, a laptop or a multimedia mobile handset. All these devices can be connected to IPTV programs using a set to box or media gateways supplied by the IPTV service providers.
- In order to watch IPTV, we need to have th following important parts :
  1. Adaptors or viewing devices for converting IP packets to the original audio visual information.
  2. High speed broadband Internet connection.
  3. IPTV service provider.
  4. Media content provider.

9 Real Time Interactive Audio and Video :

In this class of applications, people are allowed to use audio/video to communicate with each other in real time.

Real time interactive audio over the internet is called as **Internet phone**. This can provide local, PBX and long distance telephone service at a very low cost.

This service also facilitates some special services such as :

1. Web phone integration
2. Group real time communication
3. Directory services
4. Caller filtering

Real time interactive video is also called as video conferencing. Here the users communicate visually as well as audibly.

Delays should not be longer than 400 msec.

This is an example of real time interactive audio/video.

Characteristics of real time interactive audio/video :

1. Time relationship 2. Timestamp
3. Playback buffer 4. Ordering
5. Translation 6. Mixing
7. Multicasting

1. **Time relationship :** On a packet switched network, real time data requires protection of the time relationship among the packets of a session.
2. **Timestamp :** We can timestamp the packets for the prevention of jitter and arrival and playback time can be separated.
3. **Playback buffer :** For separation of the arrival time from the playback time, buffer is required to store the data until they are played back. This buffer is known as a **playback buffer**.
4. **Ordering :** To order the packet, a sequence number for each packet is required.
5. **Translation :** Translation is required sometimes for real time traffic. The main function of translator is to change the format of high bandwidth video signal to low quality narrow bandwidth signal.
6. **Mixing :** The traffic with multiple streams are formed if there is more than one source which can send data at the same time. Data from various sources can be mixed to meet the traffic to one stream. For this, mixer is used which mathematically adds signals coming from various sources to from one single signal.
7. **Multicasting :** In case of heavy traffic data can be divided using multicasting methods.

4.10 Forward Error Correction in Real Time Multimedia :

- In real time multimedia transmission, retransmission of lost and corrupted packet is not useful because it generates delay in reproducing the packet. Until the corrupted or lost packet is resent we need to wait.
- It is necessary to correct the error or reproduce the packet instantly. In the case some schemes have been designed known as forward error correction (FEC) technique.

4.10.1 FEC Techniques :

1. Error correction using hamming distance.
2. Error correction using XOR.
3. Chunk Interleaving
4. Combining hamming distance and interleaving.
5. Compounding high and low resolution packets.

4.10.2 Error Correction Using Hamming Distance :

- In chapter 8, we will discuss in detail the concept of hamming distance.
- For detection of 's' errors, the minimum hamming distance should be $d_{min} = s + 1$.

- We need more hamming distance for detection of error. To detect 't' errors, $d_{min} = 2t + 1$
- i.e. If we want to correct 12 bits in a packet, minimum hamming distance $(d_{min}) = [2(12) + 1] = 25$ bits. That means with the data a lot of redundant bits need to be sent.

4.10.3 Error Correction using XOR :

- If exclusive-OR operation is performed on N data items (P_1 to P_N) by ex-oring all the data items we can regenerate any of the data item, replaces the one to be generated by the result of the previous operation (R).
- That means a packet is divided into N chunks, perform the exclusive OR of all chunks and N + 1 chunks are sent.

$$R = P_1 \oplus P_2 \oplus \ldots \oplus P_i \oplus \ldots \oplus P_N$$

$$P_i = P_1 \oplus P_2 \oplus \ldots \oplus R \oplus \ldots \oplus P_N$$

(G-2366) **Fig. 4.10.1 : Exclusive-OR operation**

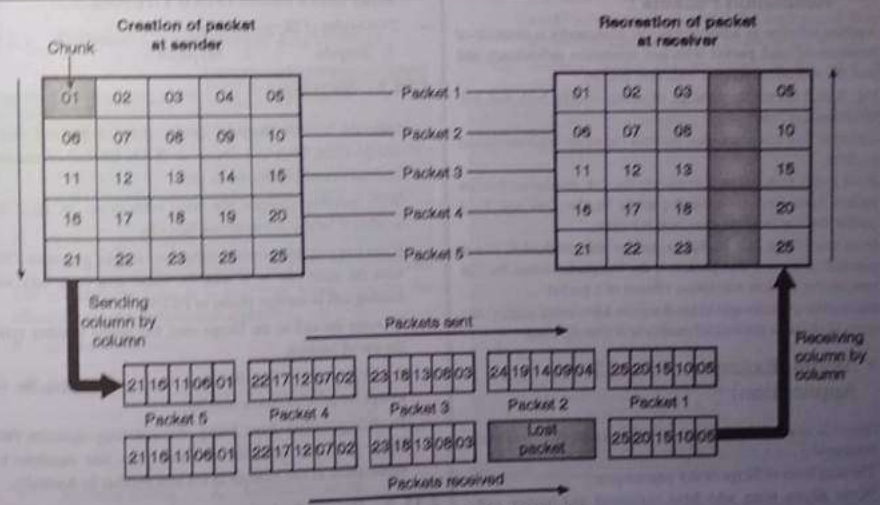
- At the receiver site a chunk is created if any of chunk is corrupted or lost.

4.10.4 Chunk Interleaving :

- Chunk interleaving is another technique to achieve forward error correction in Multimedia.
- This technique allows some small chunks to be missing at the receiver side.
- In each packet if one chunk is missing than can be affordable but all the chunks which belongs into the same packet are missing is not affordable.
- Fig. 4.10.2 shows chunk interleaving. Each packet is divided into 5 chunks. Horizontally we can generate data chunk by chunk. To form the packets chunks are combined vertically.
- Each sent packet contains a chunk from many original packets.
- We miss only one chunk in each packet if any packet is lost which can be acceptable in multimedia communication.

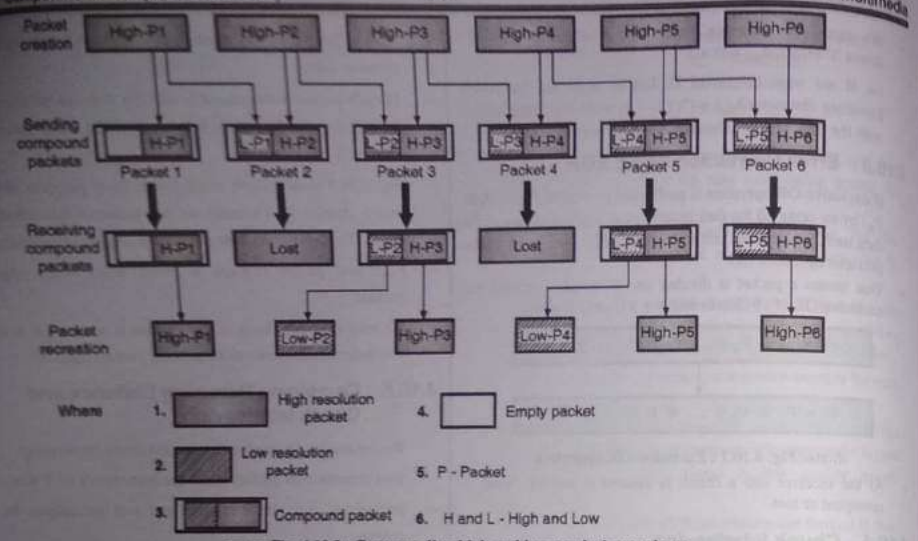
4.10.5 Combining Hamming Distance and Chunk Interleaving :

- We can combine hamming distance and chunk interleaving.
- First generate n-bit packets which can correct error of 't' bits.
- Second 'm' rows are interleaved and sent bits column by column.
- In such a way burst errors upto 'mxt' bit errors are corrected automatically.



(G-2367) **Fig. 4.10.2 : Chunk interleaving**

Scanned by CamScanner



(G-2268) **Fig. 4.10.3 : Compounding high and low resolution packets**

4.10.6 Compounding High and Low Resolution Packets :

- Another solution to achieve FEC in multimedia is creation of duplicate of each packet with low resolution redundancy and join the redundant version with next packet.
- Fig. 4.10.3 shows the concept of compounding high and low resolution packets.
- Generate five low resolution packets out of six high resolution packets.
- If we lost a packet then we can use the low resolution version packet from next compound packet. In the first and third packet the low resolution section is empty.
- Note that if the last packet is lost in this method it is not possible to recover that packet. If the lost packet is not the last one we can use low resolution version of a packet.
- Recreation of audio and video does not have same quality, but most of the time the lack of quality is not recognized.

4.11 Skype (Example of Real Time Application) :

- Skype is one of the leading global Internet communication company.
- The long form of Skype is sky peer-to-peer.
- Skype allows users who have registered and having audio input and output devices on their machines (PCs) to make free calls to other registered user over the Internet.
- Skype provides some other features such as SMS (Short message service), IM (instant messaging), Video conferencing file transfer etc.
- To communication with traditional land-line phones and mobile phones with less charges, services SkypeIn and SkypeOut are used.
- Skype offers free pc-to-pc calls. But Skype is a free-based service when it involves PSTN or a cell phone.
- Two modes of Skype conversation :
  1. SkypeIn 2. SkypeOut

4.11.1 SkypeIn :

- Over the Internet **SkypeIn** service allows registered user to accept a call from cell phone or PSTN on his/her machine. This service offers free voice mail.
- With monthly charges the user subscribers to an online number if he/she wants to use SkypeIn.
- Users can call this number using their mobile phone or PSTN with the same rate as if with the same area code they were making call to another phone or PSTN.
- To route the call to the Skype user, the online number makes the use of Internet.
- A call is costfree for registered user who accepts the call except for price of online number.
- To reduce callers from being charged long distance rates, Skype user can subscribe to more than one number. e.g. subscription to one number in US and another in Australia.

4.11.2 SkypeOut :

- In this service, Skype registered users can make a call from their PC to any cell phone or PSTN anywhere in the world and it pays local rates.
- To use SkypeOut service the user has to buy either Skype credit minutes or monthly subscription.
- User can dial the phone numbers of PSTN or mobile phones from their PCs.

- Skype user pays a small global and local rate for the service plus Skype credit minute cost or monthly subscription rate. In this service user can forward incoming call to their mobile phone.
- One important note about Skype is that it is not a replacement for telephone service and we cannot use Skype emergency situation.

4.12 Optimal Compression :

- If we try to transmit the uncompressed speech or image over a digital network, it requires a large bandwidth.
- The uncompressed speech, video, images etc. need a large memory space for its storage.
- Therefore it is necessary to compress audio, video or data information in order to reduce the bandwidth requirement and storage space.
- There are many compression algorithms available. The general requirements of any compression algorithm are as follows :
  1. It must have an adequately high compression ratio yet the quality of the sound, video or data should not be affected too much.
  2. The compression algorithm should be simple.
  3. The compression technique should not introduce any delay (ideally).

4.12.1 Optimal Compression Algorithms :

MU : May 14, May 15, May 16

University Questions

Q. 1 What is compression ? List different compression algorithms. **(May 14, 3 Marks)**

Q. 2 What is compression ? List different compression algorithm. Why adaptive Huffman coding is used ? **(May 15, 4 Marks)**

Q. 3 What is compression ? List different compression algorithm. **(May 16, 4 Marks)**

- The compression ratio is a parameter which indicates the effectiveness of a compression algorithm.
- It is defined as follows :

$$\text{Compression ratio} = 1 - \frac{\text{Compressed size}}{\text{Uncompressed size}} \times 100\ \%$$

- Two very important and widely used compression algorithms are :
  1. Huffman coding 2. Arithmetic coding
- Two important approaches to the data compression are :
  1. Statistical data compression
  2. Dictionary systems
- Examples of dictionary systems are : LZ77 and LZ78 algorithms.
- For the image compression purpose the widely used compression algorithms are : GIF and JPEG.

4.13 Huffman Coding :

MU : Dec. 15

University Questions

Q. 1 Describe Huffman decoding procedure with example. **(Dec. 15, 10 Marks)**

- The Huffman code is a source code. It is a prefix code as well. Here word length of the code word approaches the fundamental limit set by the entropy of discrete memoryless source.
- This code is "optimum" as it provides the smallest average code word length for a given discrete memoryless source. It encodes each message transmitted by a DMS with different value of number of bits based on their probabilities.
- The Huffman encoding algorithm is as follows :
  1. The source symbols (messages) are arranged in the order of decreasing probability. The two source symbols having the lowest probability are assigned with binary digits 0 and 1.
  2. These two source symbols (messages) are then "combined" into a new source symbol (message) with probability equal to the sum of the two original probabilities. The probability of the new symbol is placed in the list of symbols as per its value.
  3. This procedure is repeated until we are left with only two source symbols (messages) for which a 0 and a 1 are assigned.
  4. The code of each original source symbol is obtained by working backward and tracing the sequence of 0s and 1s assigned to that symbol. (As shown in Ex. 4.13.1).
- The Huffman coding can be shown in the form of an algorithm as follows :

1. List source symbols (messages) in the order of decreasing probability.
   ↓
2. The two source symbols of lowest probability are assigned numbers 0 and 1.
   ↓
3. These two source symbols are combined into a new message.
   ↓
4. The probability of this new message is equal to the sum of probabilities of the two original symbols.
   ↓
5. The probability of this new message is placed in the list according to its value.
   ↓
6. Repeat this procedure until we are left with only two source symbols, for which a 0 and a 1 are assigned.

(E-104)

Ex. 4.13.1 : Consider the five source symbols (messages) of a discrete memoryless source and their probabilities as shown in the Table P. 4.13.1(a). Follow the Huffman's algorithm to find the code words for each message. Also find the average code word length and the average information per message.

Dec. 15, 10 Marks

Scanned by CamScanner

Table P. 4.13.1(a)

Message	m_1	m_2	m_3	m_4	m_5
Probability	0.4	0.2	0.2	0.1	0.1

Soln. :

(a) To find the code word for each message :

Steps to be followed :

Step 1 : Arrange the messages in the order of decreasing probabilities.

Step 2 : Assign numbers 0 and 1 to the two messages having lowest probability.

Step 3 : Combine these two messages into a new message and place this probability in the probability list as per its value.

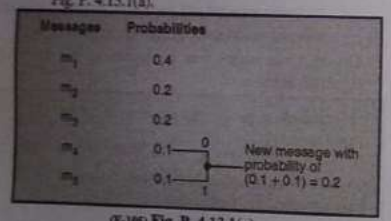
Steps 4 and 5 : Repeat this procedure.

Step 6 : Write the code word for each message by tracking back from the last stage to the first stage.

Let us find code word for each message by following the Huffman's algorithm in steps :

Step 1 : Arrange the given messages in the order of decreasing probabilities as shown in Fig. P. 4.13.1(a).

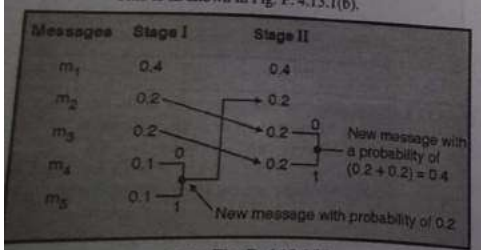
Step 2 : The two messages having lowest probability are assigned 0 and 1. The two messages with lowest probabilities are m_4 and m_5 as shown in Fig. P. 4.13.1(a).



(E-105) **Fig. P. 4.13.1(a)**

Step 3 : Now consider that these two messages m_4 and m_5 as being combined into a new message (Fig. P. 4.13.1(a)) and place the probability of the new combined message, in the list according to its value.

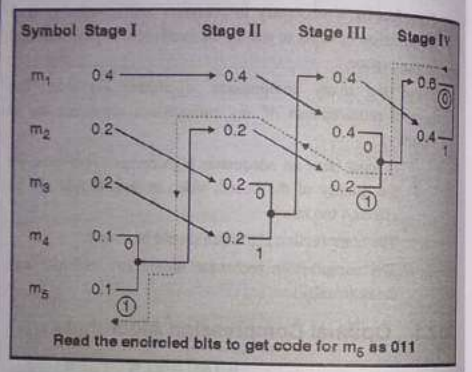
Place the combined message as high as possible when its probability is equal to that of the other messages. This is as shown in Fig. P. 4.13.1(b).



(E-106) **Fig. P. 4.13.1(b)**

Step 4 : Now consider the two messages of lowest probabilities in stage II of the Fig. P. 4.13.1(b). Assign 0 and 1 to these two messages. Consider that these two messages are combined to form a new message with a probability of (0.2 + 0.2) = 0.4. Place the probability of the combined message according to its value in stage III. Place it as high as possible if the other messages have the same probability. This is as shown in Fig. P. 4.13.1(b).

Step 5 : Follow the same procedure till only two messages remain and assign the 0 and 1 for them. All this is as shown in Fig. P. 4.13.1(c).



(E-107) **Fig. P. 4.13.1(c)**

Step 6 : How to write the code word for a message ?

Consider the dotted path shown in Fig. P. 4.13.1(c). To write the code for message m_5 this path is to be used. Start from stage IV and track back upto stage I along the dotted path. And write down the code word in terms of 0s and 1s starting from stage IV.

The code word for message m_5 is 0 1 1.

Similarly write code words for the other messages as shown in Table P. 4.13.1(b).

Table P. 4.13.1(b)

Messages	m_1	m_2	m_3	m_4	m_5
Probabilities	0.4	0.2	0.2	0.1	0.1
Code words	00	10	11	010	011

(b) To find the average code word length :

The average code word length is given as,

$$L = \sum_{k=1}^{5} P_k \text{ [Length of } m_k \text{ in bits]}$$

$$= (0.4 \times 2) + (0.2 \times 2) + (0.2 \times 2) + (0.1 \times 3) + (0.1 \times 3) = 2.2$$

(c) To find the entropy of the source :

The entropy of the source is given as,

$$H = \sum_{k=1}^{5} p_k \log_2 (1 / p_k)$$

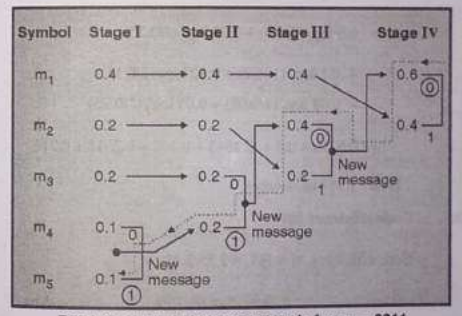
$$H = 0.4 \log_2 (1 / 0.4) + 0.2 \log_2 (1 / 0.2) + 0.2 \log_2 (1/0.2) + 0.1 \log_2 (1/0.1) + 0.1 \log_2 (1/0.1)$$

$$= 0.52877 + 0.46439 + 0.46439 + 0.33219 + 0.33219$$

$$\therefore H = 2.12193$$

Ex. 4.13.2 : Consider the same memoryless source as in Ex. 4.13.1, all the data is same. Find the Huffman code by moving the probability of the combined message as low as possible. Tracking backwards through the various steps find the code words of this second Huffman code.

Soln. : All the steps to be followed are same as those followed for the Huffman's first code explained in Ex. 4.13.1, except for the change that the combined message is to be placed as low as possible. This is as shown in Fig. P. 4.13.2.



(E-108) **Fig. P. 4.13.2 : Huffman's second code**

To find code word : This procedure is same as that followed in the previous example. Follow the dotted path in Fig. P. 4.13.2 to obtain the code for message m_5 as,

Code word for the message m_5 is 0 0 1 1.

Similarly the code words for the other messages can be obtained. They are as listed below :

Messages	Probability	Code word
m_1	0.4	1
m_2	0.2	0 1
m_3	0.2	0 0 0
m_4	0.1	0 0 1 0
m_5	0.1	0 0 1 1

Note that to transmit the same messages as those of the previous example now we need more number of bits per message.

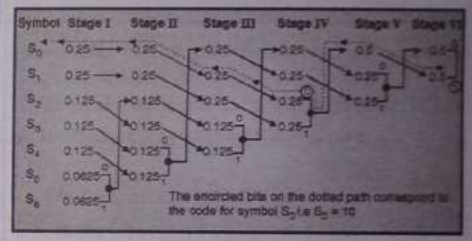
Ex. 4.13.3 : A discrete memoryless source has an alphabet of seven symbols with probabilities for its output as described in Table P. 4.13.3(a).

Table P. 4.13.3(a)

Symbol	S_0	S_1	S_2	S_3	S_4	S_5	S_6
Probability	0.25	0.25	0.125	0.125	0.125	0.0625	0.0625

Compute the Huffman code for this source moving the "combined" symbol as high as possible. Explain why the computed source code has an efficiency of 100 percent.

Soln. : The Huffman code for the source alphabets is as shown in Fig. P. 4.13.3.



(E-109) **Fig. P. 4.13.3 : Huffman code**

Follow the path indicated by the dotted line to obtain the code word for symbol S_0 as 10. Similarly we can obtain the code words for the remaining symbols. These are as listed in Table P. 4.13.3(b).

Table P. 4.13.3(b)

Symbol	Probability	Code word	Code word length
S_0	0.25	10	2 bit
S_1	0.25	11	2 bit
S_2	0.125	001	3 bit
S_3	0.125	010	3 bit
S_4	0.125	011	3 bit
S_5	0.0625	0000	4 bit
S_6	0.0625	0001	4 bit

To compute the efficiency :

1. The average code length = L

$$= \sum_{k=0}^{6} P_k \times \text{(length of symbol in bits)}$$

From Table P. 4.13.3(b)

$$L = (0.25 \times 2) + (0.25 \times 2) + (0.125 \times 3) \times 3 + (0.0625 \times 4) \times 2$$

$$\therefore L = 2.625 \text{ bits/symbol}$$

2. The average information per message = H

Scanned by CamScanner

$$= \sum_{i=0}^{6} p(x_i)\log_2[1/p(x_i)]$$

$$\therefore \quad H = [0.25\log_2(4)]\times 2 + [0.125\log_2(8)]\times 3 + [0.0625\log_2(16)]\times 2$$

$$= [0.25\times 2\times 2] + [0.125\times 3\times 3] + [0.0625\times 4\times 2]$$

$$\therefore \quad H = 2.625 \text{ bits/message.}$$

3. Code efficiency $\eta = \frac{H}{L}\times 100 = \frac{2.625}{2.625}\times 100$

$$\therefore \quad \eta = 100\%$$

Note : As the average information per symbol (H) is equal to the average code length (L), the code efficiency is 100%.

Ex. 4.13.4 : Use the Huffman coding for data compression. For a discrete memoryless source X with six symbols $x_1, \ldots, x_6$, find a compact code for every symbol if the probability distribution is as follows :

$p(x_1) = 0.30$, $p(x_2) = 0.25$, $p(x_3) = 0.20$,

$p(x_4) = 0.12$, $p(x_5) = 0.08$, $p(x_6) = 0.05$

Calculate entropy of the source, average length of the code, efficiency and redundancy of the code. **May 14, 10 Marks**

Soln. :

Part I : Huffman coding :

The codeword for the symbol x_1 is 00 (see dotted line). Similarly the codewords for the other symbols are as listed in Table P. 4.13.4(b).

Table P. 4.13.4(b)

Symbol	x_1	x_2	x_3	x_4	x_5	x_6
Probability	0.3	0.25	0.2	0.12	0.08	0.05
Codeword	00	10	11	011	0100	0101
Codeword length	2	2	2	3	4	4

1. **Average codeword length (L) :**

$$L = \sum_{k=1}^{6} p_k \text{ (Length of } k^{th} \text{ codeword)}$$

$$= (0.3\times 2) + (0.25\times 2) + (0.2\times 2) + (0.12\times 3) + (0.08\times 4) + (0.05\times 4)$$

$$L = 2.38 \text{ bits /message}$$

2. **Average information per message OR source entropy (H)**

$$H = \sum_{k=1}^{6} p_k \log_2(1/p_k)$$

$$= 0.3\log_2(1/0.3) + 0.25\log_2(1/0.25) + 0.2\log_2(1/0.2) + 0.12\log_2(1/0.12) + 0.08\log_2(1/0.08) + 0.05\log_2(1/0.05)$$

$$= 0.5210 + 0.5 + 0.4643 + 0.367 + 0.2915 + 0.216$$

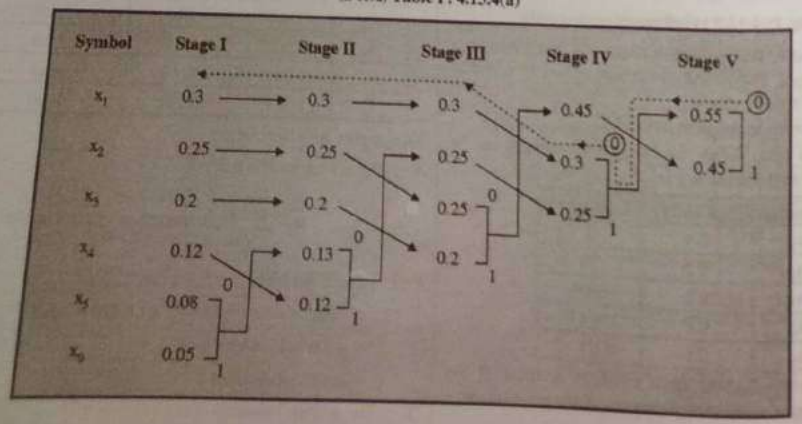
$$\therefore \quad H = 2.35 \text{ bits /symbol.}$$

3. **Code efficiency (η) :**

Code efficiency $\eta = H/L = 2.35/2.38$

$= 0.9915$ or 99.15% Ans.

(E-1192) **Table P. 4.13.4(a)**



Ex. 4.13.5 : Consider a DMS with source probabilities {0.20, 0.20, 0.15,0.15,0.10, 0.10,0.05,0.05} Determine the Huffman code for this source. **Dec. 14, 10 Marks**

Soln. :

Huffman code : The coding is as shown in Fig. P. 4.13.5.

Similarly we can obtain the codes for all other messages. They are listed in Table P. 4.13.5.

Table P. 4.13.5

Message	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8
Code	11	000	001	010	100	101	0110	0111

Ex. 4.13.6 : Given $x_i = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}$ with probabilities as below :

$P(x_i) = \{0.3, 0.25, 0.2, 0.06, 0.04, 0.05, 0.06, 0.04\}$

1. Determine the efficient fixed length code for the source
2. Determine the Huffman code for this source
3. Compare the two codes and comment. **May 15, 10 Marks**

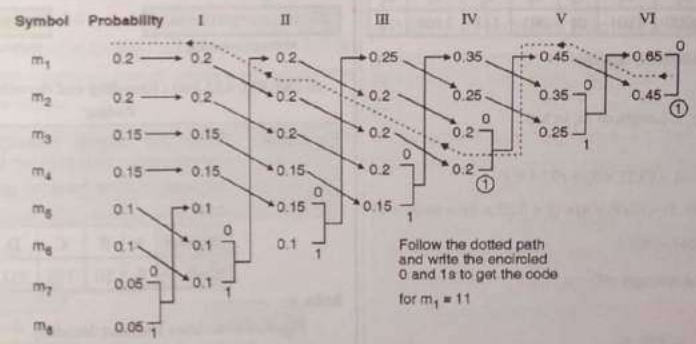
Soln. :

Step 1 : Obtain the codewords :

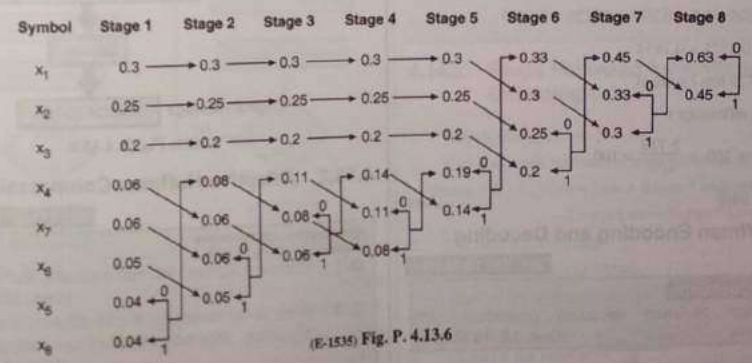
Refer Fig. P. 4.13.6. The codewords for various messages are obtained from Fig. P. 4.13.6 and they are listed in Table P. 4.13.6.

Codeword for various messages are as given in Table P. 4.13.6.

Message	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
Probability	0.3	0.25	0.2	0.06	0.04	0.05	0.06	0.04
Codewords	01	10	11	0011	00010	00001	00000	00011
Codeword length	2	2	2	4	5	5	5	5

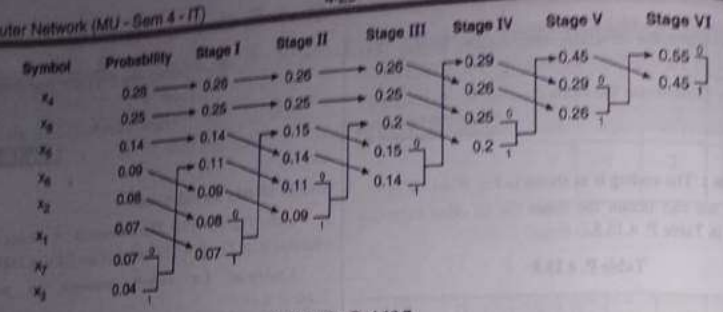


(E-1194) **Fig. P. 4.13.5**



(E-1535) **Fig. P. 4.13.6**

Scanned by CamScanner



(G-1901) Fig. P. 4.13.7

Ex. 4.13.7 : Construct Huffman code for the given symbols $\{x_1, x_2, ..., x_8\}$ with probabilities $P(x) = \{0.07, 0.08, 0.04, 0.26, 0.14, 0.09, 0.07, 0.25\}$. Find coding efficiency.

May 16, 10 Marks

Soln. :

Step 1 : Obtain the codewords :

Table P. 4.13.7

Symbol	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
Code	0001	0000	1101	01	001	111	1100	10

Step 2 : Average codeword length :

$$L = \sum_{k=1}^{8} p_k \times \text{Length of } m_k \text{ in bits}$$

$$\therefore L = (0.26 \times 2) + (0.25 \times 2) + (0.14 \times 3) + (0.09 \times 3) + (0.08 \times 4) + (2 \times 0.07 \times 4) + (0.04 \times 4)$$

$$\therefore L = 2.75 \text{ bits / symbol}$$

Step 3 : Find source entropy (H) :

$$H = -\sum_{k=1}^{8} p_k \log_2 p_k$$

$$= 0.505 + 0.5 + 0.397 + 0.3126 + 0.2915 + 0.5371 + 0.1858$$

$$= 2.729 \text{ bits / symbol}$$

Step 4 : Coding efficiency :

$$\% \eta = \frac{H}{L} \times 100 = \frac{2.729}{2.75} \times 100$$

$$\% \eta = 99.24\%$$

...Ans.

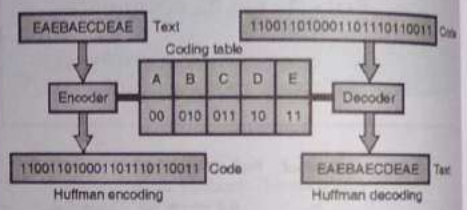
4.13.1 Huffman Encoding and Decoding :

Dec. 15, 10 Marks

University Questions

Q. 1 Describe Huffman decoding procedure with example. **(Dec. 15, 10 Marks)**

- Let us see how to encode and decode text using the code for five characters.
- Fig. 4.13.1(a) shows encoding and decoding using Huffman coding with the help of Table 4.13.1.



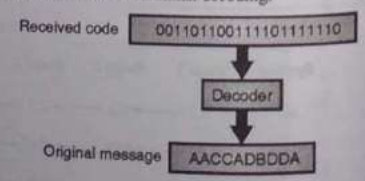
(G-2269) **Fig. 4.13.1(a) : Encoding and decoding in Huffman coding**

Ex. 4.13.8 : Show the original message if the code "0011011001111011111110" is received if the following coding table is given in Huffman coding.

Symbol	A	B	C	D
Code	0	10	110	111

Soln. :

Fig. P. 4.13.8 shows Huffman decoding.



(G-2270) **Fig. P. 4.13.8**

4.13.2 Adaptive Huffman Compression :

MU : Dec. 14, May 15

University Questions

Q. 1 Explain adaptive Huffman encoding technique. **(Dec. 14, 5 Marks)**

Q. 2 What is compression ? List different compression algorithm. Why adaptive Huffman coding is used ? **(May 15, 4 Marks)**

In order to overcome the drawbacks of basic Huffman algorithm; adaptive Huffman algorithm is used.

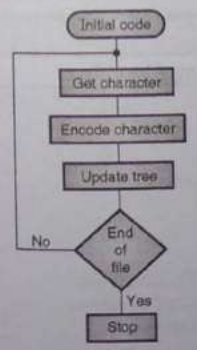
Drawbacks of basic Huffman algorithm :

1. The statistical knowledge of the data to be compressed; is required. That means in some applications live audio, live video is required. But in many cases this data is not available.
2. Many times, the probability of current symbol is dependent on the probability of previous symbol. So, Huffman's compression becomes tedious.
3. The knowledge of the data from the compressed file is required; for the data to be compressed. So, for the encoding of file more memory space is required.

Adaptive algorithm :

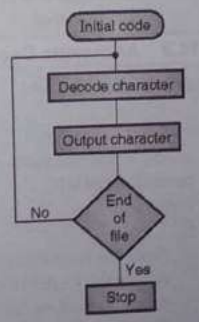
- In adaptive algorithm; sibling property is used. It states that, the nodes can be listed in the order of increasing weight and every node appears adjacent to its sibling.
- In this algorithm; the statistics are collected and dynamically updated every time.
- Based on the knowledge of frequency counts; initial code is assigned to each symbol.
- "update-tree" is used to construct adaptive Huffman's tree. It increments the frequency count of symbols and updates the configuration of tree.
- For every node, a number is assigned from left to right and top to bottom. Every time a sibling property is maintained.
- If any node violets the sibling property then swapping is done.
- The flow graph is shown in Figs. A and B.

Encoder :



(E-1199) **Fig. A**

Decoder :



(E-1200) **Fig. B**

- Basically encoding starts with empty Huffman tree. The first symbol is added to the tree and a code is assigned to it.
- When this symbol appears next time; its present code is generated as output. Then its frequency is incremented by 1. This will modify the tree.
- But every time, the tree is modified. So that it will be Huffman's tree.
- All the nodes having same weight are considered to belong to one block.

4.14 Arithmetic Coding :

- In the compression methods discussed earlier, each sequence of symbol or symbol is encoded separately. A small interval [0, 1) is used in an arithmetic coding, an entire message is mapped into this small interval.
- Arithmetic coding is based on the concept of interval subdivision.
- In this technique, we can have infinite number of small intervals inside the half-open interval [0, 1).

Arithmetic encoding :

- In arithmetic coding, to encode a message, we need to assign probability of occurrence of each symbol. If we have M number of symbols with probability $P_1, P_2, ..., P_M$ in which $P_1 + P_2 + ... + P_M = 1$
- Assign non-overlapping intervals on the [0, 1) axis for each symbol. The length of each interval must be proportional to the probability of the corresponding symbol.

4.14.1 Arithmetic Encoding Algorithm :

```
Arithmetic Encoding (message)
{
    current←interval L = 0.0, H = 1.0 ;
    while (more symbols in the message)
    {
        s = Input (next symbol);
        divide current Interval into subintervals
        subInter = subInterval related to s
        currentInterval = subInter
    }
    Output (bits related to the current interval);
}
```

4.14.2 Steps Followed for Arithmetic Encoding :

1. Initialization : L = 0, H = 1
2. Calculate code subinterval using formulae given below.
   Range = H – L, High = Low + Range * highvalue of symbol
   Low = Low + Range * Lowvalue of symbol
3. Get next input symbol.
4. Update the code subinterval.
5. Until all the sequence has been encoded, repeat steps 2, 3 and 4
6. Choose a tag value = $\frac{\text{Low + high}}{2}$

Scanned by CamScanner

Arithmetic encoding example :

Ex. 4.14.1 : Consider A = {a, b, c, d} with P = {0.4, 0.3, 0.2, 0.1}

Encode the message sequence "bcab".

Soln. :

Symbol	Probability	Interval Q (x – 1), Q (x)
a	0.4	0, 0.4
b	0.3	0.4, 0.7
c	0.2	0.7, 0.9
d	0.1	0.9, 1

1. Initialize the current interval [0, 1)
2. Given message = "bcab"

Input 'b' :

- Subdivision of current interval (0.4, 0.7) takes place with the help of formula given below.

High = Low + Range * highvalue of symbol

Table P. 4.14.1(a) shows subdivision of interval (0.4, 0.7).

Table P. 4.14.1(a)

Symbol	Value	Interval
a	$0.4 + (0.3 \times 0.4) = 0.52$	(0.4, 0.52)
b	$0.4 + (0.3 \times 0.7) = 0.61$	(0.52, 0.61)
c	$0.4 + (0.3 \times 0.9) = 0.67$	(0.61, 0.67)
d	$0.4 + (0.3 \times 1) = 0.7$	(0.67, 0.7)

Input 'c' :

- Table P. 4.14.1(b) shows subdivision of interval (0.61, 0.67).

Table P. 4.14.1(b)

Symbol	Value	Interval
a	$0.61 + (0.06 \times 0.4) = 0.634$	0.61, 0.634
b	$0.61 + (0.06 \times 0.7) = 0.652$	0.634, 0.652
c	$0.61 + (0.06 \times 0.9) = 0.664$	0.652, 0.664
d	$0.61 + (0.06 \times 1) = 0.67$	0.664, 0.67

Input 'a' :

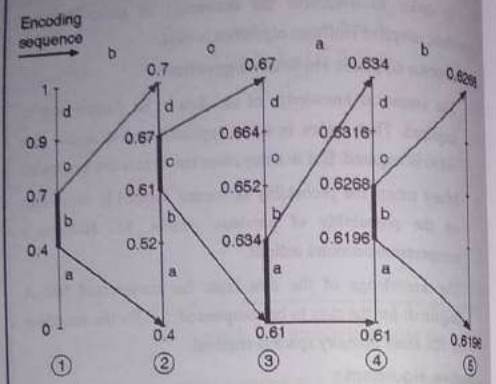
- Table P. 4.14.1(c) shows subdivision of interval (0.61, 0.634).

Table P. 4.14.1(c)

Symbol	Value	Interval
a	$0.61 + (0.024 \times 0.4) = 0.6196$	0.61, 0.6196
b	$0.61 + (0.024 \times 0.7) = 0.6268$	0.6196, 0.6268
c	$0.61 + (0.024 \times 0.9) = 0.6316$	0.6268, 0.6316
d	$0.61 + (0.024 \times 1) = 0.634$	0.6316, 0.634

Input 'b' :

- The final sequence interval is [0.6196, 0.6268).
- This process is described graphically in Fig. P. 4.14.1.



(G-2271) **Fig. P. 4.14.1 : Encoder**

5. The tag value is calculated as average of lower and upper limits.

$$\text{Tag value} = \frac{0.6196 + 0.6268}{2}$$

$$\text{Tag value} = 0.6232$$

6. This tag value is then converted into binary which is approximately $(0.10011111)_2$ but as a code we keep only fractional part i.e. $(10011111)_2$.

Note : We may get an infinite number of bits if we change a real number between 0 and 1 to binary. To recover the original message we have to keep enough bits. Few bits than enough bits may results in wrong decoding whereas encoding is not efficient if we use more than enough bits. Suppose in this example if we use only three bits (100), it represents real value 0.5 which is not in the range of current interval [0.6196, 0.6268). If we use nine bits (100111111), it represents real value 0.6542 which is also not in the range of current interval.

4.14.3 Arithmetic Decoding Algorithm :

```
ArithmeticDecoding (code)
{
    c = Input (givencode)
    number = find real number related to code
    currentInterval = [0, 1) ;
    while (true)
    {
        divide the currentInterval into subInterval;
        subInterval = subInterval related to number;
        output (symbol related to subInterval);
        if (symbol is terminating)
        return;
        currentInterval = subInterval;
    }
}
```


4.14.4 Steps Followed for Arithmetic Decoding :

- The working of decoder is just opposite to the encoder.
- It first gets the number and looks for the interval in which it fits.
- The first symbol is now determined according to its interval.
- Now new range is calculated according to the found symbol and new value should be modified.
- The modification is done with the help of following formula.

$$\text{Modified value} = \frac{\text{New value} - \text{Low value of symbol}}{\text{Range (High value} - \text{Low value)}}$$

- Look at new value again and see in which interval it fits.
- Repeat the same procedure till the termination of symbol.
- We can continue decoding as long as required. When we reach the number of encoded symbol, we should stop the decoding.

Arithmetic decoding example :

Ex. 4.14.2 : Decode the message given in Ex. 4.14.1.

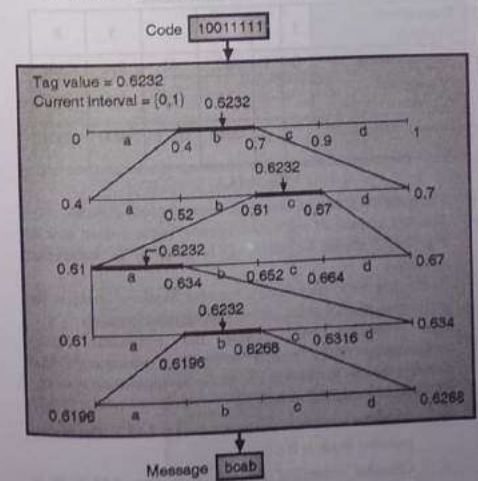
Soln. :

Table P. 4.14.2 shows the decoding process.

Table P. 4.14.2

Value	Output symbol	Low	High	Range (H – L)	New value
0.6232	b	0.4	0.7	0.3	$\frac{0.6232 - 0.4}{0.3} = 0.744$
0.744	c	0.7	0.9	0.2	$\frac{0.744 - 0.7}{0.2} = 0.22$
0.22	a	0	0.4	0.4	$\frac{0.22 - 0}{0.4} = 0.55$
0.55	b	0.4	0.7	0.3	$\frac{0.55 - 0.4}{0.3} = 0.5$

If we use the arithmetic encoder obtained in Ex. 4.14.1, arithmetic decoder is as shown in Fig. P. 4.14.2.



(G-2272) **Fig. P. 4.14.2 : Decoder**

Ex. 4.14.3 : In arithmetic coding, assume that we have received the code 100110010. If we know that the alphabet is made of four symbols with the probabilities of P(A) = 0.4, P(B) = 0.3, P(C) = 0.2 and P(*) = 0.1. Find the original message.

Soln. :

Table P. 4.14.3(a)

Symbol	Probability	Interval
A	0.4	0, 0.4
B	0.3	0.4, 0.7
C	0.2	0.7, 0.9
*	0.1	0.9, 1.0

Step 1 : Convert given binary code into decimal.

Binary : 0.100110010

Decimal : $0.2^{-1} + 2^{-4} + 2^{-5} + 2^{-8} = 0.5976$

Step 2 : Decoding process

Table P. 4.14.3(b) shows decoding process.

Table P. 4.14.3 (b)

Value	Output symbol	Low	High	Range	New Value
0.5976	B	0.4	0.7	0.3	$\frac{0.5976 - 0.4}{0.3} = 0.6586$
0.6586	B	0.4	0.7	0.3	$\frac{0.6586 - 0.4}{0.3} = 0.862$
0.862	C	0.7	0.9	0.2	$\frac{0.862 - 0.7}{0.2} = 0.81$
0.81	C	0.7	0.9	0.2	$\frac{0.81 - 0.7}{0.2} = 0.55$

∴ Obtained original message is "BBCC".

4.15 Dictionary Based Compression :

- The statistical models generally encode a single symbol at a time into a single code. But a dictionary based compression scheme uses a different concept.
- It reads the input data and looks for groups of symbols that appear in a dictionary.
- If a string of such symbols is found, a pointer or index into the dictionary can be output instead of the code for each symbol. The longer the string, the better is the compression ratio.
- The dictionary compression technique generally uses simple coding techniques.

Scanned by CamScanner

- The static dictionary is used like the list of references in an academic paper. But the problem with a static dictionary is that the dictionary needs to be transmitted alongwith the text. But this problem could be solved by using the adaptive dictionary scheme.
- The example of adaptive dictionary scheme is the Lampel and Ziv compression technique.

4.15.1 Lempel ZIV Coding :

- The major disadvantage of the Huffman code is that the symbol probabilities must be known or estimated if they are unknown.
- In addition to this, the encoder and decoder must know the coding tree.
- Moreover when text messages are to be modelled using Huffman coding, the storage requirements do not allow this code to capture the higher order relationship between words and phrases.
- So we have to compromise the efficiency of code.
- These practical limitations of Huffman code can be overcome by using the Lempel ZIV algorithm.
- The advantages of Lempel ZIV algorithm are its adaptability and simplicity of implementation.

Principle of Lempel ZIV algorithm :

> The encoding in this algorithm is done based on parsing the source data stream into segments that are the shortest substances not encountered previously.

Encoding :

- To illustrate this principle let us consider the example of an input binary sequence specified as :

  00010101001

- It is assumed that the binary symbols 0 and 1 have already been stored in this order in the code book.

  Hence we write,

  Subsequences stored : 0, 1

  Data to be parsed : 00010101001 ...(4.15.1)

- Now start examining the data in Equation (4.15.1) from LHS and find the shortest subsequence which is not encountered previously.
- This subsequence cannot be only 0 because it has already been encountered. It is 00. So we include 00 as the next entry in the subsequence and move 00 from Data to subsequence as follows :

  Subsequences stored : 0, 1, 00

  Data to be parsed : 010101001 ...(4.15.2)

- The next shortest subsequence which is not previously repeated is 01. in Equation (4.15.2). Note that we are examining from LHS. Hence we write,

  Subsequences stored : 0, 1, 00, 01

  Data to be parsed : 0101001 ...(4.15.3)

- The next shortest subsequence which is previously not encountered is 010. Note that it can't be 01 because we have already stored it. Hence we write,

  Subsequences stored : 0, 1, 00, 01, 010

  Data to be parsed : 0101

- Similarly we can continue until the data stream has been completely parsed. The code book of binary subsequences gets ready as shown in Fig. 4.15.1.

Numerical position	1	2	3	4	5	6
Subsequences	0	1	00	01	010	0101

Fig. 4.15.1 : Code book of sequences

- The first row in the codebook shows the numerical positions of various subsequences in the codebook.

Numerical representation :

- Let us now add third row to Fig. 4.15.1. This row is called as numerical representation, as shown in Fig. 4.15.2.

Numerical position	1	2	3	4	5	6
Subsequences	0	1	00	01	010	0101
Numerical representations			11	12	41	44

Fig. 4.15.2

- The subsequences 0 and 1 are originally stored. So consider the third subsequence i.e. 00. This is the first subsequence in the data stream and it is made up of concatenation of the first subsequence i.e. 0 with itself.
- Hence it is represented by 11 in the row of numerical representation in Fig. 4.15.2.
- Similarly, subsequence 01 is obtained by concatenation of first and second subsequence so we enter 12 below that.
- The remaining subsequences are treated accordingly.

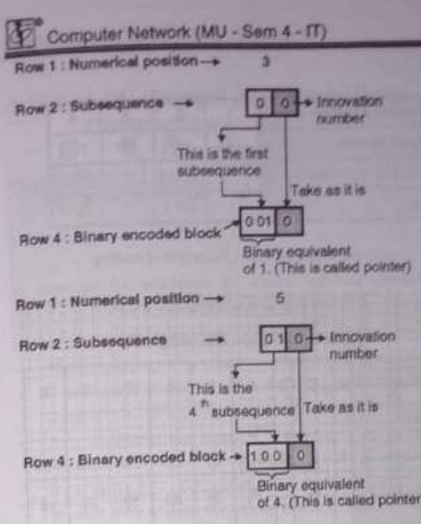
Binary encoded representation :

- The last (4th) row added as shown in Fig. 4.15.3, is the binary encoded representation of each subsequence.

Numerical position	1	2	3	4	5	6
Subsequences	0	1	00	01	010	0101
Numerical representations			11	12	41	44
Binary encoded blocks			0010	0011	1000	0100

Fig. 4.15.3

- The question is how to obtain the binary encoded blocks.
- The last symbol of each subsequence in the second row of Fig. 4.15.3 (called as codebook) is called as an **innovation symbol.**
- So the last bit in each binary encoded block (4th row) is the innovation symbol of the corresponding subsequence.
- The remaining bits provide the equivalent binary representation of the "pointer" to the "root subsequence" that matches the one in question except for the innovation symbol.
- This can be explained as follows :
  1. Consider numerical position 3 in Fig. 4.15.3. The binary encoded block is 0010.
  2. Consider numerical position 5 in Fig. 4.15.3. It is partially reproduced below.



Similarly the other entries in the fourth row are made. In this way we get the binary encoded version of the original sequence using LZ algorithm.

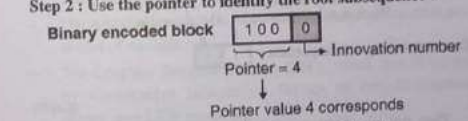
Decoder :

- The decoding is as simple as encoding. The steps followed at the time of decoding are as follows :

Step 1 : Take the binary encoded block :

For example consider the binary encoded block in position 5 i.e. 1000.

Step 2 : Use the pointer to identify the root subsequence :



Step 3 : Append the innovation symbol to the subsequence in step 2 :

- Append the innovation number i.e. 0 to the root subsequence of 01 to get the subsequence 010 corresponding to position 5.
- This is how the process of decoding can be used to recover the original bit sequence from the LZ encoded signal.

Ex. 4.15.1 : Determine the Lempel-Ziv code for the following bit stream :

1001111100101000001010101100110000

Recover the original sequence from the encoded stream.

Soln. :

Part I : Encoding :

- We assume that the binary symbols 0 and 1 are already stored in the code book.

  ∴ Subsequences stored : 0, 1

- Encoding is accomplished by parsing the source data stream into segments that are shortest substances, not encountered previously.
- The given stream of bits can be parsed into subsequences as shown below :

  0, 1, 00, 11, 111, 001, 01, 000, 0010, 10, 101, 100, 110, 000

- These subsequence are encoded as shown in Fig. P. 4.15.1.

Numerical position	1	2	3	4
Subsequences	0	1	0 0	1 1
Numerical representation	–	–	1 1	2 2
Code	0	1	0010	0101

(E-1674) **Fig. P. 4.15.1**

- Using the same technique we can encode the remaining subsequences as shown in the encoding table of Table P. 4.15.1(a).
- The required LZ code is as written in the last row of Table P. 4.15.1(a).

(E-159) **Table P. 4.15.1(a) : Encoding table**

Numerical position	1	2	3	4	5	6	7	8	9	10	11	12
Subsequences	0	1	00	11	111	001	01	000	0010	10	101	100
Numerical representation	–	–	11	22	42	32	12	31	61	21	102	100
Code	0	1	0010	0101	1001	0111	0011	0110	1100	0100	10101	10100

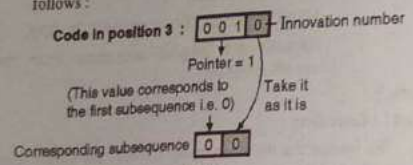
(E-161) **Table P. 4.15.1(b) : Decoding table**

Code	0010	0101	1001	0111	0011	0110	1100	0100	10101	10100
Innovative bit	0	1	1	1	1	0	0	0	1	0
Pointer	001	010	100	011	001	011	110	010	1010	1010
Decoded subsequence	0 0	1 1	1 1 1	0 01	01	000	0010	10	101	100

Scanned by CamScanner

Part II : Decoding :

- In the decoding process, the LZ code is given to us and we have to obtain the original code from it.
- Consider the code in the numerical position 3 of Table P. 4.15.1(a). It is 0010. Its decoding takes place as follows :



(E-1675)

Thus the decoded subsequence corresponding to the code 0010 is 00. Similarly for each code segment in Table P. 4.15.1(a), we can obtain the corresponding decoded subsequence as shown in decoding table of Table P. 4.15.1(b). Thus we get the original sequence back.

Ex. 4.15.2 : Determine the Lempel ZIV code for the following bit stream 11101001100010110100. Recover the original sequence from the encoded stream.

Soln. :

Part I : Encoding :

- We assume that the binary symbols 0 and 1 are already stored in the code book.

∴ Subsequences stored : 0, 1

- Encoding is accomplished by parsing the source data stream into segments that are shortest substances, not encountered previously.
- The given bit stream can be parsed into subsequences as shown below :

1, 11, 0, 10, 01, 100, 010, 110, 100

These subsequences are encoded as shown in Fig. P. 4.15.2.

Numerical position	1	2	3	4
Subsequences	1	1 1	0	1 0
Numerical representation	–	1 1	–	1 3
Code	1	0011	0	0010

(E-1676) **Fig. P. 4.15.2 : Principle of coding**

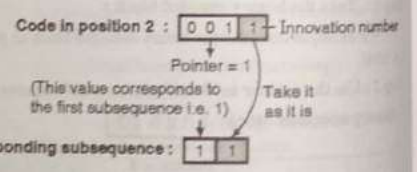
- Similarly we can encode the remaining subsequences as shown in the encoding table of Table P. 4.15.2(a).

Table P. 4.15.2(a) : Encoding table

Numerical position	1	2	3	4	5	6	7	8	9
Subsequences	1	11	0	10	01	100	010	110	100
Numerical Representation	–	11	–	13	31	43	53	23	43
Code	1	0011	0	0010	0111	1000	1010	0100	1000

Part II : Decoding :

- Consider the code corresponding to numerical position-2 in Table P. 4.15.2(a). It is 0011.



(E-1677)

- Thus the decoded subsequence corresponding to code 0011 is 11. Similarly we can decode each code segment in Table P. 4.15.2(a) to obtain the corresponding decoded subsequences as shown in the decoding table of Table P. 4.15.2(b).

Thus the decoded sequence is as follows :

11101001100010110100

This is same as the encoded sequence.

(E-1228) **Table P. 4.15.2(b) : Decoding table**

Code	1	0011	0	0010	0111	1000	1010	0100	1000
Innovative bit	–	1	–	0	1	0	0	0	0
Pointer	1	001	–	001	011	100	101	010	100
Decoded subsequence	1	1 1	0	1 0	0 1	1 0 0	0 1 0	1 1 0	1 0 0

4.15.2 LZW (Lempel Ziv Welch) Data Compaction :

MU : May 15, Dec. 15, May 16

University Questions

Q. 1 Write short note on : LZW compression **(May 15, 5 Marks)**

Q. 2 Explain LZW compression algorithm with example. **(Dec. 15, 10 Marks)**

Q. 3 Explain LZW compression with example. **(May 16, 10 Marks)**

- This is a dictionary technique of data compression.
- If the source is generating recurring patterns then for such frequently occurring patterns; a dictionary is maintained.
- Any pattern at the input is compared with the data in dictionary and accordingly encoding is done.
- If the probability of frequently occurring patterns is known in advance then a static dictionary is used; otherwise adaptive dictionary is used.
- All letters of source alphabet are initially stored in the dictionary.
- Every time, index in the dictionary is set.
- All inputs are accumulated till the pattern say 'P' formed is present in the dictionary.
- When any new pattern is formed then index of previous pattern (P) is transmitted and new pattern is added in the dictionary.
- This produces encoded sequence.
- The decoding procedure makes use of same initial dictionary as that of encoder.
- The Graphics Interface Format (GIF), which was developed by Compuserve Information Service to encode graphical image, uses LZW encoding.
- This algorithm is basically used for encoding of all kinds of images, both computer generated and natural images. The creation of dictionary in LZW is dynamic.

Ex. 4.15.3 : Encode the sequence bcdefghbcmfbc using LZW.

Soln. : Consider initial source alphabet as {bcdefghm}. Add these letters in the dictionary as follows :

Index	Entry
1	b
2	c
3	d
4	e
5	f
6	g
7	h
8	m

Consider first letter 'b', combine it with next letter c to generate bc and transmit index of 'b' that is 1. Similarly continue the process as shown in table.

Input	Entry	Index	Output
b	bc	9	1
c	cd	10	2
d	de	11	3
e	ef	12	4
f	fg	13	5
g	gh	14	6
h	hb	15	7
bc	bcm	16	9
m	mf	17	8
f	fb	18	5
bc	–	–	9

Thus encoded output is, 12345679859

Decoding :

Initial dictionary will be same as encoder. The first output is 1, so decode it as 'b'. Next output is 2. So decode C ; then combine bc and enter in dictionary at index g. This procedure is continued as shown in table.

Input	Decoded symbol	Dictionary	
		Input	Entry
1	b	–	–
2	c	9	bc
3	d	10	cd
4	e	11	de
5	f	12	ef
6	g	13	fg
7	h	14	gh
9	bc	15	hbc
8	m	16	bcm
5	f	17	mf
9	bc	18	fbc

4.16 Run Length Encoding (RLE) :

MU : May 14, Dec. 14, May 16

University Questions

Q. 1 Write short notes on : RLE **(May 14, Dec. 14, 5 Marks)**

Q. 2 Write short notes on RLE **(May 16, 5 Marks)**

- The Run Length Encoding (RLE) is the simplest method that can be used for removing redundancy.
- The data made of any combination of symbols can be compressed using the RLE.
- In this technique, we replace a repeated sequence (also called as run) of the same symbol with two entities : a count and the symbol inself as illustrated in the following example.

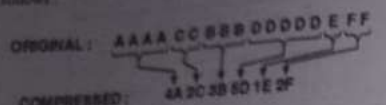
Ex. 4.16.1 : Use the RLE method to compress the following sequence of symbols :

A A A A C C B B B D D D D D E F F

Scanned by CamScanner

Soln. :

We can compress the given sequence of symbols using RLE as follows :



(E-1686) **Fig. P. 4.16.1 : RLE encoding**

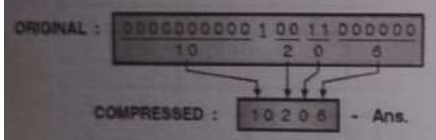
- In this way a string of 17 symbols has been compressed into a string of only 12 symbols.
- We can use a modified version of this method if the given data consists of only two symbols such as 0 and 1.
- In such a case only the count of one of the symbols which occurs between each occurrence of the other symbol is used.
- This concept has been illustrated in the following example :

Ex. 4.16.2 : Use the RLE method of compression to compress the following data :

Data : 0000000000110011000000

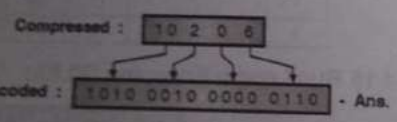
Soln. :

In the given binary data pattern there are more 0s than 1s. Therefore we will just show the number of 0s that occur between 1s.



(E-1685) **Fig. P. 4.16.2(a)**

It is possible to encode the compressed data into binary using a fixed number of bits per digit as shown in Fig. P. 4.16.2(b).



(E-1686) **Fig. P. 4.16.2(b)**

Thus the number of bits in the original sequence were 21 and those in the compressed binary is 16. Hence the rate of compression is 21/16 = 1.31 for this example.

1 Alternative Format of RLE :

An alternative version of RLE is as follows :

If the given data stream is :

0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1

Here we can encode this as follows :

Four 0s, Four 1s, Four 0s, Six 1s.

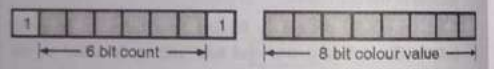
It can be written is the binary form as follows :

0 100 1 100 0 110 1

- The FAX image encoding is done using the RLE technique. The most bit map formats such as TIFF, BMP, PCX support RLE.

The PCX format :

- The PCX format makes use of RLE in order to compress the picture images.
- A picture (image) is made of small pixels. So if the pixels in an image are of same colour, then they are encoded as a special flag byte.
- The code consists of number of pixels and the flag value. If the pixel does not repeat itself in terms of colour, then it is encoded as the byte itself.
- As an example, suppose 256 colours are to be represented, then we may need two bytes for their representation : one byte for string colour and the other byte to store count.
- Thus we need two bytes for every coded pixel.
- Thus we need a huge amount of data to encode an entire image. This makes the encoding highly inefficient.
- The coding efficiency can be improved by using only 192 colours instead of 256, because most of the images are unlikely to have 256 colours.
- This scheme works in the following manner :
  1. If the pixel colour is between 0 and 191 then check for the presence of the **run.**
  2. If the **run** exists with its length n < 63 then encode it as shown in Fig. 4.16.1.



(E-1687) **Fig. 4.16.1**

  3. If the run length n > 63, then slit the run in such a way that each subrun will have at the most 63 bits. Then follow the technique mentioned above.
  4. If there is no run, encode the pixel using single byte.
  5. If the colour of pixel > 191, then use two byte code as shown in Fig. 4.16.1. The count of colour run will be shown in byte – 1 and the colour value in the second byte.

4.17 Speech Compression : MU : Dec. 14

University Questions

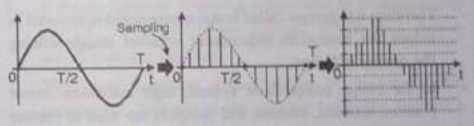
Q. 1 Write short notes on : Speech Compression. **(Dec. 14, 5 Marks)**

- The source coding has become an important part of the modern communication systems.
- This is because the modern communication systems need a large bandwidth and storage capacity. The improvements in the integrated circuits and signal processing techniques enable the engineers to satisfy these needs.
- One more important reason for the wide use of source encoding is the definition of the industry-wide standards.
- The standards used for the source coding algorithms or the compressor algorithms are the CCITT standards.

- The source coding and compression algorithms are used in the following applications :
  1. For speech
  2. For audio
  3. For the still images
  4. For the moving images

4.17.1 Digitizing Audio :

- When a sound wave hit a microphone, they get converted in an analog electrical signal which represents the sound amplitude as a function of time.
- A human ear can hear frequencies in the range from 20 Hz to 20 kHz. The ear hears logarithmically. So the sound intensity is expressed in dB (decibels).
- Audio waves can be converted into digital form by an ADC (analog to digital converter). An A/D converter receives electrical voltage as input (from the microphone, amplifier combination) and generates a binary number as output.
- The A to D conversion process takes place in two steps namely the sampling and quantization. They are illustrated in Fig. 4.17.1.
- Quantization is a process of approximation and in the process of approximation, there is bound to be some error. Such an error is called as **quantization error** or **quantization noise.**
- If this noise is too large then it can be detected by ears.



(a) Analog sinewave **(b) Sampled signal** **(c) Quantized sampled signal**

(E-1204) **Fig. 4.17.1**

- Two well known examples where sampled sound is used are :
  1. Telephone
  2. Audio compact discs.
- Telephone systems use 8 bit pulse code modulation (PCM) at the sampling rate of 8000 samples per second. Such a system gives data rate of 56 kbps or 64 kbps.
- Audio CDs are digital storage devices with a sampling rate of 44,100 samples per second.
- Digitized sound can be easily processed by computers using software. Many programs exist on PCs to allow users to perform many operations including mixing, recording and storing sound waves from multiple sources.
- All professional sound recording and editing processes are digital now a days.

4.17.2 Audio Compression :

- The audio compression means the process of reducing the bandwidth required for an audio signal so as to improve the bandwidth efficiency. The fields or applications in which the technique of audio compression is used are as follows :
  1. Compact disc (CD).
  2. Digital audio tape (DAT).
  3. Mini disc (MD).
  4. Digital compact cassette (DCC).
  5. Digital versatile disc (DVD).
  6. Digital audio broadcasting (DAB).
  7. Motion picture expert group (MPEG).
  8. Audio layer 3 (MP3) distribution on the internet.
  9. Speech compression for telephony.
  10. Speech compression for cellular telephony. (to preserve bandwidth and battery life).
- Different algorithms are used to the speech signals and the other consumer entertainment signals which have larger bandwidths.
- The audio and speech compression schemes can be differentiated from each other depending on the demand of quality.
- The factors that affect the partition between the audio and speech compression schemes are frequency range of the original signal, sampling frequency, number of encoding bits per sample and system bit rates as shown in Table 4.17.1.

Table 4.17.1 : Typical parameter values for various audio signals

Sr. No.	Types of signal	Frequency range	Sampling rate	PCM bits/sample	PCM bit-rate
1.	Telephone speech	300-3400 Hz	8 kHz	8	64 kb/s
2.	Wideband speech	50-7,000 Hz	16 kHz	14	224 kb/s
3.	Wideband audio	10-20,000 Hz	48 kHz	16	768 kb/s

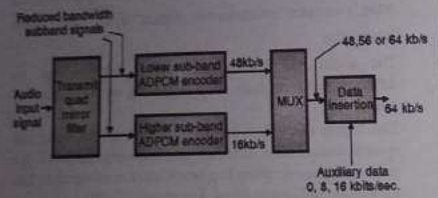
4.17.3 Audio Compression for Telephone Speech Signal :

- The standard used for the compression of the telephone speech signals is the CCITT standard, the G.726 adaptive differential pulse code modulation (ADPCM) codec (coder decoder).
- This standard encodes sample by sample, by predicting the value of each sample from the previous samples. It uses the adaptive feedback predictor to do so.
- The compressor is an 8 bit linear A-law or μ-law type which samples the speech at the rate of 64 kb/s and outputs the speech at a compressed rate of 16, 24, 32 or 40 kb/s.
- The reconstruction errors can be reduced to a minimum by using the encoder with a decoder connected in its feedback path. The decoder analyses and modifies the algorithm parameter so that the errors could be minimized.

Scanned by CamScanner

4.17.4 Audio Compression for Wideband Speech Signals :

- The range of signal frequencies for the wideband speech signal is 60-7,000 Hz. The standard used for the wideband speech compression is CCITT G.722.
- The wideband compression results in significant improvement in the quality and the quality of compressed speech is close to broadcast quality and the quality of music signals.
- The 7 kHz signal is sampled at 16 kHz and the sampled signal is separated into halves (higher and lower subbands) because the coder uses complementary low pass and high pass filters.
- All these functions are implemented in a digital filter known as the quadrature mirror filter. The block diagram of the wideband CODEC is shown in Fig. 4.17.2.

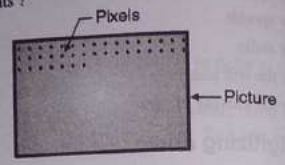


(E-1205) **Fig. 4.17.2 : Wideband QMF - ADPCM (64 kb/s) Codec (G.722)**

- The reduced bandwidth signals at the output of the quadrature mirror filter are processed by two independent ADPCM (Adaptive Differential Pulse Code Modulation) encoders and form the 48 kb/s and 16 kb/s data rates respectively as the low and high band outputs.
- The data rates at the output of the multiplexer can be 48, 56, or 64 kb/s. The lower data rates of 48 or 56 kb/s are obtained if the LSBs of the prediction filter coefficients are discarded.
- This allows the communication system to assign the unused bits to an auxiliary data stream which operates at 0, 8, 16 k bits/s as shown in Fig. 4.17.2.

4.18 Image Compression :

- A picture is equivalent to about five million words. That means transmitting 5 million words is equivalent to transmitting a picture.
- Therefore the transmission of a picture with high quality requires a large transmission bandwidth. But with so many TV channels to be transmitted simultaneously we cannot afford to allot such a large bandwidth for each TV channel.
- Therefore source coding (PCM, DM, DPCM or ADM) has to be used to reduce the bandwidth and memory requirement.
- The two standards used for image compression are :
  1. Joint Photographic Experts Group (JPEG)
  2. Motion Picture Experts Group (MPEG)
- A picture is worth a thousand words. For example, 1000 words contain 6000 characters. If each character is coded into 7-bit ASCII symbols then we require 6000 × 7 i.e. 42000 bits.
- What will be the size of a picture that can be described with 42000 bits ?



(E-1206) **Fig. 4.18.1**

- As shown in Fig. 4.18.1, an image is formed with the picture elements called pixels. Generally a medium quality picture is formed with 300 pixels per inch.
- With existing standards the 42,000 bits will be able to describe a picture of size 1/4 inch i.e. a very small picture.
- If the picture size is increased then the number of pixels will increase and hence the number of bits will also increase. A picture of 8.5 inch by 11.0 inch with 300 pixels per inch would require about 2×10^8 bits.
- If such a picture is to be transmitted, then we will require a bandwidth which is approximately half the number of bits. Thus BW requirement increases with increase in the size of picture.
- The bandwidth requirement further increases if the quality of image is to be improved.
- This much channel bandwidth is practically impossible to be allotted.
- Therefore a technique called image compression is invented to reduce the bandwidth requirement **without compromising the quality of image.**
- In the image compression system, high resolution colour printers, scanners, cameras and monitors are used to capture and present high quality images for advertisement and entertainment.
- To transmit this image, we have to use some kind of source coding technique to reduce bandwidth and memory requirements.

4.18.1 Digitizing Video :

- In the conventional video reproduction on the TV or computer screen, the picture frames are displayed at a very rapid rate (typically 50 frames per sec.).
- The interlaced scanning is used in which 25 frames are displayed per second in an alternate manner.
- Each frame is divided into small grids called pixels. For the black and white TV, each 8 bit pixel represents one of 256 possible different gray levels, because $256 = 2^8$.
- For colour TV each pixel is represented by 24 bits out of which a group 8 bits is used to represent 8 bits one primary colour (Red, Green and Blue).
- The lowest resolution for a coloured picture is 1024 × 768 pixels per frame.
- So the number of bits corresponding to one picture is calculated as follows :

$$\text{Number of bits/pictures} = 2 \times \text{Number of frames/sec.} \times \text{Resolution}$$

$$= 2 \times 25 \times 1024 \times 768$$
$$= 944 \text{ Mbps} = 944 \times 10^6 \text{ bps}$$

- To send video with minimum resolution, we need to transmit at 944 Mbps which requires a huge bandwidth, (approximately equal to 944/2 = 472 MHz) per channel.
- This much bandwidth is not available practically. So we have to use the compression technique so as to reduce the number of bits and hence to reduce the bandwidth.
- Compression is essential to send video over the Internet as well.
- It is possible to sample and quantize the video images so that a binary data stream can be used to represent the image in a satisfactory manner.
- It is interesting to note that we can represent a picture by anything from 1000 to 1 million bytes of data. The quality of picture will depend on the number of bytes used.
- For the storage and transmission of such a huge picture data, some kind of a compression is necessary.

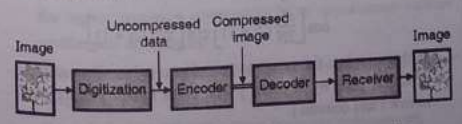
4.18.2 Characteristics of Images :

Some of the important characteristics of images are as follows :

1. Since a very large number of bits is required for the representation of an image, it is necessary to use extremely high compression ratios to make storage and transmission practically possible.
2. If the transmission of moving images is to be done (examples are TV, movies, computer graphics, WWW etc.) then it should executed very fast.
3. The most important characteristics of images if the redundancy. That means the adjacent horizontal lines in a picture contain nearly identical information.
4. Human eyes are highly tolerant to the approximation errors in an image. This makes the compression practically possible. Such a compression is called is the lossy compression.

Video compression techniques :

- We can compress video by compressing images. The two standards used for image compression are :
  1. Joint Photographic Experts Group (JPEG).
  2. Moving Picture Experts Group (MPEG).
- Out of these the JPEG is used to compress still images whereas the MPEG is used for compressing moving pictures.
- Fig. 4.18.2 shows the general principle of image compression.



(E-1207) **Fig. 4.18.2 : Principle of image compression**

4.18.3 JPEG Standards :

- Video is simply a sequence of images (plus sound). So video compression is called as image compression.
- One of the standards used for compression is JPEG i.e. Joint Photographic Experts Group standards. This is a standard for compressing still pictures such as photographs.

4.18.4 The JPEG Standard for Lossless Compression :

- The JPEG was formed jointly by CCITT and ISO, the two standard organizations.
- The lossless compression option of JPEG image compression standard is a description of 29 different coding systems for compressing images.
- So many approaches are described because the needs of different users are extremely different as compared to each others.
- In this section we will discuss only two methods which use the entropy coding. They are :
  1. Huffman code and
  2. Arithmetic code

Out of these we have already discussed the Huffman code. Let us now discuss the **Arithmetic code.**

Arithmetic code :

- This code achieves the compression in transmission or storage by making use of the probabilistic nature of the data.
- The number of bits after compression will be less than those used in the source data stream.
- Arithmetic code has an advantage over the Huffman code that it comes closer to the Shannon entropy limit of compression.
- The reason for this is that the Huffman code works effectively when the probabilities of the symbols can be expressed as fractions of powers of two. This constraint is not present for the arithmetic code.
- It is possible to achieve some compression if we can predict the next pixel in an image using the previous pixels.
- In this method one has to transmit only the difference in values (predicted and actual) which is called as the prediction coefficient. Note that the entire pixel is not to be transmitted.
- In JPEG, three are various schemes used for predicting the next pixel.
- These variations are not dependent on the users choice. But that scheme for prediction is selected which gives the best possible prediction.
- In all there are eight prediction methods available in JPEG coding standards one of them is not used for the lossless compression. The remaining seven are classified into the following categories :
  1. This predicts that the next pixel on the line has the same value as the previous pixel.

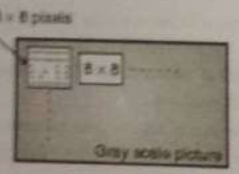
Scanned by CamScanner

2. This group of schemes predicts that the next pixel on a line has the same value as the pixel at the same position on the previous line.
3. This group of schemes predicts that the next pixel on a line is related to a combination of the previous, above and previous to above pixel values. In one such technique they take the average of the three values.

- One of the lossless compression techniques used in JPEG standards is the **differential encoding**. It consists of the difference between the actual pixel value and the predicted value.
- Due to the redundancy present in an image, the difference between the predicted and actual pixel value will be small. So this scheme is suitable for the entropy coding.

4.18.5 The JPEG Standard for Lossy Compression :

- As some image distortion is acceptable to human eye, the JPEG standard includes a set of lossy compression options.
- The JPEG lossy compression first simplifies the image and removes the image complexity. Then the simplified image is passed through the lossless compression based on predictive filtering and Huffman or Arithmetic coding.
- The lossy image simplification step called as the image reduction is carried out by using the Discrete Cosine Transform (DCT).
- If the picture is not coloured (gray scale), then each pixel can be represented by an 8-bit integer (i.e. $2^8 = 256$ levels). If a coloured picture is to be represented, then we have to use 24 bits (3×8 bits) with each 8 bits representing one of the three basic colours (Red, Green and Blue).
- As shown in Fig. 4.18.3 in JPEG, a gray scale picture is divided into blocks of 8×8 pixels.



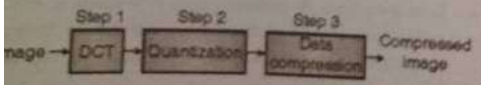
(E-1208) **Fig. 4.18.3**

- The JPEG changes the picture into a linear (vector) set of numbers. This process is explained below.

Three steps in JPEG :

- The three steps in JPEG compression process are as follows :
  1. Discrete Cosine Transform (DCT).
  2. Quantization
  3. Data compression.

  These steps are illustrated in Fig. 4.18.4.



(E-1209) **Fig. 4.18.4 : JPEG process**

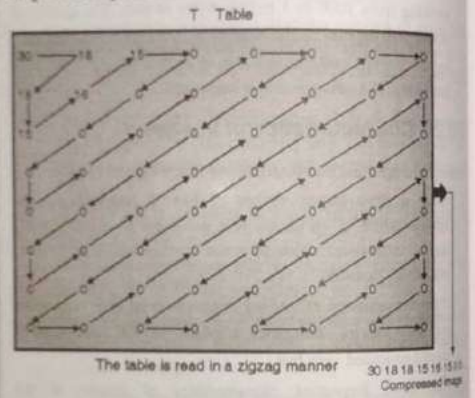
Step 1 : Discrete Cosine Transform (DCT) :

- The image in the form of blocks of $8 \times 8 = 64$ pixels is applied to the DCT box.
- Each 8×8 block will undergo a transformation called discrete cosine transform (DCT).

Step 2 : Quantization :

- The DCT transformed 8×8 blocks are then quantized. The process of quantization reduces the number of bits required to be used for encoding.
- Quantization is the process of approximation. Hence we lose some information and it is not possible to recover the information at all.
- This is why the JPEG is called as lossy compression.

Step 3 : Compression :



(E-1210) **Fig. 4.18.5 : Compression**

- In the first step (DCT) a transformation table T is created.
- After quantization, the values in this table are read to remove redundant zero bits.
- The table is read in a zig-zag manner, as shown in Fig. 4.18.5 to produce the compressed digital image.
- Note that the numbers in the table indicate the gray scale (shade in between black and white) and zeros indicate redundancy i.e. no change in shade.
- So at the output of the compressor, we get the compressed digitized image.

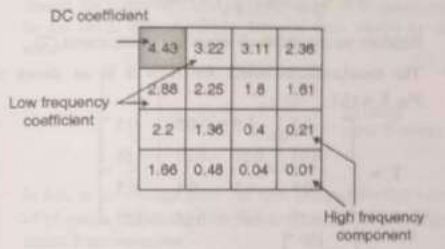
4.18.6 Discrete Cosine Transform (DCT) :

- The discrete cosine transform is defined as follows :

$$Y(k, l) = \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} 4\, y(i, j) \cos\left[\frac{\pi k}{2N}(2i+1)\right] \cos\left[\frac{\pi l}{2M}(2j+1)\right]$$

- In this equation the image to be compressed is assumed to be of size N pixel by M pixel, y (i, j) is the intensity of the pixel in row i and column j.

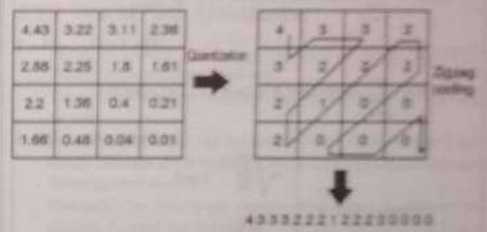
- Y (k, l) is the DCT coefficient in the kth row and l^{th} column of the DCT matrix.
- In the DCT all the multiplications are real. So there are less number of multiplications as compared to Discrete Fourier Transform (DFT).
- For most of the images a large part of signal energy lies at the lower frequencies which appears in the upper left corner of the DCT as shown in Fig. 4.18.6.
- The values on the lower right side represent the higher frequencies as shown in Fig. 4.18.6 and these values are generally small.



4.43	3.22	3.11	2.36
2.88	2.25	1.8	1.61
2.2	1.36	0.4	0.21
1.66	0.48	0.04	0.01

(E-1211) **Fig. 4.18.6 : Typical values of DCT corresponding to an image**

- The values of high frequency components are usually so small that we can neglect them without much distortion getting introduced.
- In JPEG, as mentioned earlier, the input image is divided into 8×8 pixel blocks. For application of DCT. For example an image of 256×256 pixel size, will be broken into 32 blocks each containing $8 \times 8 = 64$ pixels. Each of these 32 blocks are considered separately.
- The 64 pixel values in each block are then transformed by the DCT into a set of 64 new values. These new values are known as the DCT coefficients as shown in Fig. 4.18.7.
- The component on the top left in Fig. 4.18.6 is called as DC coefficient and its value is proportional to the average value of the 8×8 block of pixels. The remaining coefficients are called as the AC coefficients.
- As far as the image reduction using DCT is concerned, here is an interesting observation. For most images the maximum information lies in the low frequency spectrum than the high frequency components.
- So, in order to exercise the image reduction, we can represent the higher frequency components in an approximate manner or eliminate them totally.
- This will not have much of an effect on the quality of the image.
- This is how the DCT will achieve the image compression.
- The compression takes place by following the steps given below :
  1. The lowest (high frequency) coefficients are trimmed by setting them to zero. This will reduce the higher frequency components.
  2. The remaining low frequency higher value coefficients are then quantized. This will reduce some of the medium and low frequency components in the given image.
- The AC coefficients are quantized as shown in Figs. 4.18.7(a) and (b). This will convert most of the small value components to zero, as shown in Fig. 4.18.7(b).
- Finally the zigzag coding is used to obtain the code as shown in Fig. 4.18.7(b).
- The zigzag coding is used in order to move smoothly from low frequency to high frequency components in the image without abrupt jumps.



(a) **Original DCT coefficients** (b) **Quantized DCT values and zigzag coding**

(E-1212) **Fig. 4.18.7**

4.18.7 Types of DCT :

- Types of DCT :
  1. One-dimensional DCT
  2. Two-dimensional DCT
- In multimedia compression we use two-dimensional DCT.

4.18.8 One-dimensional DCT :

- In one-dimensional DCT, Transformed data (i.e. column matrix M) is obtained by the matrix multiplication of source data (i.e. column matrix P) by a DCT coefficient (i.e. square matrix T).
- Since DCT coefficient is an orthogonal matrix (i.e. inverse and transpose of matrix are the same). Inverse transformation is multiplication of M (i.e. transformed data matrix) by T^T (i.e. the transpose matrix of the DCT coefficient).
- The transformation in matrix is as shown in Fig. 4.18.8 and formulas used for one-dimensional forward and inverse transformation is as shown in Fig. 4.18.9.

Scanned by CamScanner

Transformation : $[T] \times [P] = [M]$

Inverse transformation : $[T^T] \times [M] = [P]$

Where, T^T = Transpose of matrix

P = Source data

M = Transformed data

T = DCT coefficient

$$T(x, y) = C(x) \cos\left[\frac{\pi y (2x+1)}{2N}\right]$$

Where, N = Size of matrix T

For $x = 0$ to $N-1$

For $y = 0$ to $N-1$

$$C(x) = \begin{cases} \sqrt{\frac{1}{N}} & x \\ \sqrt{\frac{2}{N}} & x \end{cases}$$

Fig. 4.18.8 : One-dimensional DCT

$$M(x) = \sum_{y=0}^{N-1} C(x) \cos[\pi y(2x+1)/2N] \times P(y)$$

For $x = 0 \ldots\ldots N-1$

$$P(y) = \sum_{x=0}^{N-1} C(y) \cos[\pi x(2y+1)/2N] \times M(x)$$

For $y = 0 \ldots\ldots N-1$

$$\text{Where, } C(i) = \begin{cases} \sqrt{\frac{1}{N}} & i = 0 \\ \sqrt{\frac{2}{N}} & i > 0 \end{cases}$$

Fig. 4.18.9 : Formulae for 1-D DCT

- The following example explains the concept of one dimensional DCT.
- This example shows how we can transform the sequence of numbers to another sequence of numbers.

Ex. 4.18.1 : Find the 1D-DCT matrix for N = 4.

Soln. :

x \ y	0	1	2	3
0	(0, 0)	(0, 1)	(0, 2)	(0, 3)
1	(1, 0)	(1, 1)	(1, 2)	(1, 3)
2	(2, 0)	(2, 1)	(2, 2)	(2, 3)
3	(3, 0)	(3, 1)	(3, 2)	(3, 3)

T =

We know that $T(x, y) = C(x) \cos\left[\frac{\pi y (2x+1)}{2N}\right]$,

$$C(i) = \begin{cases} \sqrt{\frac{1}{N}} & x = 0 \\ \sqrt{\frac{2}{N}} & x > 0 \end{cases}$$

$$\text{For } T(0, 0) = \sqrt{\frac{1}{N}} \cos\left[\frac{\pi \times 0 (2 \times 0 + 1)}{2 \times 4}\right] = 0.5$$

$$T(0, 1) = \sqrt{\frac{1}{N}} \cos\left[\frac{\pi \times 1 (2 \times 0 + 1)}{8}\right]$$

$$= \sqrt{\frac{1}{4}} \cos\left(\frac{\pi}{8}\right) = 0.5$$

$$T(1, 1) = \sqrt{\frac{2}{N}} \cos\left[\frac{\pi \times 1 (2 \times 1 + 1)}{8}\right]$$

$$= \sqrt{\frac{2}{4}} \cos\left(\frac{3\pi}{8}\right) = 0.27$$

$$T(1, 3) = \sqrt{\frac{2}{N}} \cos\left[\frac{\pi \times 3 (2 + 1)}{8}\right]$$

$$= \sqrt{\frac{2}{4}} \cos\left(\frac{9\pi}{8}\right) = -0.65$$

- Similarly we can obtain all values in a square matrix (T).
- The transformation matrix for N = 4 is as shown in Fig. P. 4.18.1.

$$T = \begin{bmatrix} 0.5 & 0.5 & 0.5 & 0.5 \\ 0.65 & 0.27 & -0.27 & -0.65 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.27 & -0.65 & 0.65 & -0.27 \end{bmatrix}$$

$$\text{and} \quad P = \begin{bmatrix} 100 \\ 101 \\ 102 \\ 103 \end{bmatrix}$$

- In square matrix, T, first row has 4 equal values whereas the other rows have positive and negative values.
- Multiply each row by the source data matrix. If the source data values are close to each other then we can expect that result of positive and negative values are close to zero.
- We expect this is what from the transformation to show that in the data source only some values are important and other more values are redundant.

$$\underset{T}{\begin{bmatrix} 0.5 & 0.5 & 0.5 & 0.5 \\ 0.65 & 0.27 & -0.27 & -0.65 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.27 & -0.65 & 0.65 & -0.27 \end{bmatrix}} \times \underset{P}{\begin{bmatrix} 100 \\ 101 \\ 102 \\ 103 \end{bmatrix}} = \underset{M}{\begin{bmatrix} 203 \\ -2.22 \\ 0.0 \\ -0.16 \end{bmatrix}}$$

(a) Transformation

$$\underset{T^T}{\begin{bmatrix} 0.5 & 0.65 & 0.5 & 0.27 \\ 0.5 & 0.27 & -0.5 & -0.65 \\ 0.5 & -0.27 & -0.5 & 0.75 \\ 0.5 & -0.65 & 0.5 & -0.27 \end{bmatrix}} \times \underset{M}{\begin{bmatrix} 203 \\ -2.22 \\ 0.0 \\ -0.16 \end{bmatrix}} = \underset{P}{\begin{bmatrix} 100 \\ 101 \\ 102 \\ 103 \end{bmatrix}}$$

(b)

Fig. P. 4.18.1 : Inverse transformation

- From this example it is clear that we can transform the sequence of numbers [100, 101, 102, 103] to other sequence of number [203, – 2.22, 0.0, –0.16].

4.18.9 Properties of DCT Transformation :

1. Reversible transformation.
2. Orthogonal transformation matrix i.e. $T^{-1} = T^T$. That means in the calculation of the reveres transformation no need to use inverse matrix. Transposed matrix can be used.
3. First row of column matrix i.e. M is always weighted average of the source data matrix i.e. P matrix.
4. Other row values can be ignored because the values are very small (positive or negative)

- The very important note about this transformation is that if we change the values in P matrix, three values of M matrix will be the same. But correlation between them should be the same.

$$\text{i.e. If } P = \begin{bmatrix} 6 \\ 7 \\ 8 \\ 9 \end{bmatrix} \text{ then } M = \begin{bmatrix} 15 \\ -2.22 \\ 0.0 \\ -0.16 \end{bmatrix} \text{ by using same T-matrix}$$

- In this, as the average value has been changed the first value of M matrix will change. The last three values in source data matrix P are redundant.

4.18.10 Two-Dimensional DCT :

- For compression of audio, video and images, we need two-dimensional DCT.
- The principle of one-dimensional and two-dimensional DCT is same. Only change is that the source data and transformed data are two-dimensional square matrices.
- In two-dimensional DCT, T matrix is used twice in the transformation i.e. T and T^T.
- In inverse transformation, matrix T is used two times but in reverse order.
- The two-dimensional DCT in matrix format is as shown in Fig. 4.18.10 and formula for two-dimensional DCT is as shown in Fig. 4.18.11.

Transformation : $[T] \times [P] \times [T^T] = [M]$

Inverse transformation : $[T^T] \times [M] \times [T] = [P]$

Where, $$T(x, y) = C(x, y) \cos\left[\frac{x \pi (2y+1)}{2N}\right]$$

For $x = 0$ to $N-1$

$y = 0$ to $N-1$

$$c(m, n) = \begin{cases} \sqrt{\frac{1}{N}} & x = 0 \\ \sqrt{\frac{2}{N}} & x > 0 \end{cases}$$

Fig. 4.18.10 : Two-dimensional DCT

$$M(x, y) = \frac{2}{N} C(x) C(y) \sum_{M=0}^{N-1} \sum_{N=0}^{N-1} P(m, n) \cos\left[\frac{x \pi (2m+1)}{2N}\right] \cos\left[\frac{y \pi (2n+1)}{2N}\right]$$

...for $x = 0$ to $N-1$

...for $y = 0$ to $N-1$

$$P(m, n) = \frac{2}{N} C(m) C(n) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} M(x, y) \cos\left[\frac{m \pi (2x+1)}{2N}\right] \cos\left[\frac{n \pi (2y+1)}{2N}\right] \ldots\ldots$$

...for $m = 0$ to $N-1$

...for $n = 0$ to $N-1$

$$C(u) = \begin{cases} \sqrt{\frac{1}{2}} & u = 0 \\ 1 & u > 0 \end{cases}$$

Fig. 4.18.11 : Formulae for 2-D DCT

4.19 The MPEG Standards :

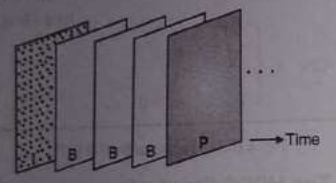
- MPEG is another standard. Long form of MPEG is Motion Picture Experts Group standards.
- These algorithms are standardized to compress any moving pictures.
- Digital motion video can be accomplished with the JPEG still image standard if the hardware used is fast enough to process 30 images per second.
- However, the maximum compression potential cannot be attained because the redundancy between frames is not being exploited.
- Furthermore, there are many other things to be considered in compressing and decompressing motion video, as indicated in the objectives.
- The MPEG compression standards are among the most popular compression techniques.
- Various MPEG standards are as follows :
  1. MPEG 1 : For CD-ROM quality video (1.5 Mbps).
  2. MPEG 2 : For high quality DVD video (3-6 Mbps).
  3. MPEG 4 : For object oriented video compression.
- The H.261 video compression standards are also very popular in the Internet.

Principle of image compression in MPEG-2 :

- MPEG-2 takes the advantage of the fact that there exists a high correlation between successive frames of a moving picture. It uses this fact to compress a sequence of moving images.
- MPEG constructs three types of pictures namely :
  1. Intra pictures (I-pictures).
  2. Predicted pictures (P-pictures).
  3. Bidirectional predicted pictures (B-pictures).
- In MPEG every M^{th} picture in a sequence can be fully compressed by using a standard MPEG algorithm, these are I pictures.

Scanned by CamScanner

- Then the successive I-pictures are compared and the portion of the image that have moved are identified.
- The image sections which do not move are carried forward in time domain to intermediate pictures by the decoder memory.
- Then a subset of intermediate pictures is selected and the prediction and correction of locations of the image section which have moved, is carried out.
- These predicted and corrected images are the P-pictures.
- The pictures between I and P-pictures are the B-pictures. They incorporate the stationary image sections which are not covered by the moving sections.
- Fig. 4.19.1 shows the relative position of these pictures.

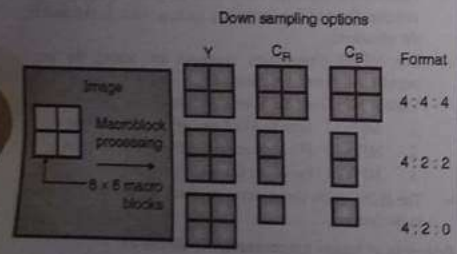


(E-1213) Fig. 4.19.1 : Sequence of pictures in MPEG compression

- The P and B pictures are allowed but they are not required and their number keeps changing.
- It is possible to form a sequence without P or B pictures but a sequence without I pictures is not possible.

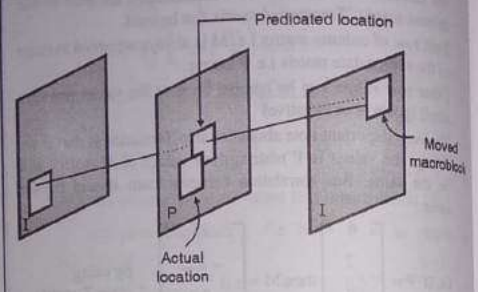
Compression process :

- The I-pictures are compressed as if they are JPEG images.
- The compressed images are then applied to four 8 × 8 blocks called macro blocks.



(E-1214) Fig. 4.19.2 : Processing of macroblocks for chrominance down sampling

- The macro blocks are down sampled for subsequent compression of chrominance (colour component) component as shown in Fig. 4.19.2.
- The first step in MPEG is to identify the macroblocks moved between the I-pictures.
- Next step is to form the P-frame between the I-pictures. Each macro block is placed at its predicted location on the P-frame and is cross-correlated in its neighbourhood to determine the true location of the macro block in P-frame.
- The difference between the predicted and true position of the macro block represents the error in prediction.
- This error is compressed using DCT and used for correcting the P- frame.
- Fig. 4.19.3 shows the macro block shift between I-pictures and an intermediate P-picture.



(E-1215) Fig. 4.19.3 : Movement of macroblocks between I-pictures and P-picture

4.20 Graphics Interchange Format (GIF) :

- GIF is a bitmap image format introduced by Compuserve in 1987.
- It makes use of lossless compression algorithm.
- GIF supports upto 8 bits per pixel. This gives limitation upto 256 colors.
- The different colors are selected from 24 bit RGB color space.
- Most commonly, GIF is used for graphics or logos.
- A lossless compression of GIF images is done using LZW lossless data compression technique.
- The compression ratio of 2 : 1 is used. That means, compressed image is one half of the original image.
- Since maximum 256 color levels can be obtained; GIF is basically used for graphic and text based images.
- When interlaced GIF is used a low resolution image is displayed inside the webpage. This image gradually comes into focus.
- But if interlaced GIF is used then file size increases.
- When non-interlaced GIF is used then an empty box with red color "X" is displayed on the screen; until the full image is downloaded.
- Since human being is more sensitive to the sharpness of edges; GIF image appears more sharper than JPEG.
- Generally two types of GIF are used :
  1. Animated GIF 2. Transparent GIF

- In animated GIF, multiple images are stored and they are controlled in such a way that appearance is like a real time animation.
- In case of transparent GIF is a special color is used as a background, so image appears as transparent.
- GIF uses a small indexed table (palette) of colours which contains 256 (2^8), colours. GIF maps a true colour with the indexed table colour.

4.20.1 Advantages :

- It is simple bit map image format which has wide support and portability.
- GIF supports transparency, animation and interlacing.
- Lossless compression is achieved by using fewer colors.
- GIF images are much sharper than JPEG.

4.20.2 Disadvantages :

- Since only 256 colors for each frame can be used as GIF is not applicable for reproducing color photographs and images having continuous colors.
- LZW compression algorithm is used, but this algorithm is not designed specifically for graphics.Due to this, GIF is not suitable for black and white images and true color images.

Review Questions

Q. 1 What is multimedia ?
Q. 2 What do you understand by streamed stored audio and video ?
Q. 3 How are the multimedia applications classified ?
Q. 4 Write a short note on : Streamed interactive audio and video.
Q. 5 What are the problems faced by multimedia over the existing internet ?
Q. 6 State and explain the limitations of the best effort service.
Q. 7 State the real time interactive applications.
Q. 8 Write a short note on : VoD.
Q. 9 What is the use of metafiles in the streamed stored audio/video applications ?
Q. 10 What is an IPTV ? Explain its principle.
Q. 11 Explain the Huffman coding.
Q. 12 What is data compaction ?
Q. 13 Explain adaptive Huffman encoding algorithm.
Q. 14 Explain the Lempel ZIV coding.
Q. 15 What is meant by dictionary compression ?
Q. 16 Explain the LZW coding.
Q. 17 What do you understand by Run Length Encoding (RLE) ? State its examples.
Q. 18 Write a note on data compression.
Q. 19 Write short note on :
  1. Digital audio 2. Audio compression
  3. Streaming audio.
Q. 20 State objectives of JPEG.
Q. 21 List various objectives of MPEG.
Q. 22 Explain the audio and video compression.
Q. 23 Write a note on : JPEG standards.
Q. 24 Explain the MPEG standards.
Q. 25 Explain the steps in JPEG compression.
Q. 26 Explain the MPEG compression process.

□□□

Scanned by CamScanner

CHAPTER 5

Module III

Session Layer

Syllabus :

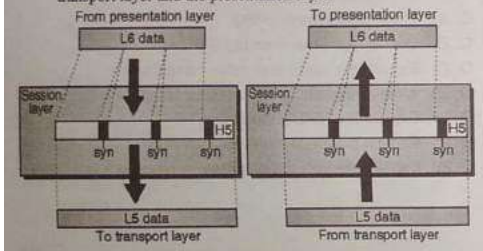
Session layer design issues, Session layer protocol-Remote procedure call (RPC).

5.1 The Session Layer : MU : May 04

University Questions

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

- The main function of this layer is to establish, maintain and synchronise the communication between interested systems.
- Fig. 5.1.1 shows the relationship of the session layer to the transport layer and the presentation layer.



(G-68) **Fig. 5.1.1 : 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**.
- In fact 22 different services are provided by the session layer. These are grouped into subsets such as the Kernel Function Unit, the Basic Activity Subset and the Basic Synchronization Subset.
- However the two most important services provided by the session layer are :

1. Dialog control and 2. Dialog separation

1. Dialog control :

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

2. Dialog separation :

- It is a process of inserting a reference marker called as a checkpoint into the data stream travelling between the sending and receiving systems.
- This allows the checking of status of both the machines at the same point in time.
- This will avoid any possible confusion and collision situation.

5.2 Session Layer Design Issues :

Following are the important design issues that are related to session layer.

1. If traffic is permitted only in one direction, in this case it must manage the dialog by keeping the track of whose turn is next.
2. Sometimes it may be the case that both the sides do not attempt to carry out the same operation simultaneously. In such case the responsibility of the session layer is to provide some sort of token management which makes sure this mutual exclusion in communication.
3. In case of a long data transmission to a failure-prone line, it can happen that after some portion of data has been transferred, the link may break. In such case, data transmission starts right from the beginning. If line is faulty, the transfer may never complete. In such cases the session layer should have a synchronization mechanism such as checkpoints, to make sure that the data transmission begins next time from the point where the link went dead.

5.3 Session Layer Protocols :

- Table 5.3.1 shows the list of session layer protocols.

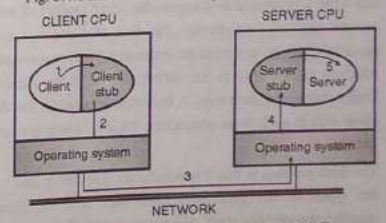
Table 5.3.1 : Session layer protocols

Sr. No.	Protocol	Function
1.	NFS (Network File System)	Provides transparent access to resources stored on remote locations.
2.	SQL (Structured Query Language)	To provide users with a simpler way to define their data requirements between local and remote systems.
3.	RPC (Remote Procedure Call)	RPC allows procedures to be created on a client and subsequently be performed on a remote device i.e. server.
4.	X window	X window accesses the services of the host server, which allows them to operate like locally attached monitors.
5.	NetBios (Network basic input/output services)	This protocol provides session layer interoperatability with other NetBios enabled operating system.
6.	UDP (User Datagram Protocol)	UDP provides fast data delivery.
7.	NCP (Netware Core Protocol)	It supports file and print services, network management, accounting and security functions.
8.	ASP (Appletalk Session Protocol)	In between Apple client and any server application which supports ASP, it provides session layer services.
9.	ADSP (Appletalk Data Stream Protocol)	A session layer protocol that runs at both transport and session layer. It allows communication to take place in a sequence of multiple transactions.

Generally session layer protocols are transparent to the end user. Without session layer protocols you cannot initialize and maintain a virtual connection between clients. In this chapter we will discuss only one session layer protocol i.e. RPC. (Remote Procedure Call).

5.4 RPC (Remote Procedure Call) :

- Sending message to a remote host and getting a reply is very similar to making a function call in a programming language.
- In both the cases the user starts with one or more parameters and get back a result. Due to this people have tried to arrange request reply interactions on networks in the form of procedure calls. This makes network applications very easy to program and deal with.
- For example, consider a procedure called get-IP-address (host-name) in which a UDP packet is sent to a DNS server and the reply is awaited. If timed out, it tries again. In this way all the details of networking can be hidden from the programmer.
- An extremely important work in this area was done by Birrell and Nelson. They suggested to allow programs to call procedures located on remote hosts.
- When a process on machine-1 calls a procedure on machine-2, then the calling process on 1 is suspended and execution of the called procedure takes place on machine-2. No message passing is visible to the programmer. This technique is called as **RPC (Remote Procedure Call).** Traditionally the calling procedure is known as client and the called procedure is known as the server. These names are used for RPC too.
- The principle behind RPC is to make a remote procedure call look like a local call.
- To call a remote procedure, the client program should be bound with a small library procedure called as **client stub** which represents the server procedure in the client's address space.
- Similarly a server is bound with a procedure called as the **server stub.**
- Fig. 5.4.1 shows the actual steps in making an RPC.



(G-628) **Fig. 5.4.1 : Steps in making RPC**

Step 1 : Client calls the client stub. This is a local procedure call and the parameters are pushed on to the stack in the normal way.

Step 2 : Client stub encapsulates the parameters into a message and makes a system call and sends the message. Packing the parameters into a message is called as marshaling.

Scanned by CamScanner

Step 3 : The message is sent from client machine to server machine.

Step 4 : The received packet by the server is passed to the server stub.

Step 5 : Server stub calls the server procedure with the unmarshaled parameters.

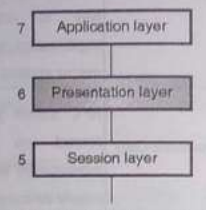
- The reply from server to client follows the same path in the opposite direction.
- It is important to note that, the client procedure written by the user makes a normal (local) procedure call to the client stub (which has the same name as the server procedure). The client procedure and client stub are in the same address space. Therefore the parameters are passed in the normal manner. On the server side, for the server procedure nothing is new. Thus instead of I/O being done on socket, the network communication takes place by **faking** a normal procedure call.

Problems with RPC :

- RPC is conceptually good but has some problems. The biggest one is the use of pointer parameters. Generally passing a pointer to a procedure is not a problem. The called procedure can use the pointer in the same way the caller procedure uses it, because both the procedures have the same virtual address space. But with RPC it is not possible to pass pointers because client and server are in different address space.
- It is however possible to use tricks to pass pointers. But even this can not pass all the pointers. (pointers pointing to a graph or other complex data structure). Hence some restrictions should be placed on parameters in case of RPC.
- The second problem is that in the languages such as C, we can write a procedure to compute the inner product of two vectors (arrays) even though the size of vectors is not specified. Each vector could be terminated by a special value which is known only to the calling and called procedures. Under these circumstances, it becomes impossible for the client stub to pack those parameters, the size of which is not known.
- The third problem is that it is not always possible to find out the types of the parameters, not even from a formal specification or code itself. For example **printf**, it can have any number of parameters of different types. Trying to call printf as a remote procedure would not be practically possible.
- The fourth disadvantage is related to the use of global variables. Generally the calling and called procedures can communicate by using global variables in addition to using parameters. But if the called procedure is present on a remote machine, then the code will fail because the global variables are not being shared anymore.
- All these problems put some limitations on the use of RPC.
- It is not compulsory that we use UDP packets for RPC but UDP is very well suited for RPC.
- But sometimes a TCP connection is required to be set up rather than using UDP.

5.5 Presentation Layer :

- The presentation layer is the 6th layer the OSI model as shown in Fig. 5.5.1.
- Above it there is the application layer and below it there is the sessions layer.



(G-707) **Fig. 5.5.1 : 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.

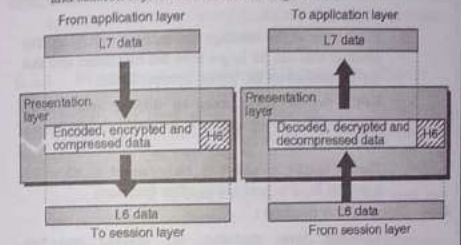
- At the receiving end, an exactly opposite process called Decryption is carried out in which the received information is transformed back to its original form.
- Encryption and Decryption are carried out by the presentation layer.

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. 5.5.2.



(G-69) **Fig. 5.5.2 : 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. 5.5.2.
- This is then sent to the session layer as L-6 data. These processes take place at the sending end of the system.
- While receiving the data from session layer, the operations carried out by the presentation layer are exactly opposite to those carried out while transmitting.
- The received data from the session layer undergoes decryption, decompression and decoding at the presentation layer.
- The header H-6 is detached from the data and then the L-7 data is sent to the application layer.

Functions of presentation layer :

- The presentation layer performs the following function :
  1. It translates data between the formats the network requires and the format the computer expects (e.g. ASCII or EBCDIC).
  2. It does the protocol conversion.
  3. For security and privacy purpose it carries out encryption at the transmitter and decryption at the receiver.
  4. It carries out data compression to reduce the bandwidth of the data to be transmitted.
- Unlike the session layer, which provides many different functions, the presentation layer has only one function.
- It basically functions as a pass through device. It receives primitives from the application layer and issues duplicate primitives to the session layer below it, using the Presentation Service Access Point (PSAP) and Session Service Access Point (SSAP).

Review Questions

Q. 1 State the functions of session layer.

Q. 2 State the important design issues related to session layer.

Q. 3 Write short note on : Session layer protocols.

Q. 4 Explain the concept remote procedure call.

Q. 5 State the problems with RPC.

Q. 6 Write short note on : Presentation layer.

Q. 7 State the functions of presentation layer.

□□□

Scanned by CamScanner

CHAPTER 6

Transport Layer

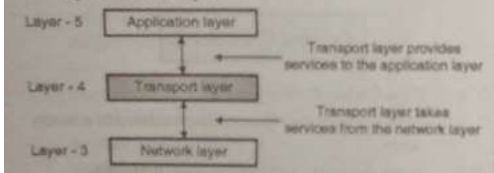
Module - III

Syllabus :

Transport layer services, Transport layer protocols : Simple protocol, Stop-and wait protocol, Go-Back-N protocol (GBN), Selective repeat protocol, Bidirectional protocols : Piggibacking, Internet transport layer protocols, User datagram protocol : User datagram, UDP services, UDP applications, Transmission Control Protocol : TCP services, TCP features, Segment, A TCP connection, State transition diagram, Windows in TCP, Flow control, Error control, TCP congestion control, TCP timers, Options.

6.1 Introduction :

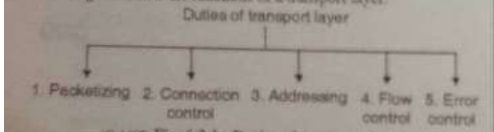
- The transport layer is the core of the Internet model. The application layer programs interact with each other using the services of the transport layer.
- Transport layer provides services to the application layer and takes services from the network layer.
- Fig. 6.1.1 shows the position of the transport 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.
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

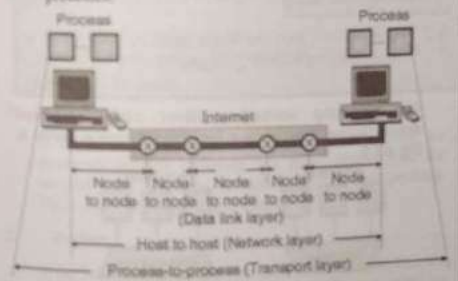
University Questions

Q. 1 Discuss the services offered by transport layer. (Dec. 05, 8 Marks, May 07, 10 Marks)

- In this section we are going to discuss the services provided by the transport layer.

6.3.1 Process-to-Process Communication :

- The data link layer performs a node to node delivery. The network layer carries out the datagram delivery between two hosts (host to host delivery).
- But the real communication takes place between two processes or application programs for which we need the **process-to-process delivery.**
- The transport layer takes care of the **process-to-process delivery.** In this a packet from one process is delivered to the other process.
- The relationship between the communicating processes is the client-server relationship. Fig. 6.3.1 demonstrates the three processes.

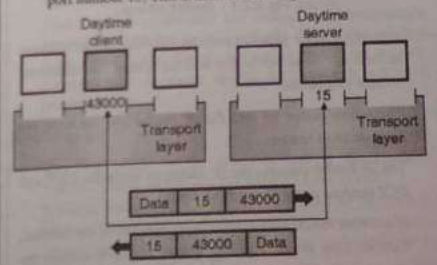


(G-594) **Fig. 6.3.1 : Types of data deliveries**

- 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 :

- There are several ways of achieving the process-to-process communication, but the most common method is using the client-server paradigm.
- **Client** is defined as the process on the local host. It needs services from another process called **server** which is on the other (remote) host.
- Both client and server have the same name. Some of the important terms related to the client-server paradigm are :
  1. Local host 2. Remote host
  3. Local process 4. Remote process
- We can use the IP addresses to define the local host and remote host. But this is not enough to define a process.
- In order to define a process, we have to use one more identifier called **Port Numbers.** In TCP/protocol suite, the port numbers are integers and they are numbered between 0 and 65,535.
- At the data link layer we need a MAC address, at the network layer we need to use an IP address. A datagram uses the destination IP address to deliver the datagram and uses the source IP address for the destination's reply.
- At the transport layer a transport layer address called a **port number** is required to be used to choose among multiple processes running on the destination host.
- The destination port number is required to make the packet delivery and the source port number is needed to return back the reply.
- In the Internet model, the port numbers are 16 bit integers. Hence the number of possible port numbers will be $2^{16} = 65{,}535$ and the port numbers range from 0 to 65,535.
- The client program identifies itself with a port number which is chosen randomly. This number is called as **ephemeral port number.** Ephemeral means short lived. It is used because life of a client is generally short.
- The server process should also identify itself with a port number but this port number can not be chosen randomly.
- The Internet uses universal port numbers for servers and these numbers are called as **well known port numbers.**
- Every client process knows the well known port numbers of the pre identified server process.
- For example, a Day time client process can use an ephemeral (temporary) port number 43000 for identifying itself, the Day time server process must use the well known (permanent) port number 15. This is illustrated in Fig. 6.3.2.



(G-595) **Fig. 6.3.2 : Concept of port numbers**

Scanned by CamScanner

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.

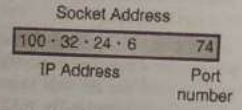
IANA Ranges :

- 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.

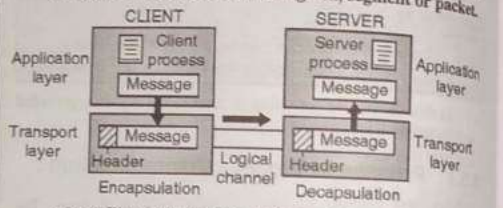
If we want to use the transport layer services in the Internet, then we have to use a pair of socket addresses namely the clients socket address and the server's socket address.

6.3.3 Encapsulation and Decapsulation :

- 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.

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.

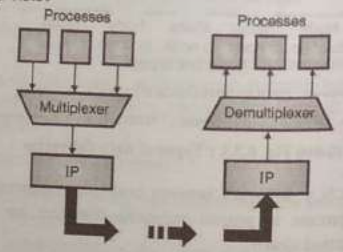
6.3.4 Multiplexing and Demultiplexing :

MU : Dec. 03

University Questions

Q. 1 How are the port numbers used by TCP/UDP in demultiplexing incoming segments. **(Dec. 03, 10 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 :

- 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 :

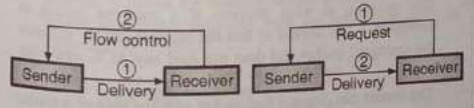
- There are two different ways of delivering the packets produced by the sender to the receiver. They are pushing or pulling.

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 requested by the receiver then the delivery is called as **pulling.** Fig. 6.3.6(b) illustrates the principle of pulling.



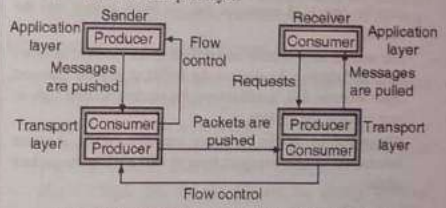
(a) Concept of pushing **(b) Concept of pulling**

(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.

Scanned by CamScanner

- 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.

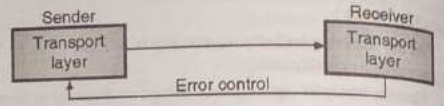
6.3.7 Error Control :

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.

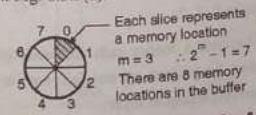
- The receiver silently discards the duplicate packets. It will either discard the out of order packets or stored until the missing packet is received.
- Note that every discarded packet is treated as a lost packet by the sender.

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.
- 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.

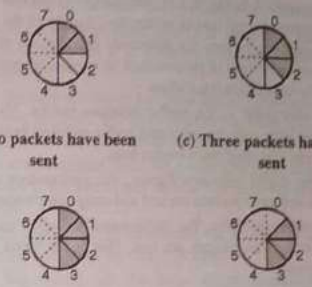
Sliding window :

- 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

Fig. 6.3.9



(b) Two packets have been sent **(c) Three packets have been sent**

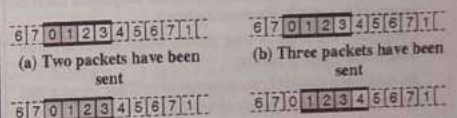
(d) Four packets have been sent. The window is full **(e) Packet 0 has been acknowledged and the window slides**

(G-2017) **Fig. 6.3.9**

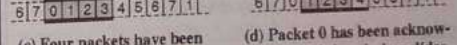
- When the acknowledgement for segment "0" arrives at the sending end, the corresponding segment (segment 0) is unmarked and window slides ahead by one slice as shown in Fig. 6.3.9(e). The size of the **sending window** is 4.
- Note that the sliding window is just an abstraction. In actual practice, 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**

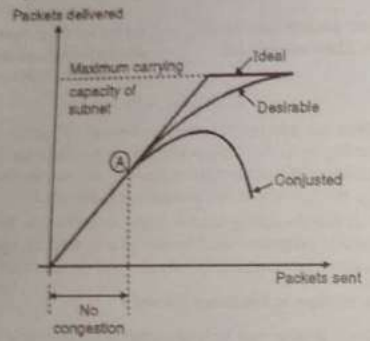
(G-2075) **Fig. 6.3.10 : Sliding windows presented in the linear format**

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.

Scanned by CamScanner

- 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.



(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 : MU : Dec. 14, May 16

University Questions

Q. 1 Differentiate between connection oriented and connectionless services. **(Dec. 14, 5 Marks)**

Q. 2 Compare connectionless and connection oriented services. **(May 16, 5 Marks)**

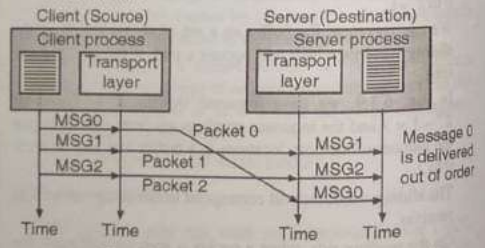
- A transport layer protocol is capable of providing two types of services :
  1. Connectionless services.
  2. Connection oriented services.
- The meaning of the words connectionless and connection oriented is different at the transport layer than that at the network layer.
- A connectionless service at the network layer means different datagrams of the same message following different paths.
- However at the transport layer, the meaning of connectionless service is independency between different packets.
- On the other hand a connection oriented service means the packets are interdependent.

Connectionless 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).

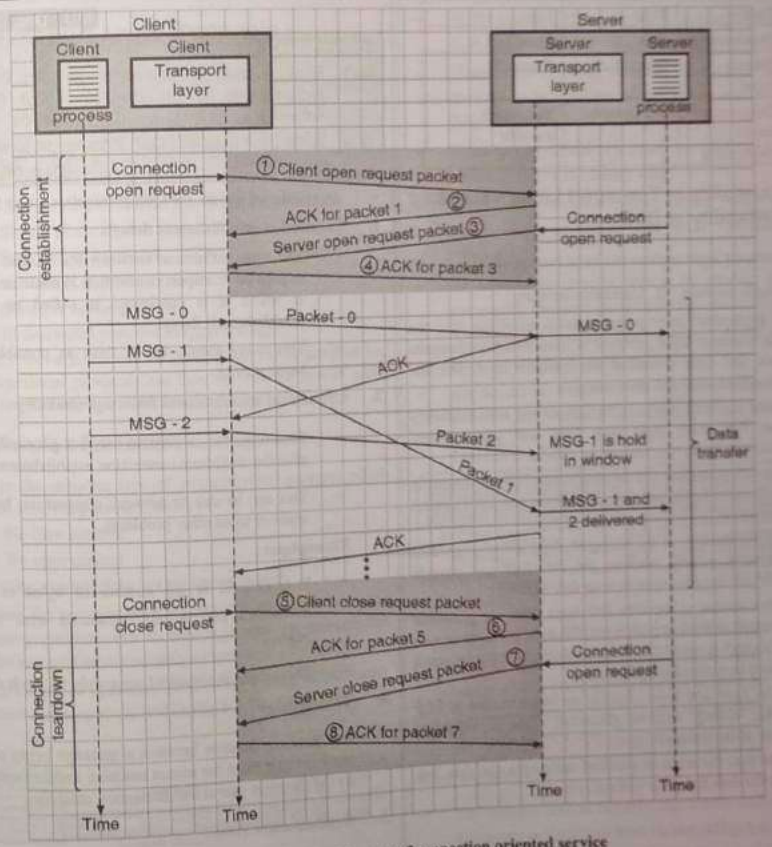
- If these chunks are of the same message then due to their out of order delivery the server will receive a strange message.

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 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

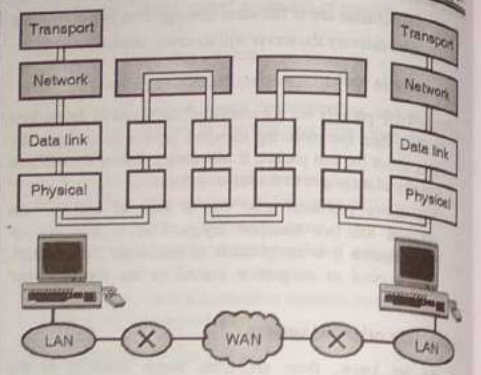
Comparison of Connection Oriented and Connectionless Services :

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.
- 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.



(G-598) **Fig. 6.3.14 : Error control**

6.3.12 Quality of Service (QoS) :

MU : Dec. 04, Dec. 06

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 note on : QoS in transport layer. **(Dec. 06, 3 Marks)**

- As mentioned earlier, the QoS parameters are as follows :

1. **Connection establishment delay :**
   - The time difference between the instant at which a request for transport connection is made and the instant at which it is confirmed is called as **connection establishment delay.**
   - This delay should be as short as possible to ensure better service.
2. **Connection establishment failure probability :**
   - Sometimes the connection may not get established even after the maximum connection establishment delay.
   - This can be due to network congestion, lack of table space or some other problems.
3. **Throughput :**
   - It is defined as the number of bytes of user data transferred per second, measured over some time interval.
   - Throughput is measured separately for each direction.
4. **Transit delay :**

   It is the time duration between a message being sent by the transport user from the source machine and its being received by the transport user at the destination machine.
5. **Residual error ratio :**
   - It measures the number of lost or garbled messages as a percentage of the total messages sent.

   - Ideally the value of this ratio should be zero and practically it should be as small as possible.
6. **Protection :**

   This parameter provides a way to protect the transmitted data against reading or modifying it by some unauthorised parties.
7. **Priority :**
   - Using this parameter the user can show that some of its connections are more important (have higher priority) than the other ones.
   - This is important when congestions take place. Because the higher priority connections should get service before the low priority connections.
8. **Resilience :**

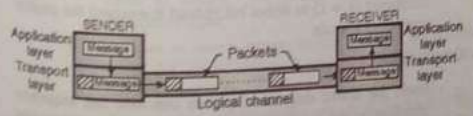
   Due to internal problem or congestion the transport layer spontaneously terminates a connection. The resilience parameter gives the probability of such a termination.

6.4 Transport Layer Protocols :

- We have discussed a few transport layer services in the previous section. By combining a set of these services as per requirement, we can create a transport layer protocol.
- It is important to understand the behavior of these general protocols, before we discuss the transport layer protocols such as UDP and TCP.
- In this section we will discuss the following protocols :
  1. Simple protocol.
  2. Stop and wait protocol.
  3. Go back N (GBN) protocol.
  4. Selective repeat protocol.
  5. Bidirectional protocol. (Piggybacking).
- 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.

6.4.1 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. 6.4.1(a).



(G-2179) **Fig. 6.4.1(a) : Layout of the simple protocol**

Operation :

At the sender :

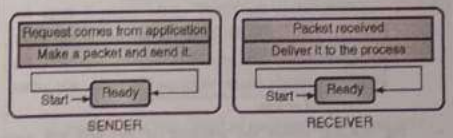
- The application layer at the sender, sends its message to the transport layer.
- The sender transport layer receives the message and makes a packet out of it.
- This packet is then sent over the logical channel between the transport layers on the two ends.

At the receiver :

- The network layer at the receiver (not shown in Fig. 6.4.1(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.

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. 6.4.1(b) : FSM for the simple protocol**

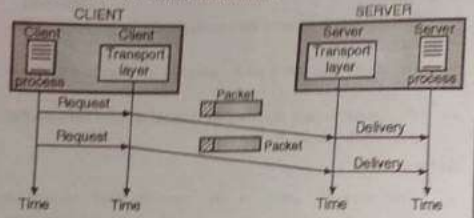
- Note that the UDP protocol is a slight modification of this protocol. The FSM (Finite State Machine) for this protocol has been shown in Fig. 6.4.1(b) and its flow diagram is as shown in Fig. 6.4.1(c).

Flow Diagram :

- The communication between the sender and receiver using the simple protocol has been shown in Fig. 6.4.1(c).

Scanned by CamScanner

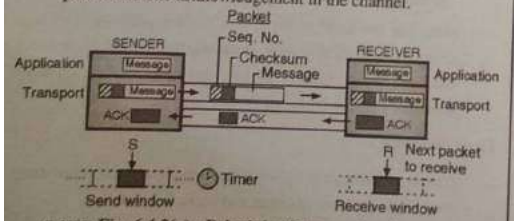
- The sender keeps sending the packets, without taking the receiver into consideration at all.



(G-2181) **Fig. 6.4.1(c) : Flow diagram for the simple protocol**

6.4.2 Stop and Wait Protocol :

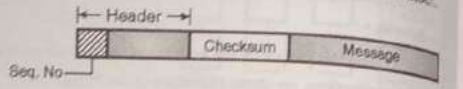
- The second transport layer protocol that we will discuss now is a **connection oriented** protocol called as **stop and wait protocol.**
- The operation of this protocol are as follows :
  1. It is a connection oriented protocol.
  2. It provides both flow and error control.
  3. Sender sends one packet 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. 6.4.2(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. 6.4.2(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. 6.4.2(b), an additional field is created in the packet header of each packet to hold its sequence number.



(G-2183) **Fig. 6.4.2(b) : Packet**

- 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. 6.4.2(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. 6.4.2(a).

FSMs of stop and wait protocol :

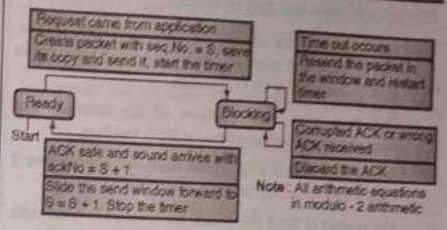
- This protocol is a connection oriented protocol. Therefore a connection between the two ends should be established before transferring the data.
- In other words both sender and receiver must be in the **established state** before the beginning of data exchange.

1. Sender FSM :

- The sender's FSM is shown in Fig. 6.4.2(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."
- It stores a copy of this packet and sends the packet. The sender starts the timer and moves into its **blocking state.**



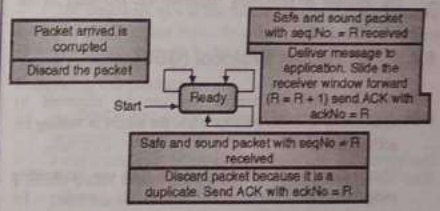
(G-2184) **Fig. 6.4.2(c) : Sender's FSM for stop and wait protocol**

2. Blocking state :

- When the sender is in the blocking state as shown in Fig. 6.4.2(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 condition), the sender resends the only outstanding packet with it. It then restarts the timer as shown in Fig. 6.4.2(c).

2. Receiver FSM :

- The receiver's FSM is shown in Fig. 6.4.2(d). Note that there is no blocking state in the receiver's FSM. There is only the ready state.
- At the receiver also there is a possibility of following three events happening after the arrival of a packet.



(G-2185) **Fig. 6.4.2(d) : FSM of receiver for stop and wait protocol**

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.

Scanned by CamScanner

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 :

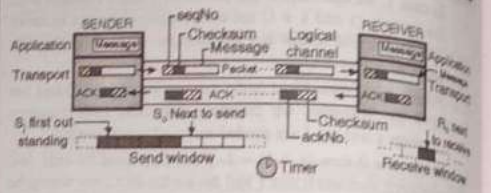
- In networking and even other areas, a task is started before the ending of previous task. This is known as **pipelining.**
- In the stop and wait protocol, the senders sends a packet and waits for its acknowledgement before sending the next packet.
- This shows that there is no pipelining in the stop 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.

6.4.3 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.

A copy of every sent packet is kept by the sender until it receives the acknowledgement of that packet.

Fig. 6.4.3(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. 6.4.3(a) : Principle of Go Back-N (GBN) protocol**

Sequence numbers :

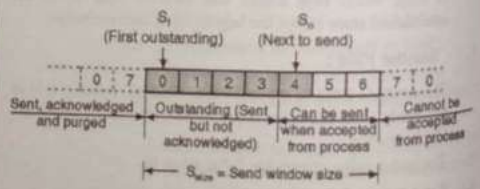
In GBN protocol, the sequence numbers are modulo 2^m, where **m** denotes the size of sequence number field in bits.

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. 6.4.3(b). Note that the window size = $2^m - 1 = 2^3 - 1 = 7$.



(G-2187) **Fig. 6.4.3(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. 6.4.3(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.

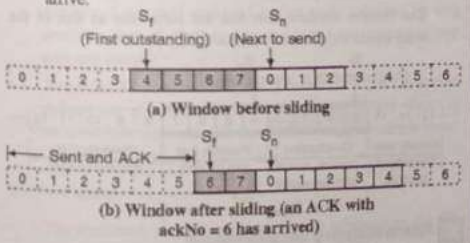
- The second region which is shaded in Fig. 6.4.3(b) contains the sequence numbers belonging to the packets that are already sent but not acknowledged by the receiver. That means the exact status of these packets is not known.
- These packets are called as **outstanding packets.**
- The third range, which is not shaded in Fig. 6.4.3(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. 6.4.3(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. 6.4.4 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.



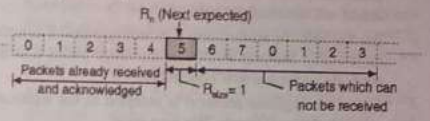
(G-2188) **Fig. 6.4.4 : Sliding of send window**

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. 6.4.5. It has only one variable R_n, i.e. receive window, next packet expected.



(G-2189) **Fig. 6.4.5 : 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.

Scanned by CamScanner

- 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 :

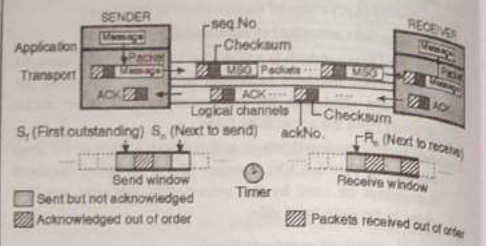
- The GBN and stop and wait protocols are somewhat similar to each other.
- The stop and wait protocol is actually a GBN protocol with only two sequence numbers (0 and 1) and send window size of 1.
- In stop and wait protocol, the modulo 2 arithmetic is used whereas in GBN protocol, modulo 2^m arithmetic is said to have been used.
- Thus stop and wait protocol is a GBN protocol with m = 1.

6.4.4 Selective Repeat Protocol : MU : May 17

University Questions

Q. 1 Explain selective repeat protocol. **(May 17, 5 Marks)**

- 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 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. 6.4.6 : Outline of selective repeat protocol**

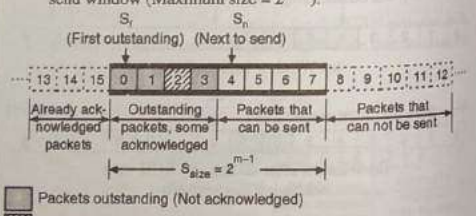
- The principle of selective repeat protocol has been illustrated in Fig. 6.4.6.

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. 6.4.6(a) shows the structure of the send window.
- Fig. 6.4.6(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}).

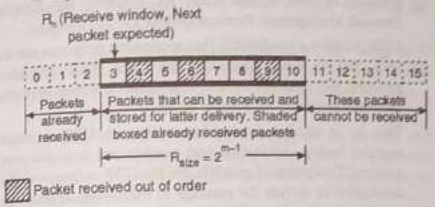


(G-2191) **Fig. 6.4.6(a) : Send window for selective repeat protocol**

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. 6.4.6(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. 6.4.6(b) : Receive window for selective repeat protocol**

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.

6.4.5 Bidirectional Protocols :

- 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.

6.4.6 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.

6.5 User Datagram Protocol (UDP) :

MU : May 14

University Questions

Q. 1 Write short notes on : UDP. **(May 14, 5 Marks)**

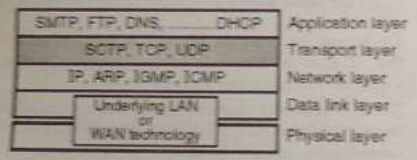
- The User Datagram Protocol is a very simple protocol. It adds little to the basic functionality of IP. Like IP, it is an unreliable, connectionless protocol.
- You do not need to establish a connection with a host before exchanging data with it using UDP, and there is no mechanism for ensuring that data sent is received.
- A unit of data sent using UDP is called a Datagram. UDP adds four 16-bit header fields (8 bytes) to whatever data is sent.
- These fields are : a length field, a checksum field, and source and destination port numbers. "Port number", in this context, represents a software port, not a hardware port.
- The concept of port numbers is common to both UDP and TCP. The port numbers identify which protocol module sent (or is to receive) the data.

Scanned by CamScanner

- 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. 6.5.1. 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. 6.5.1 : Relation between UDP and other protocols**

6.5.1 Responsibilities of UDP :

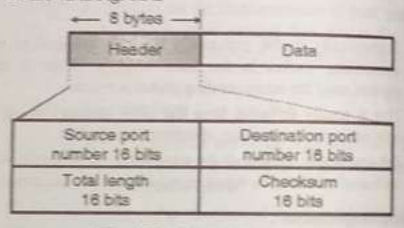
- Being a transport layer protocol, the UDP has the following responsibilities :
  1. To create a process to process communication, UDP uses port numbers to accomplish this.
  2. To provide control mechanisms at the transport layer, UDP does not provide flow control or acknowledgements. It provides error detection. The erroneous packet is discarded.
  3. UDP does not add anything to the services of IP except for providing process to process communication.

6.5.2 Advantages of UDP :

- UDP, despite all its simplicity and powerlessness is still used because it offers the following advantages :
  1. UDP has minimum overheads.
  2. UDP can be easily used if the sending process is not too bothered about reliability.
  3. UDP reduces interaction between sender and receiver.

6.5.3 User Datagram :

- User Datagram Protocol (UDP) provides a connectionless packet service that offers unreliable 'best effort' delivery. This means that the arrival of packets is not guaranteed, nor is the correct sequencing of delivered packets.
- Applications that do not require an acknowledgement of receipt of data, for example, audio or video broadcasting uses UDP.
- UDP is also used by applications that typically transmit small amounts of data at one time, for example, the Simple Network Management Protocol (SNMP).
- UDP provides a mechanism that application programs use to send data to other application programs. UDP provides protocol port numbers used to distinguish between multiple programs executing on a single device.
- That is, in addition to the data sent, each UDP message contains both a destination port number and a source port number. This makes it possible for the UDP software at the destination to deliver the message to the correct application program, and for the application program to send a reply.
- UDP packets are called as **user datagrams.** They have a fixed-size header of 8-bytes. The format of user datagram is as shown in Fig. 6.5.2



(G-424) **Fig. 6.5.2 : User datagram format**

- The UDP header is divided into the following four 16-bit fields :
  1. Source port
  2. Destination port
  3. Total length
  4. Checksum.

Source Port 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 :

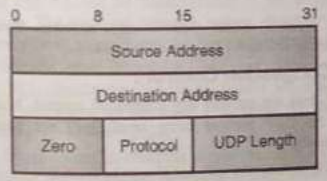
  UDP length = IP length – IP header length
- Note that while delivering the UDP datagram to UDP layer, the IP software drops the IP header.

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.

6.5.4 UDP Pseudo Header :

- The purpose of using a pseudo-header is to verify that the UDP packet has reached its correct destination.
- The correct destination consists of a specific machine and a specific protocol port number within that machine.



(G-625) **Fig. 6.5.3 : UDP pseudo header**

- The UDP header itself specifies only the protocol port number. Thus, to verify the destination, UDP on the sending machine computes a checksum that covers the destination IP address as well as the UDP packet.
- At the ultimate destination, UDP software verifies the checksum using the destination IP address obtained from the header of the IP packet that carried the UDP message.
- If the checksum agrees, then it must be true that the packet has reached the intended destination host as well as the correct protocol port within that host.

User Interface :

- A user interface should allow the creation of new receive ports, receive operations on the receive ports that return the data octets and an indication of source port and source address, and an operation that allows a datagram to be sent, specifying the data, source and destination ports and addresses to be sent.

IP Interface :

- The UDP module must be able to determine the source and destination Internet addresses and the protocol field from the Internet header.
- One possible UDP/IP interface would return the whole Internet datagram including the entire Internet header in response to a receive operation. Such an interface would also allow the UDP to pass a full Internet datagram complete with header to the IP to send.
- The IP would verify certain fields for consistency and compute the Internet header checksum.

Protocol Application :

- The major uses of this protocol are the Internet Name Server, and the Trivial File Transfer.

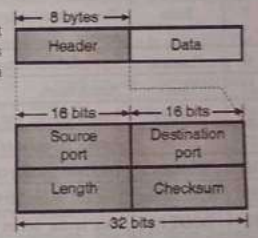
Protocol Number :

- This is protocol 17 (21 octal) when used in the Internet Protocol.

Ex. 6.5.1 : The dump of a UDP header in hexadecimal format is as follows :
B C 8 2 0 0 0 D 0 0 2 B 0 0 1 D
Obtain the following from it :
1. Source port number
2. Destination port number
3. Total length
4. Length of the data.
5. Packet direction.
6. Name of client process.

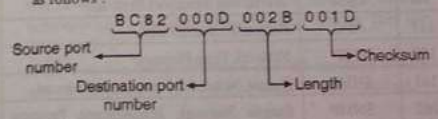
Soln. :

- The standard format of UDP header has been shown in Fig. P. 6.5.1.



(G-2020) **Fig. P. 6.5.1 : UDP header format**

- Therefore we can split the given UDP header in 4 equal parts as follows :



(G-2021)

1. Source port number = $(BC82)_{16}$ ...Ans.

Scanned by CamScanner

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 6.6.1 which shows that for well known port number 13, the corresponding client process is "Daytime".

6.6 UDP Services :

- In this section we are going to discuss the following important services provided by the UDP :
  1. Process to process communication.
  2. Connectionless services.
  3. Flow control.
  4. Error control.
  5. Checksum.
  6. Congestion control.
  7. Encapsulation and decapsulation.
  8. Queuing.
  9. Multiplexing and demultiplexing.

6.6.1 Process to Process Communication :

- We have already discussed the process to process communication in a general sense, earlier in this chapter.
- UDP also does it with the help of sockets which is a combination of IP address and port numbers. Table 6.6.1 shows different port numbers used by UDP.

Some of these ports can be used by UDP as well as TCP.

Table 6.6.1 : Well known ports used with UDP

Port	Protocol	Description
7	Echo	The received datagram is echoed back to sender.
9	Discard	Any received datagram is discarded.
11	Users	Active users.
13	Daytime	Return the day and the current time.
17	Quote	Return the quote of the day.
19	Chargen	To return a string of characters.
53	Nameserver	Domain Name Service (DNS).
67	BOOT PS	This is the server port to download the bootstrap information.
68	BOOT PC	This is the client port to download bootstrap information.
69	TFTP	Trivial File Transport Protocol.
111	RPC	Remote Procedure Call.
123	NTP	Network Time Protocol.
161	SNMP	Simple Network Management Protocol.
162	SNMP	Simple Network Management Protocol (Trap).

6.6.2 Connectionless Services :

- As UDP is a connectionless, unreliable protocol, each user datagram sent using UDP is an independent datagram.
- Different user datagrams sent by the UDP have absolutely no relationship between them. This is true even for those datagrams which are originating from the same process and being sent to the same destination. The user datagrams do **not have any number.**
- Also the connection establishment and release are not at all required. So each datagram is free to travel any path.
- Only those processes which are sending very short messages can successfully use the UDP.

6.6.3 Flow and Error Control :

- Being a connectionless protocol, UDP is a simple, unreliable protocol. It does not provide any flow control, hence the receiver can overflow with incoming messages.
- UDP does not support any other error control mechanism, except for the checksum.
- There are no acknowledgements sent from destination to sender. Hence the sender does not know if the message has reached, lost or duplicated. If the receiver detects any error using the checksum, then that particular datagram is discarded.

6.6.4 Checksum :

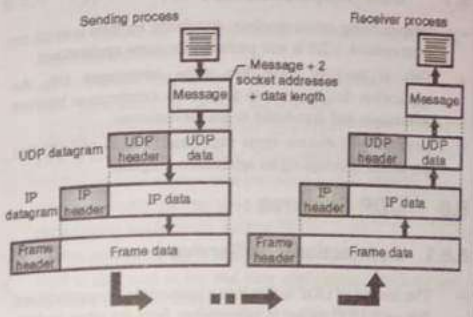
- The calculation of checksum for UDP is different than that for IP. In UDP the checksum is calculated by considering the following three sections :
  1. A pseudoheader
  2. The UDP header.
  3. The data coming from the application layer.
- The checksum in UDP is **optional.** That means the sender can make a decision of not calculating the checksum. If so, then the checksum field is filled with all zeros before sending the UDP packet.
- In case if the calculated checksum is all zeros (when the sender decides to send checksum) then an all 1 checksum is sent.
- This solution works without any problem because, a checksum will never have an all 1 value.

6.6.5 Congestion Control :

- UDP does not provide any congestion control. It assumes that the UDP packets being small, will not create any congestion.
- But this assumption may not always be correct.

6.6.6 Encapsulation and Decapsulation :

- The UDP encapsulates and decapsulates messages in an IP datagram in order to exchange the message between two communicating processes.
- This is as shown in Fig. 6.6.1. We will discuss the two processes separately.



(a) Encapsulation (b) Decapsulation

(G-2022) Fig. 6.6.1

Encapsulation :

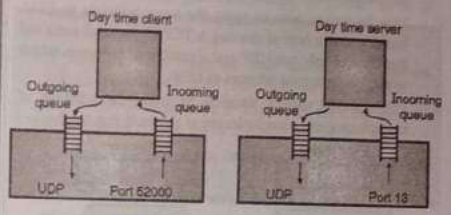
- Refer Fig. 6.6.1(a). The message produced by a process is to be sent with the help of UDP. The process passes the message and two socket addresses alongwith the length of data to UDP.
- UDP receives this data and adds the UDP header to it as shown. This is called as UDP datagram which is passed to IP with the socket address.
- IP adds its own header to UDP datagram as shown. It enters value 17 into the protocol field. This is an indication that UDP is being used. The IP datagram is then passed on to the data link layer.
- The DLL adds its own header and possibly a trailer to create a frame and sends it to the physical layer.
- Finally the physical layer converts these bits into electrical or optical signals and sends them to the destination machine.

Decapsulation :

- Refer Fig. 6.6.1(b) for understanding of the decapsulation process. The encoded message arrives at the destination physical layer where it decodes the electrical/optical signals into bits and passes them to the DLL.
- The DLL checks the data using header and trailer. The header and trailer are discarded if no errors are found, and the datagram is passed to IP.
- The IP carries out its checking to find the errors and if none are found, the datagram is passed on to UDP, after dropping the IP header.
- The datagram from IP to UDP also contains the sender and receiver IP addresses. This entire user datagram is checked by the UDP with the help of checksum.
- If there is no error detected, then the UDP header is dropped and the application data plus senders socket address are handed over to the process.
- The process can use this senders socket address if it wants to respond to the message received.

6.6.7 Queuing :

- The queues in UDP are related with ports as shown in Fig. 6.6.2.



(G-626) Fig. 6.6.2 : Queues in UDP

- A process starts at the client site by requesting a port number from the operating system. In some implementations both incoming and outgoing queues are created in association with each process.
- Every process gets only one port number and hence it can create one outgoing and another incoming queue. The queues function only when the process is running. They are destroyed as soon as the process is terminated.
- The client process uses the source port number mentioned in the request to send message to its outgoing queue.
- UDP removes the queue messages one by one by adding the UDP header and delivers them to IP.
- If the outgoing queue overflows, then operating system tells that client process to wait before sending the next message.
- When the client receives a message, UDP checks if the incoming queue has been created or not. If the queue has been created, then the UDP sends the received datagram to the end of the queue.
- If the queue is not present then UDP will simply discard the user datagram. If the incoming queue overflows, then UDP discards the user datagram and arranges to send the port unavailable message to the server.
- The mechanism to create the server queue is different. The server creates the incoming and outgoing queues using its well known port as soon as it starts running. The queues exist as long as the server is running.
- When a message is received at the server, the UDP checks if the incoming queue has been created or not.
- If the queue is not present, the UDP discards the user datagram. If the queue is present then UDP sends the datagram at the end of the queue.
- If the incoming queue overflows, then UDP drops the user datagram and arranges to send the port unavailable message to the client.
- When the server wants to send a message to client it sends that message to the outgoing queue. These messages are then removed one by one after adding the UDP header. They are delivered to IP.
- If the outgoing queue overflows then the operating system will ask the server to wait before it sends the next message.

Scanned by CamScanner

6.6.6 Multiplexing and Demultiplexing :

- We have discussed the general principle of multiplexing and demultiplexing in the transport layer.
- Now let us see how it 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. 6.6.7.

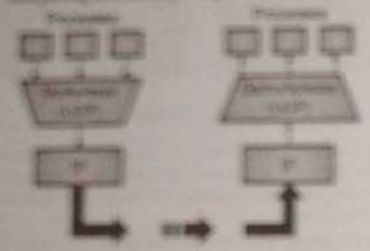


Fig. 6.6.7 : Multiplexing and demultiplexing

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 then 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. 6.6.7.

Demultiplexing :

- At the receiving end, the relationship is one to many. So we need a demultiplexer.
- First the UDP layer receives datagrams from the IP.
- The UDP then checks for errors and drops the header to obtain the messages and delivers them to appropriate process based on the port number.

6.6.5 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.

6.7 UDP Applications :

- Despite being connectionless, unreliable, no flow control, no error control, UDP is still preferred for some applications.
- This is because UDP has some advantages. So the 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.

6.8 UDP Features :

6.8.1 Connectionless Service :

- The feature of UDP is that it is a connectionless protocol, so that each UDP packet is independent from the other packets. This 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 a 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 connection-oriented 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.

6.8.2 Lack of Error Control :

- UDP is an unreliable protocol which does not provide any error control. Now this is actually a disadvantage but it becomes an advantage for some applications as explained below.
- If TCP is used for reliable service and if a packet is lost, then TCP will resend it. So the receiver transport layer is unable to deliver that part of the message to the application immediately. Due to this an uneven delay is introduced between different parts of the messages which is undesirable for some delay sensitive applications.
- This delay is actually a side effect of the reliable operation of TCP.
- Some applications are not affected by this delay but for some others it is very crucial.

6.8.3 Lack of Congestion Control :

- We know that there is no provision for congestion control in UDP. But this disadvantage can become an advantage for some applications.
- A good side effect of lack of congestion control is that UDP does not create any additional traffic that is created by TCP for congestion control.
- Hence the UDP is preferred for some congestion prone networks.

6.8.4 Typical Applications of UDP :

1. UDP is suitable for the applications (processes) that have the following requirements :
   (a) A simple response to request is to be made.
   (b) Flow and error controls are 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.

6.9 Transmission Control Protocol (TCP) :

- The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model.
- Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.
- TCP is the layer 4 protocol in the TCP/IP suite and it is a very important and complicated protocol. TCP has been revised multiple times in last few decades.
- With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers.
- This service benefits applications because they do not have to chop data into blocks before handing it off to TCP. Instead, TCP groups bytes into segments and passes them to IP for delivery.
- TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork.
- It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive.
- Bytes not acknowledged within a specified time period are retransmitted.
- The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or corrupted packets. A time-out mechanism allows devices to detect lost packets and request retransmission.
- TCP offers efficient flow control, which means that, when sending acknowledgments back to the source, the receiving TCP process indicates the highest sequence number that it can receive without overflowing its internal buffers.
- TCP supports a full-duplex operation means that TCP processes can both send and receive at the same time.
- Finally, TCP's multiplexing means that numerous simultaneous upper-layer conversations can be multiplexed over a single connection.

6.9.1 Relationship Between TCP and IP :

- The relationship between TCP and IP is very interesting. Each TCP message gets encapsulated or wrapped in an IP datagram and then this datagram is sent over the network to the destination.
- IP interprets this datagram (from packet to packet) without knowing 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 datagram from one computer to the other.
- Thus TCP treats IP as the source and destination addresses of the data unit (packets of data).
- Many applications such as FTP, Telnet, login (TELNET) or Long sending data to TCP software on the sending computer.
- The TCP software acts as a multiplexer at the sending computer. It receives data from various applications, multiplexes the data and hands it over to the IP software at the sending end as shown in Fig. 6.9.1.
- IP adds its own header to this TCP packet and related up IP packet out of it. Then this packet is sent to the destination.
- At the destination exactly opposite process will take place. The IP software hands over the multiplexed data to the TCP software.
- The TCP software at the destination computer then demultiplexes the multiplexed data and gives it to the corresponding applications as shown in Fig. 6.9.1.

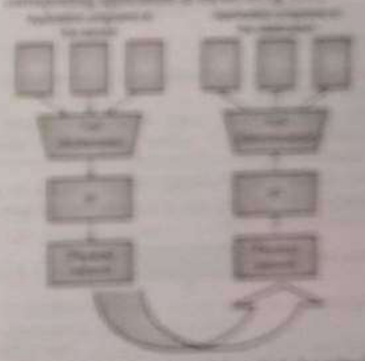


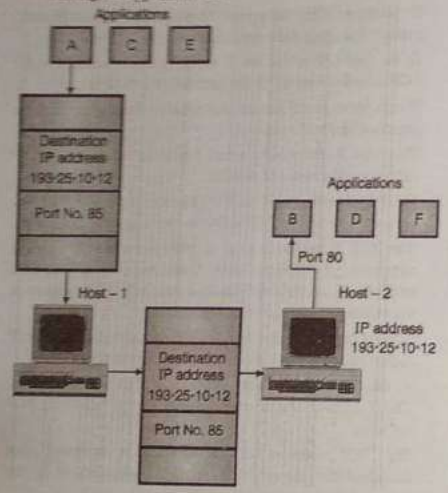
Fig. 6.9.1 : Multiplexing and demultiplexing using TCP

6.9.2 Ports and Sockets :

1. **Ports :**
   - Applications running on different hosts communicate with TCP with the help of ports. Every application has been allocated 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 computer, then port plays a key role.
   - Let an application A on host 1 wants to communicate with an application B on host 2. In the process other ports as shown in Fig. 6.9.2 and explained below.

Scanned by CamScanner

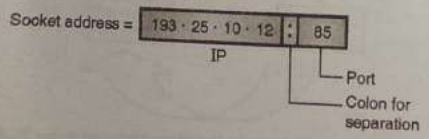
- Application A running on computer 1 provides the IP address of computer 2 and the port number corresponding to application B as shown in Fig. 6.9.2.
- Computer 1 communicates with computer 2 using the IP address and computer 2 uses the port number to direct the message to application B.



(G-1437) **Fig. 6.9.2 : Use of port numbers**

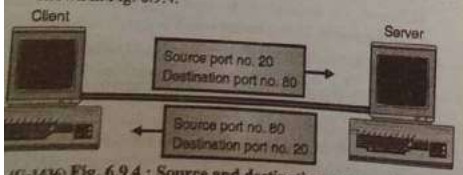
2. Sockets :

- A port is a 16 bit unique number used for identification of a single application.
- But socket address or simply socket would identify the combination of the IP address and the port number concatenated together as shown in Fig. 6.9.3.
- For example if the IP address = 193.25.10.12 and the port number is 85. Then this port of this computer will have the following socket address.



(G-1438) **Fig. 6.9.3**

- So a pair of sockets is required to identify a TCP connection between two applications on two different hosts. These two socket addresses specify the end points of the connection as shown in Fig. 6.9.4.



(G-1436) **Fig. 6.9.4 : Source and destination port numbers**

- Generally the server port numbers are known as the **well known ports.** Some of the well known port numbers have already been mentioned for UDP and TCP earlier in this chapter.
- Multiple TCP connections between different applications or same applications on two hosts exist in practice. Here the IP addresses of the two hosts are same but the port numbers are different.
- The communication using port numbers is illustrated in Fig. 6.9.4

6.10 TCP Services :

Following are some of the services offered by TCP to the processes at the application layer :

1. Stream delivery service
2. Sending and receiving buffers
3. Bytes and segments
4. Full duplex service
5. Connection oriented service
6. Reliable service.
7. Process to process communication.

6.10.1 Process to Process Communication :

- The TCP uses port numbers a transport layer addresses. Table 6.10.1 shows some well known port numbers used by TCP.
- Note that if an application can use both UDP and TCP, the same port number is assigned to this application.

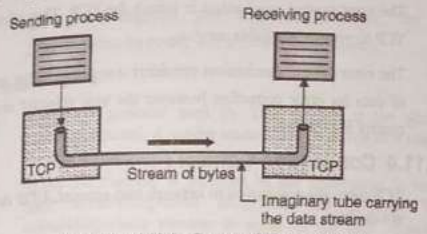
Table 6.10.1 : Well known ports used by TCP

Port	Protocol	Description
7	Echo	Sends received datagram back to sender
9	Discard	Discards any received packet
11	Users	Active users
13	Daytime	Sends the date and the time
17	Quote	Sends a quote of the day
19	Chargen	Sends a string character
20	FTP, Data	File Transfer protocol for data
21	FTP, Control	File Transfer protocol for control
23	TELNET	Terminal network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

6.10.2 Stream Delivery Service :

- TCP is a stream oriented protocol. The sending process delivers data in the form of a stream of bytes and the receiving process receives it in the same manner.

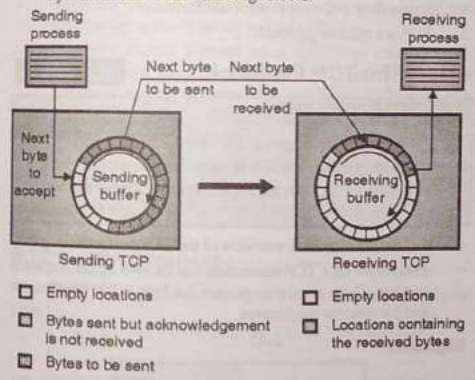
- TCP creates a working environment in such a way that the sending and receiving processes seem to be connected by an imaginary "tube" as shown in Fig. 6.10.1.
- This is called as stream delivery service.



(G-621) **Fig. 6.10.1 : Stream delivery service**

6.10.3 Sending and Receiving Buffers :

- The sending and receiving processes may not produce and receive data at the same speed.
- Hence TCP needs buffers for storage of data at both the ends. There are two types of buffers used in each direction :
  1. Sending buffer 2. Receiving buffer.
- A buffer can be implemented by using a circular array of 1 byte locations as shown in Fig. 6.10.2.

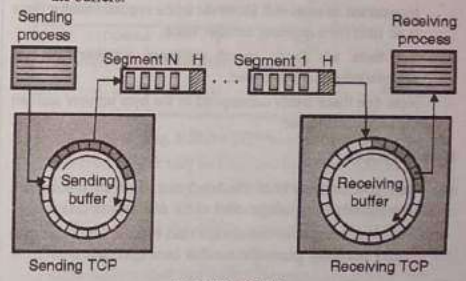


(G-622) **Fig. 6.10.2 : Sending and receiving buffers**

- Fig. 6.10.2 shows the direction of movement of data. The sending buffer has three types of locations :
  1. Empty locations
  2. Locations containing the bytes which have been sent but not acknowledged. These bytes are kept in the buffer till an acknowledgement is received.
  3. The locations containing the bytes to be sent by the sending TCP.
- In practice, the TCP may be able to send only a part of data which is to be sent, due to slowness of the receiving process or congestion in the network.
- The buffer at the receiver is divided into two parts :
  1. The part containing empty locations.
  2. The part containing the received bytes which can be consumed by the sending process.

6.10.4 Bytes and Segments :

- Buffering is used to handle the difference between the speed of data transmission and data consumption.
- But only buffering is not enough. We need one more step before sending the data.
- The IP layer, which provides service to TCP, has to send data in the form of packets instead of stream of bytes.
- At the transport layer, TCP groups a number of bytes to form a packet called a segment.
- A header is added to each segment for the purpose of exercising control.
- The segments are then inserted in an IP datagram and transmitted. The entire operation is transparent to the receiving process.
- The segments may be received out of order, lost or corrupted when it reaches the receiving end.
- Fig. 6.10.3 shows the creation of segments from the bytes in the buffers.



(G-623) **Fig. 6.10.3**

- The segments are not of the same size. Each segment can carry hundreds of bytes.

6.10.5 Full Duplex Service :

- TCP offers full duplex service where the data can flow in both the directions simultaneously.
- Each TCP will then have a sending buffer and receiving buffer. The TCP segments can travel in both the directions, therefore TCP provides a full duplex service.

6.10.6 Connection Oriented Service :

- TCP is a connection oriented protocol. When process – 1 wants to communicate (send and receive) with another process (process – 2), the sequence of operations is as follows :
  1. TCP of process – 1 informs TCP of process – 2 and create a connection between them.
  2. TCP of process – 1 and TCP of process – 2 exchange data in both the directions.

Scanned by CamScanner

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.

6.10.7 Reliable Service :

TCP is a reliable transport protocol and not unreliable like UDP. Different acknowledgements are used by the receiver to convey sender the status of data.

6.11 Features of TCP :

In order to provide the services mentioned in the previous section, TCP has a number of features as follows :

6.11.1 Numbering System :

- The TCP software keeps track of the segments being transmitted or received. However in the segment header there is no field for a segment number value.
- But there are fields called **sequence number** and the **acknowledgement number.**
- Note that these fields correspond to the byte number and not the segment number.

Byte numbers :

- TCP give numbers to all the data bytes which are transmitted. The numbering is independent of the direction of data travel.
- The numbering does not always start from 0, but it can start with a randomly generated number between 0 and $2^{32} - 1$.

Sequence number :

- After numbering the bytes, the TCP assigns a sequence number to each segment that is being transmitted.
- The sequence number for each segment is same as the number assigned to the first byte present in that segment.

Acknowledgement number :

- The TCP communication is duplex. So both the communicating processes can send and receive data at the same time.
- Each process will give numbers to the bytes with a different starting byte number.
- Each party also uses an acknowledgement number to confirm the reception of bytes.

The acknowledgement number is cumulative i.e. the receiver takes the number of the last byte received, adds 1 to it and uses this sum as the acknowledgement number.

6.11.2 Flow Control :

- TCP provides flow control (UDP does not). The receiver will control the amount of data to be sent by the sender.
- This will avoid data overflow at the receiver. The TCP uses byte oriented flow control.

6.11.3 Error Control :

- The error control mechanism is inbuilt for TCP. This allows TCP to provide a reliable service.
- The error control mechanism considers a segment as the unit of data for error correction however the byte oriented error control is provided.

6.11.4 Congestion Control :

- TCP takes the congestion in network into account. UDP does not do this.
- The amount of data sent by the sender depends on the following factors :
  1. The receivers decision (flow control).
  2. The network congestion.

Summary of TCP features :

1. TCP is a process-to-process protocol.
2. TCP uses port numbers.
3. It is a connection oriented protocol (creates a virtual connection).
4. It uses flow and error control mechanisms.
5. TCP is a reliable protocol.

6.12 The TCP Protocol : MU : May 15

University Questions

Q. 1 "A datagram cannot be larger than the MTU of network over which it is sent". Is the statement true or false ? Explain with the help of suitable example. **(May 15, 5 Marks)**

- Let us take a general overview of the TCP protocol.
- Every byte on a TCP connection has its own 32-bit sequence number. These numbers are used for both acknowledgement and for window mechanism.

Segments :

- The sending and receiving TCP entities exchange data in the form of segments. A segment consists of a fixed 20 byte header (plus and optional part) followed by zero or more data bytes.

Segment size :

- The segment size is decided by the TCP software. Two limits restrict the segment size as follows :
  1. Each segment including the TCP header, must fit in the 65535 byte IP payload.
  2. Each segment must fit in the MTU (**Maximum Transfer Unit**). Each network has a maximum transfer unit. Practically an MTU which is a few thousand bytes defines the upper limit on the segment size.

Fragmentation :

- If a segment is too large, then it should be broken into small segments. Using fragmentation by a router.
- Each new segment gets a new IP header. So the fragmentation by router will increase the overhead.

Timer :

- The basic protocol used by TCP entities is the sliding window protocol. A sender starts a timer as soon as a sender transmits a segment.
- When the segment is received by the destination, it sends back acknowledgement alongwith data if any. The acknowledgement number is equal to the next sequence number it expects to receive.
- If the timer at the sender goes out before the acknowledgement reaches back, it will **retransmit** that segment again.

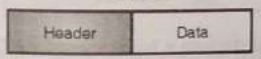
Possible problems :

- As the segments can be fragmented, a part of the transmitted segment only may reach the destination with the remaining part lost.
- Segments can arrive out of order.
- Segments can get delayed so much that timer is out and unnecessary retransmission will take place.
- If a retransmitted segment takes a different route than the original segment is fragmented then the fragments of original and retransmitted segments can reach the destination in a sporadic way. So a careful administration is required to achieve reliable byte stream.
- There is a possibility of congestion or broken network along the path.
- TCP should be able to solve these problems in an efficient manner.

6.12.1 TCP Segment :

The TCP segment as shown in Fig. 6.12.1 consists of two parts :

1. Header 2. Data



(G-1423)**Fig. 6.12.1 : TCP segment**

6.12.2 The TCP Segment Header :

MU : May 04, Dec. 04, May 05, May 08, May 10, Dec. 11, May 15, Dec. 15, May 16, May 17

University Questions

Q. 1 Describe the TCP segment header in detail. **(May 04, 10 Marks)**

Q. 2 Explain TCP segment header format in detail. **(Dec. 04, Dec. 15, 10 Marks)**

Q. 3 Draw and explain TCP header. **(May 05, 10 Marks)**

Q. 4 State different TCP Flags. **(May 08, 10 Marks)**

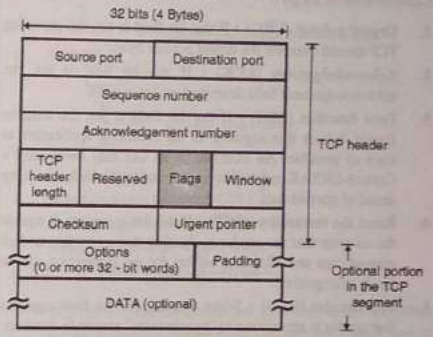
Q. 5 Explain TCP header format. **(May 10, 10 Marks)**

Q. 6 Explain TCP header or explain TCP timers. **(Dec. 11, 10 Marks)**

Q. 7 Draw and explain TCP segment header. **(May 15, May 16, 10 Marks)**

Q. 8 Draw and explain TCP segment header. **(May 17, 10 Marks)**

- Fig. 6.12.2 shows the layout of a TCP segment. Every segment begins with a 20 byte fixed format header.



(G-611)**Fig. 6.12.2 : TCP header format**

- The fixed header may be followed by header options.
- After the options, if any, upto 65535 – 20 – 20 = 65495 data bytes may follow. Note that the first 20 bytes correspond to the IP header and the next 20 correspond to the TCP header.
- The TCP segment without data are used for sending the acknowledgements and control messages.

Source port : A 16-bit number identifying the application the TCP segment originated from within the sending host. The port numbers are divided into three ranges, well-known ports (0 through 1023), registered ports (1024 through 49,151) and private ports (49,152 through 65,535). Port assignments are used by TCP as an interface to the application layer.

Destination port : A 16-bit number identifying the application the TCP segment is destined for on a receiving host. Destination ports use the same port number assignments as those set aside for source ports.

Sequence number : A 32-bit number identifying the current position of the first data byte in the segment within the entire byte stream for the TCP connection. After reaching $2^{32} - 1$, this number will wrap around to 0.

Acknowledgement number :

A 32-bit number identifying the next data byte the sender expects from the receiver. Therefore, the number will be one greater than the most recently received data byte. This field is only used when the ACK control bit is turned on.

Scanned by CamScanner

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 :

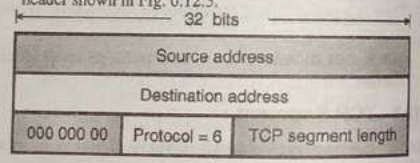
Although not used in some circumstances (e.g. acknowledgement segments with no data in the reverse direction), this variable length field carries the application data from TCP sender to receiver. This field coupled with the TCP header fields constitutes a TCP segment.

6.12.3 Checksum : MU : May 15

University Questions

Q. 1 Write short notes on : CRC and checksum. **(May 15, 5 Marks)**

- A checksum is provided to ensure extreme reliability. It checksums the header, the data and the conceptual pseudo header shown in Fig. 6.12.3.



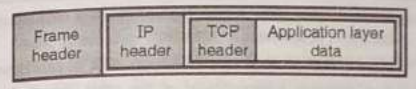
(G-612) **Fig. 6.12.3 : The pseudo header included in the TCP checksum**

- When the checksum is being computed, the TCP checksum field is set to zero, and the data field is padded out with an additional zero byte if its length is an odd number.
- Then all the 16 bit words are added in 1's complement and then 1's complement of the sum is taken to get the checksum.
- When a receiver performs the calculation on the entire segment including the checksum field, the result has to be zero.
- The pseudo header contains the 32 bit IP address of the source and destination machines, the protocol number for

TCP i.e. 6 and the TCP segment length as shown in Fig. 6.12.3.

6.12.4 Encapsulation :

- The data coming from the application layer is encapsulated in a TCP segment. This TCP segment is then encapsulated in an IP datagram.
- The IP datagram is encapsulated in a frame at the data link layer. The process of encapsulation is shown in Fig. 6.12.4.



(G-2072) **Fig. 6.12.4 : Encapsulation**

Ex. 6.12.1 : The following is a dump of TCP header in hexadecimal format

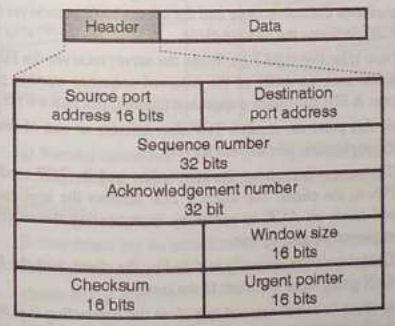
05320017 00000001 00000000 500207FF 00000000

1. What is the source port number ?
2. What is the sequence number ?
3. What is the acknowledgement number ?
4. What is the length of header ?
5. What is the window size ?

Dec. 12, 10 Marks

Soln. :

The TCP segment format and its header format are as shown in Fig. P. 6.12.1.



(G-1475) **Fig. P. 6.12.1 : TCP header**

The given TCP header consists of 5 words 32 bit each. We can identify them as follows :

1. 0532 0017 — Destination port address. (16 bit)
2. 0000 000 1 — Sequence number (32 bit)
3. 0000 0000 — Acknowledgement number (32 bit)
4. 5002 07FF — Window size (16 bit)

Therefore :

1. Sequence number = 0000 0001 = 1
2. Destination port number = $(0\ 0\ 1\ 7)_H$ = 23
3. Acknowledgement number = 0000 0000 = 0
4. Window size = 07FF = 2047 bytes

6.13 A TCP Connection :

- TCP is a connection oriented protocol. Such a protocol would establish a virtual path between the sender and the receiver.
- Multiple segments corresponding to the message are then sent over this virtual connection.
- As TCP is using the same single path for the entire path, it can use the same path for acknowledgements and retransmission of damaged or lost packets.
- While discussing the relation between TCP and IP we have seen how TCP uses the services of IP.
- TCP operates at a higher level than IP and the TCP connection is virtual and not physical.
- Though IP delivers the individual segments to the destination, the entire control on the connection is exercised by TCP.
- If a segment is lost or damaged, the TCP makes a decision of its retransmission, and IP does not know anything about it.
- The **three phases** in the connection oriented TCP transmission are as follows :
  1. Connection establishment
  2. Data transfer and
  3. Connection termination.

Scanned by CamScanner

6.13.1 TCP Connection Establishment :

MU : May 12, May 13, Dec. 14, Dec. 16

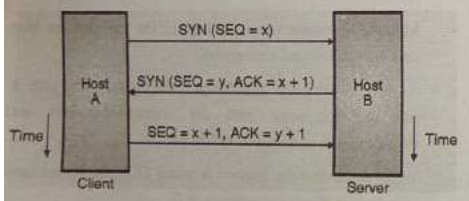
University Questions

Q. 1 Explain TCP connection establishment mechanism. **(May 12, 5 Marks)**

Q. 2 Explain TCP connection establishment and closing mechanism. **(May 13, 10 Marks)**

Q. 3 Explain connection establishment and termination in TCP with neat diagram. **(Dec. 14, Dec. 16, 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. 6.13.1(a).



(G-613) **Fig. 6.13.1(a) : TCP connection establishment (Three-way handshake)**

The requesting end (HOST A) sends a SYN segment specifying the port number of the server that the client wants to get connected to, and the client's initial sequence number (x).

The server (HOST B) responds with its own SYN segment containing the server's initial sequence number (y). The server also acknowledges the client's SYN by acknowledging the client's SYN plus one (x + 1). A SYN consumes one sequence number.

The client must acknowledge this SYN from the server by acknowledging the server's SYN plus one. (SEQ. = x + 1, ACK = y + 1).

This is how a TCP connection is established.

6.13.2 Connection Termination Protocol [Connection Release] :

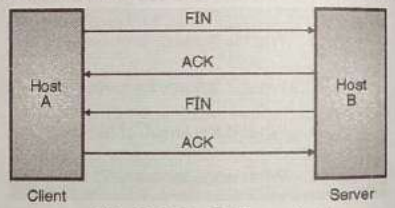
MU : May 13, Dec. 14, Dec. 16

University Questions

Q. 1 Explain connection establishment and termination in TCP with neat diagram. **(Dec. 14, Dec. 16, 10 Marks)**

Q. 2 Explain TCP connection establishment and closing mechanism. **(May 13, 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. 6.13.1(b). The rule is that either side can send a FIN when it has finished sending data (FIN indicates finished).
- When a TCP program on a host receives a FIN, it informs the application that the other end has terminated the data flow.



(G-614) **Fig. 6.13.1(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. 6.13.1(b). When the server receives the FIN it sends back an ACK of the received sequence number plus one. A FIN consumes a sequence number, just like a SYN.
- At this point the server's TCP also delivers an end-of-file to the application (the discard server).
- The server then closes its connection and its TCP sends a FIN to the client. The client's TCP informs the application and sends an ACK to server by incrementing the received sequence number by one.
- Connections are normally initiated by the client, with the first SYN going from the client to the server.
- A client or server can actively close the connection (i.e. send the first FIN). But in practice generally the client determines when the connection should be terminated, since client processes are often driven by an interactive user, who enters something like quit to terminate.
- This is how the TCP connection is released.

6.13.3 TCP Connection Management :

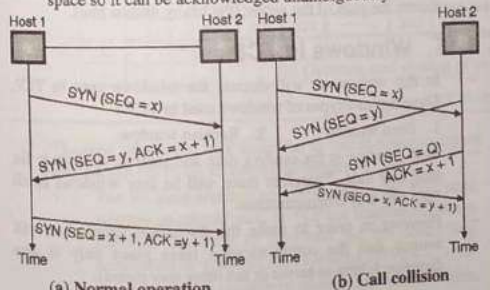
MU : May 09, Dec. 09, May 11

University Questions

Q. 1 Explain TCP connection management and TCP transmission policy. **(May 09, 6 Marks, Dec. 09, 10 Marks)**

Q. 2 Write short notes on : The TCP Connection Management. **(May 11, 5 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. 6.13.2(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. 6.13.2 : 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. 6.13.2(b).
- Under such circumstances only one connection is established. Both the connections can not be established simultaneously because connections are identified by their end points.
- If the first set up results in a connection which is identified by (x, y) and second connection is also set up, then only one table entry will be made i.e. for (x, y).
- For the initial sequence number a clock based scheme is used, with a clock pulse coming after every 4 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.

6.13.4 TCP Connection Release :

- A TCP connection is actually a full duplex connection but to understand the connection release we will assume that it is a pair of simplex connections.
- We can then think that each simplex connection is getting terminated independently.
- Releasing a TCP connection is identical on both ends. Each side can send a TCP segment with the FIN bit set, meaning it has no more data to send.
- After receiving a FIN, the Acknowledge (ACK) signal is sent and that direction is shut down, but data may continue to flow indefinitely in the other direction.
- If the sender of FIN does not receive the ACK within 2 maximum packet lifetimes, it releases the connection. The receiver will eventually notice that it receives no more data and time-out as well.
- Normally four TCP segments are required to release a connection i.e. one FIN and one ACK in each direction.
- However the first ACK and second FIN can be combined in the same segment.

Connection reset :

- The connection reset in TCP can take place when TCP at one end done any one of the following :
  1. It may deny a connection request.
  2. It may abort the existing connection.
  3. It may terminate an idle i.e. non operating connection.
- TCP does all the three with the help of the RST (reset flag).

6.14 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 6.14.1.

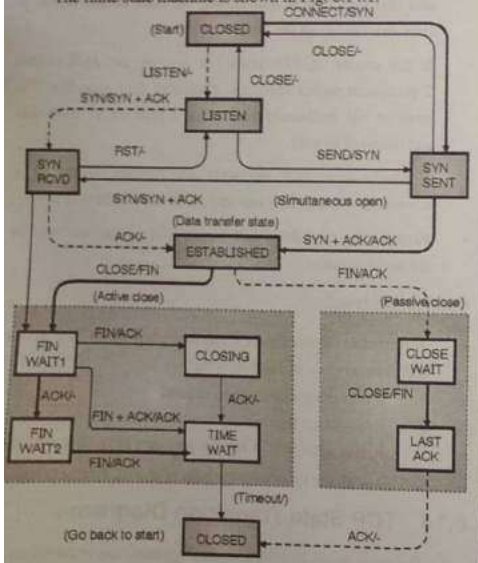
Table 6.14.1 : Different states in TCP finite state machine

State	Description
CLOSED	No connection is active or pending

Scanned by CamScanner

State	Description
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 6.14.1, 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. 6.14.1.



(G-696) **Fig. 6.14.1 : 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. 6.14.1. 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. 6.14.1 we have written the event / action pair.
- The event can either be a user-initiated system call (CONNECT, LISTEN, SEND or CLOSE), a segment arrival (SYN, FIN, ACK or RST), or a time-out.
- For the TIMED WAIT state the event can only be a time-out of twice the maximum packet length. The action is the sending of a control segment (SYN, FIN or RST) or nothing.
- The time-outs to guard for lost packets (e.g. in the SYN SENT state) are not shown here.
- There are 11 states used in the TCP connection management finite state machine. Data can be send in the ESTABLISHED and the CLOSE WAIT states and received in the ESTABLISHED and FIN WAIT1 states.

Explanation :

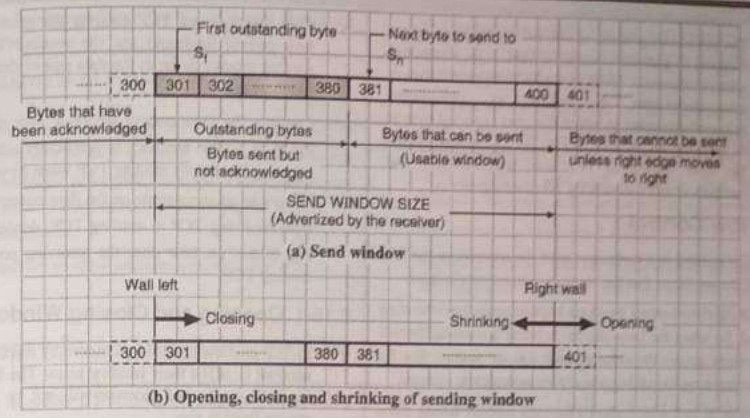
- To understand the finite state machine of Fig. 6.14.1, first follow the path of a client i.e. the heavy solid line. After that follow the path of the server (the heavy dashed line).

6.15 Windows in TCP :

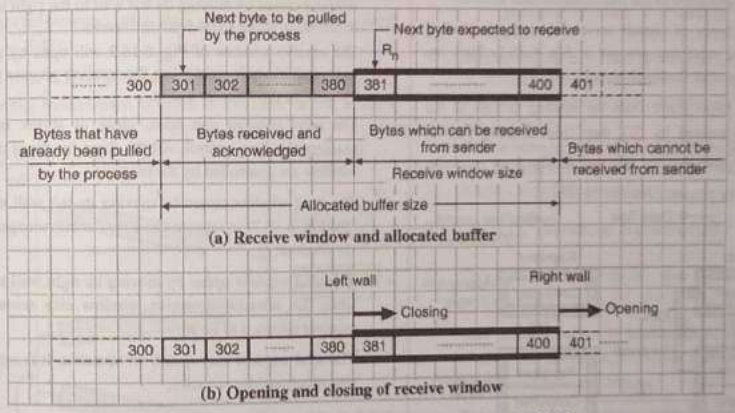
- In this section we will discuss the windows used in TCP. There are two types of windows used in TCP :
  1. Send window 2. Receive window
- Send window is for sending data and receive window is for receiving data. Therefore there will be four windows in all for a two way communication.
- However in 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).

6.15.1 Send Window :

- Fig. 6.15.1 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. 6.15.1.
- 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.



(G-1800) **Fig. 6.15.1 : Send window in TCP**



(G-1801) **Fig. 6.15.2 : Receive window in TCP**

- 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.

6.15.2 Receive Window :

- The example of receive window has been shown in Fig. 6.15.2. 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. 6.15.2.
- 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. 6.15.2). 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 :

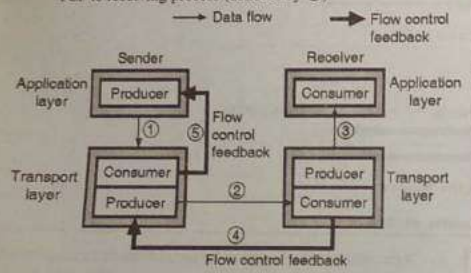
rwnd = Buffer size – Number of acknowledged bytes to be pulled

Scanned by CamScanner

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. 6.15.2) is announced. The new version of TCP uses both selective and cumulative mechanisms for acknowledgements.

6.16 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. 6.16.1 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. 6.16.1. 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. 6.16.1 : 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. 6.16.1. 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. 6.16.1. i.e. how does the receiving process control the sending TCP.

6.16.1 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. 6.16.3. 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. 6.16.3 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. 6.16.3) 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.

6.16.2 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)

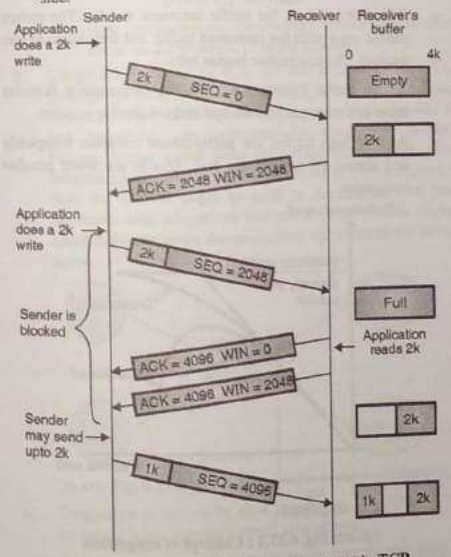
- The above relationship shows that the right wall should not move to the left.

6.16.3 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. 6.16.2.

Explanation :

- Let the receiver in Fig. 6.16.2, 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.

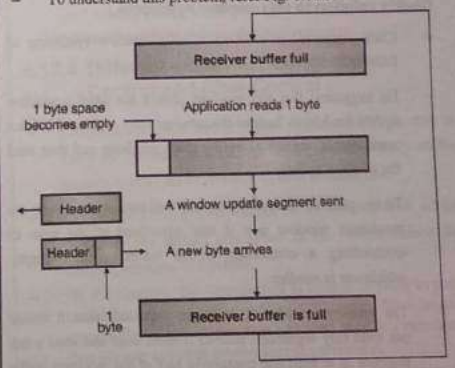


(G-616) **Fig. 6.16.2 : Windows management in TCP**

- Now the sender sends another 2k i.e. 2048 bytes segment (SEQ = 2048) which is acknowledged by the receiver (ACK = 4096, WIN = 0) which shows that window = 0 because the receiver buffer space is 0. ACK = 4096 indicates that the receiver has received 4096 bits successfully.
- The sender must now be blocked until the application process on the receiver removes some data from the buffer and some buffer space becomes available.
- As soon as the application on the receiver side reads 2k bytes, the buffer becomes partially empty and an acknowledgement with a window of 2k (ACK = 4096, WIN = 2048) is sent back to sender. Here WIN = 2048 indicates the empty buffer space on the receiver side.
- The sender may send upto 2 kbytes.
- When the window = 0, the sender should not normally send any segment. But under two exceptional conditions the sender will continue to send data even when it receives WIN = 0.
  1. First, urgent data may be send, e.g. to allow the user to kill the process running on the other machine.
  2. Second, the sender may send a 1-byte segment to make the receiver reannounce the next byte expected and the window size. This is used to prevent the possible confusion if a window announcement gets lost.
- Senders are not supposed to transmit data as soon as the data is obtained from an application. The receivers also are not supposed to send acknowledgements as soon as they receive it.
- This is done in order to reduce the usage of the system. One way to reduce the system usage is to use an algorithm called Nagle's algorithm is used.

6.16.4 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. 6.16.3.



(G-617) **Fig. 6.16.3 : Silly window syndrome**

Scanned by CamScanner

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.

6.16.5 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.

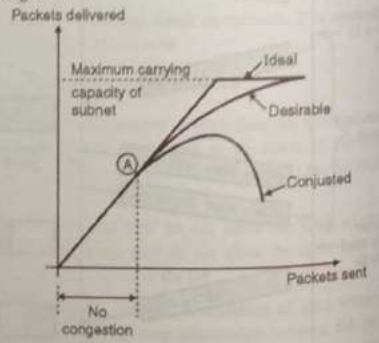
6.17 Congestion Control :

MU : May 10, Dec. 15

University Questions

Q. 1 What is congestion and what are the causes of congestion ? Explain Token bucket algorithm of congestion control. **(May 10, Dec. 15, 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. 6.17.1 explains the concept of congestion graphically.
- Upto point A in Fig. 6.17.1, the number of packets sent into the subnet by the host is within the capacity of the network. So all these packets are delivered. In short the number of packets delivered is proportional to number of packets sent and no congestion takes place.
- But after point A, the traffic increases too far. The routers cannot cope with the increased traffic and they begin to lose packets. The congestion begins here.
- As the traffic increases further, the performance degrades more and more packets are lost and congestion worsens.
- At very high traffic, the performance collapses completely and almost all packets are lost. This is the worst possible congestion.



(G-473) **Fig. 6.17.1 : Concept of congestion**

6.17.1 Need of Congestion Control :

- It is not possible to completely avoid the congestion but it is necessary to avoid it otherwise control it.
- Congestion will result in long queues, which results in buffer overflow and loss of packets.
- So congestion control is necessary to ensure that the user gets the negotiated QoS (Quality of Service).

6.17.2 Causes of Congestion :

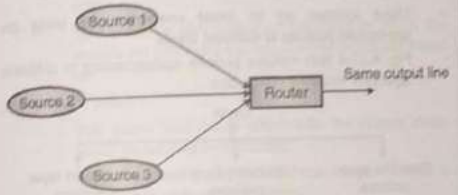
MU : May 10, Dec. 15

University Questions

Q. 1 What is congestion and what are the causes of congestion ? Explain Token bucket algorithm of congestion control. **(May 10, Dec. 15, 10 Marks)**

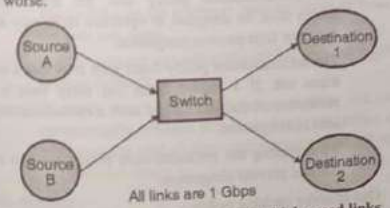
- Some of the causes of congestion are as follows :

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. 6.17.2(a). This leads to congestion.



(G-474) **Fig. 6.17.2(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. 6.17.2(b), if both the sources begin to send to destination 1 at their maximum rate, congestion will occur at the switch. Higher speed links can make the congestion condition in the switch worse.



(G-475) **Fig. 6.17.2(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.

6.17.3 Effects of Congestion :

Due to congestion, various network parameters get affected.

The most important network parameters which get affected by congestion are as follows :

1. Delay 2. Throughput

1. Delay versus load :

- When the load is very small as compared to the capacity of network, the delay is at its minimum. This minimum delay is equal to the sum of propagation delay and processing delay and it is negligible.
- But when load increases and becomes comparable to the network capacity the delay increases sharply due to the addition **waiting time** which gets added to the total delay.
- The delay becomes infinite when the load is greater than the capacity of network.
- The delay increases due to congestion.

2. Throughput versus load :

- Throughput can be defined as number of packets passing through a network per unit time. When the load is less than the capacity of network, the throughput increases proportional to the load.
- The throughput is expected to remain constant after it reaches its maximum (capacity of network). But practically the throughput reduces sharply as the load reaches its capacity.
- This happens because in the event of congestion, the routers discard some of the packets received by them.

Thus throughput reduces due to congestion.

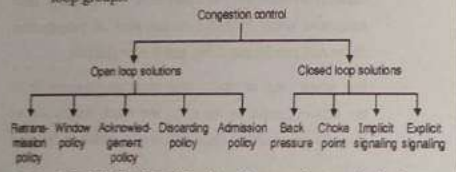
6.17.4 Difference between Congestion Control and Flow Control :

- 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.

Scanned by CamScanner

6.17.5 Principle of Congestion Control :

- 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. 6.17.3 shows the classification of congestion control schemes and various policies used in open loop and closed loop groups.



(G-476) **Fig. 6.17.3 : Classification of congestion control schemes**

Open loop control :

- Open loop solutions try to solve the congestion issue by excellent design to prevent the congestion from happening.
- Open loop control is exercised by using the tools such as deciding when to accept the new packets, when to discard the packets, which packets are to be discarded and making the scheduling decisions at various points.
- It is important to note that none of these decisions are made on the basis of the current status of a network, as no feedback is being used.

Closed loop control :

- The closed loop congestion control uses some kind of feedback. It takes into account the current status of the network.
- A closed loop control is based on the following three steps :
  1. Detect the congestion and locate it by monitoring the system.
  2. Transfer the information about congestion to places where action can be taken.
  3. Adjust the system operations to correct the congestion.
- Two examples of closed loop control are :
  1. TCP flow control.
  2. BR rate control for an ATM network.

Open loop versus closed loop :

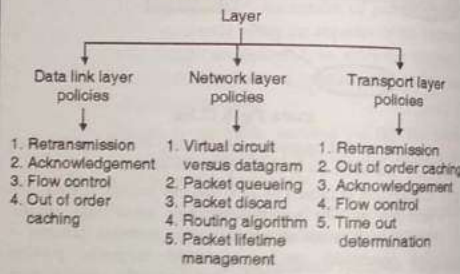
Open loop approaches do not need end-to-end feedback, one of the examples of this type are prior-reservation and hop-to-hop flow control.

In closed-loop approaches, the source can adjust its cell rate on the basis of the feedback information received from the network.

- Some people feel that closed loop congestion control schemes are too slow in todays high-speed, large range network. Because it takes a long time for feedback to go back to source. Hence before any corrective action takes place thousands of packets have been already lost.
- But on other hand, if the congestion has already taken place and the overload is of long duration, the congestion cannot be released unless the source causing the congestion is asked to reduce its rate.
- Furthermore, ABR service is designed to use any bandwidth that is left over the source must have some knowledge of what is available when it is sending cells.

6.17.6 Congestion Prevention Policies :

- 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. 6.17.4 lists various policies corresponding to different layers for avoiding congestion.



(G-477) **Fig. 6.17.4 : Policies affecting the congestion**

Policies related to data link layer :

1. **Retransmission policy :**
   - The retransmission policy and the retransmission timers must be designed to optimise efficiency and at the same time prevent congestion.
   - The retransmission policy deals with how fast a sender times out. If a sender times out early then it will retransmit all the packets and such a retransmission can lead to congestion.
   - By designing the retransmission policy we can avoid this and prevent congestion.
2. **Out of order caching policy :**

   If the receivers routinely discard all the packets which are out of order, then retransmission of these packets will take place. This will increase the load and result in congestion. So a selective repeat (retransmission) should be adopted to avoid congestion.
3. **Acknowledgement policy :**
   - If each received packet is promptly acknowledged then the acknowledgement packets will increase the traffic.
   - If the acknowledgement is delayed (piggybacking) then there is a possibility of time out and retransmission.

   - So a tight flow control has to be exercised to avoid congestion.
4. **Window policy :**

   The type of window at the sender may also affect congestion. The selective repeat window is better than the Go Back N window.

Policies related to network layer :

1. **Choice between virtual circuit and datagrams :**

   This choice at the network layer will affect the congestion because many congestion control algorithms work only with virtual circuit subnets.
2. **Packet queuing and service :**
   - This policy is related to whether the routers have one queue per input line and one queue per output line or both.
   - This policy is also related to the order in which the packets are processed e.g. round robin or priority based etc.
3. **Discard policy :**
   - This policy lays a rule which tells the routers about which packet is to be discarded.
   - A good discard policy can prevent congestion and a bad one will worsen the situation.
4. **Routing algorithms :**

   The routing algorithms can spread the traffic over all the lines. By doing so it is ensured that none of the lines are overloaded. This will certainly avoid congestion.
5. **Package lifetime management :**
   - This policy decides the maximum time for which a packet may live before being discarded.
   - This time should be of adequate value so that congestion can be avoided.

Policies related to transport layer :

- The policies at the transport layer are same as those at the data link layer.
- But at transport layer determining the time out interval is more difficult.
- If it is too short then extra packets are sent unnecessarily whereas if it is too long, congestion will reduce at the cost of increased response time (network will become slow).

Traffic shaping :

- One of the important reason behind congestion is the bursty nature of the traffic. If the traffic has a uniform data rate then congestion would not happen every now and then. But due to bursty traffic it can happen regularly.
- Traffic shaping is an open loop control. It prevents the congestion by making the packet transmission rate to be more predictable (bursty traffic is unpredictable).
- Thus traffic shaping will regulate the average rate or the burstiness of data transmission.
- Monitoring a traffic flow is called as **traffic policing.**
- Check if a packet stream (connection) is as per its descriptor, and if it is not as per its descriptor, then give penalty !
- In order to achieve this the network may want to monitor the traffic flow during the connection period. The process of monitoring and enforcing the traffic flow is called traffic policing.
- The types of penalties enforced are as follows :
  1. Drop packets that violate the descriptor.
  2. Give low priority to the packets violating the descriptor.

6.17.7 Congestion Control in Virtual Circuit Subnets :

- All the congestion control techniques discussed till now were open loop techniques.
- Now let us discuss a dynamic technique called **admission control.**

Admission control principle :

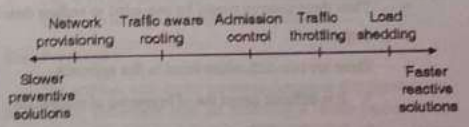
- This technique is used to keep the congestion which has already begun to a managable level and does not allow it to worsen any further.
- Its principle is as follows : Once congestion has been detected, do not set up any more virtual circuits until the congestion is cleared.
- The advantage of this 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.

6.17.8 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. 6.17.5 : Time scales of approaches to congestion control**

Scanned by CamScanner

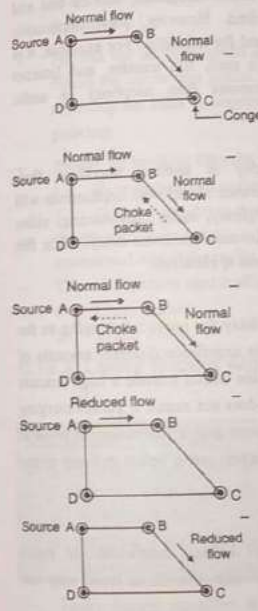
1. **Network provisioning :**
   - The fundamental way of avoiding congestion is to build a network that is properly matched to the traffic that it is going to carry.
   - If the network uses a low bandwidth link along which a heavy traffic is directed, then congestion is most certain to take place.
   - 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 tomonitor 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.

6.18 Congestion Control in Datagram Subnets :

- Let us now discuss some congestion control approaches which can be used in the datagram subnets (and also in virtual circuit subnets).
- The techniques are :
  1. Choke packets 2. Load shedding 3. Jitter control.

6.18.1 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.).

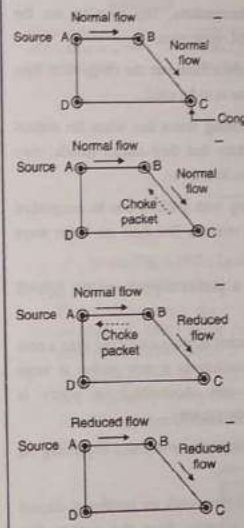


- Congestion is identified at C.
- Choke packet is sent back from C to B. But the flow from A to B and B to C is normal.
- Choke packet is sent back from B to A. But flow from A to B and B to C is still normal.
- Now the flow from A to B is reduced.
- The flow from B to C also is reduced.

(G-478) **Fig. 6.18.1(a) : Choke packet mechanism**

- If the value of "u" goes above the threshold then that output line will enter into a "warning" state. The router will check each newly arriving packet to see if its output line is in the "warning state".
- If it is in the warning state then the router will send back a **choke packet** signal to the sending host.
- The sender host will not generate any more data packets. This will reduce the congestion.
- Different congestion control algorithm have been proposed, depending on the value of thresholds.
- Depending on the threshold value, the choke packets can contain a mild warning, a stern warning or an ultimatum.
- Another algorithm may use the queue lengths or buffer utilization instead of using the line utilization as a deciding factor.
- The general concept of choke packet mechanism is demonstrated in Fig. 6.18.1(a).
- Fig. 6.18.1(a) shows that, the choke packets have to travel over the entire network, from the point of congestion to the appropriate source (i.e. from C to A).
- Then the action of reducing the flow will take place. The whole process is therefore very much time consuming.

Hop-by-Hop choke packet technique :



- Congestion is identified at point C.
- Choke packet is sent back to node B. But the flow from A to B and B to C is still normal.
- Now the flow at node B is reduced. The choke packet is sent back to source A.
- Now the flow from A is also reduced. The flow from A to B and B to C is reduced.

(G-479) **Fig. 6.18.1(b) : Concept of hop-by-hop choke packet mechanism**

- The problem associated with the general choke packet mechanism can be overcome by using another technique called as hop-by-hop choke packet technique.
- This is demonstrated in Fig. 6.18.1(b). In this approach, the choke packets are used at each hop between the destination and source.
- Each node receiving the choke packet will reduce its output flow. This will have a more effective and fast control over the overall transmission rate.
- Fig. 6.18.1(b) shows how the transmission rate is reduced at every hop in response to the choke packets.

Disadvantage :

The problem with choke packet technique is that the action to be taken by the source host on receiving a choke packet is not compulsory. The host may reduce its transmission rate or ignore the choke packets.

Scanned by CamScanner

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.

6.18.2 Load Shedding :

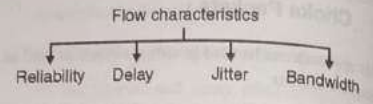
- Admission control, choke packets, fair queuing are the techniques suitable for light congestion.
- But if these techniques cannot eliminate the congestion, then the load shedding technique is to be used.
- The principle of load shedding states that when the routers are flooded with the packets that 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.

6.19 Quality of Service (QoS) :

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. 6.19.1.



(G-480) **Fig. 6.19.1 : Flow characteristics**

1. Reliability :

A data flow must have some level of reliability. Lack of reliability means a packet or acknowledgment, will be lost and retransmission will be required. However, each application programs has a different demand for reliability. For example, it is more important that electronic mail, file transfer, and Internet access have reliable transmissions than telephony or audio conferencing.

2. Delay :

Source-to-destination delay is another important flow characteristic. Again delay tolerance of different applications will be different. In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay, while file transfer or email are delay tolerant applications.

3. Jitter :

Jitter is the variation in delay for packets belonging to the same flow. i.e. different packets experience different amounts of delays. Real-time audio and video cannot tolerate a large amount of jitter. On the other hand, it does not matter if packet carrying information in a file have different delays. The transport layer at the destination waits until all packets arrive before delivery to the application layer.

4. Bandwidth :

Different applications need different bandwidths. In video conferencing needs a huge bandwidth whereas an email may not need a large bandwidth.

6.19.1 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

6.19.2 Traffic Shaping : MU : Dec. 09

University Questions

Q. 1 What is traffic shaping ? Explain Leaky Bucket algorithm for traffic shaping. **(Dec. 09, 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.

6.19.3 Leaky Bucket Algorithm :

MU : Dec. 06, Dec. 09

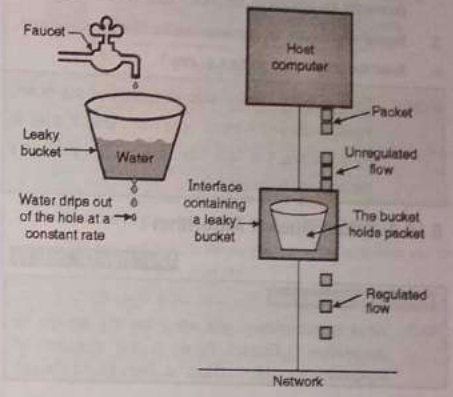
University Questions

Q. 1 Explain Leaky Bucket algorithm in detail. Also explain advantages of same compared with token bucket algorithm. **(Dec. 06, 10 Marks)**

Q. 2 What is traffic shaping ? Explain Leaky Bucket algorithm for traffic shaping. **(Dec. 09, 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.
- The principle of leaky bucket algorithm is as follows :

  Leaky bucket is a bucket with a hole at bottom. Flow of the water from bucket is at a constant rate (data rate is constant) which is independent of water entering the bucket (incoming data). If bucket is full, any additional water entering in the bucket is thrown out (Packets are discarded).
- Same technique is applied to control congestion in network traffic. Every host in the network is having a buffer (equivalent to a bucket) with finite queue length.
- Packets which are put in the buffer when buffer is full are thrown away. The buffer may send some number of packets per unit time onto the subnet (helpful if packets vary greatly in size) as shown in Fig. 6.19.2 the data flow at the input of the bucket is unregulated but that at the bucket output is a regulated one.

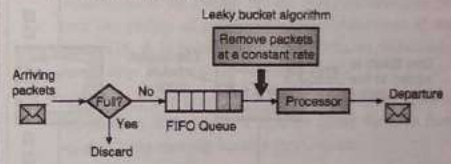


(a) (b)

(G-481) **Fig. 6.19.2 : Leaky bucket algorithm**

Leaky bucket implementation :

- Fig. 6.19.3 shows the implementation of leaky bucket principle. A FIFO (First In First Out) queue is used for holding the packets which is equivalent to the leaky bucket.
- The implementation of Fig. 6.19.3 can be discussed under two different operating conditions, namely :
  1. For packets of fixed size.
  2. For packets of variable size.



(G-482) **Fig. 6.19.3 : Implementation of leaky bucket**

1. Fixed size packets :

If the arriving packets are of fixed size (e.g. cells in ATM networks), then the process of Fig. 6.19.3 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.

Scanned by CamScanner

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.

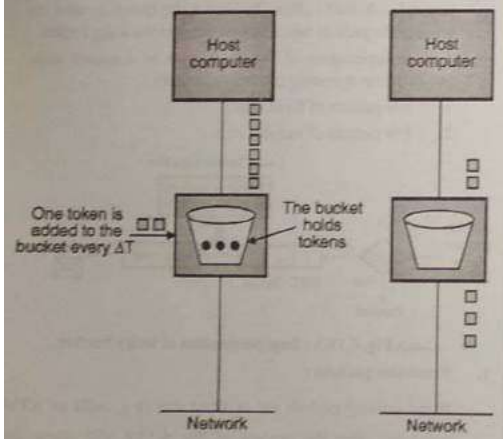
6.19.4 Token Bucket Algorithm :

MU : May 10, Dec. 15

University Questions

Q. 1 What is congestion and what are the causes of congestion ? Explain Token bucket algorithm of congestion control. **(May 10, Dec. 15, 10 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.



(a) Before (b) After

(G-483) **Fig. 6.19.4 : Token bucket algorithm**

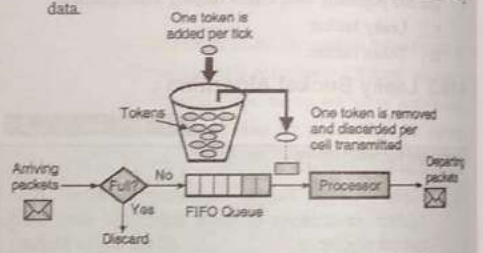
It enforces a long-term average transmission rate while permitting bounded bursts. In this approach, a token bucket is used to which manages the queue regulator that ultimately controls the rate of packet flow into the network.

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. 6.19.4. If the token bucket gets full then the extra tokens are discarded.

- Token bucket algorithm is a variant of leaky bucket algorithm discussed earlier. Here the bucket is filled with tokens.
- A packet which grabs and 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. 6.19.5 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. 6.19.5 : 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,

$$s = \frac{c}{m - \rho}$$

6.19.5 Combination of Token Bucket and Leaky Bucket :

- The token bucket and leaky bucket techniques can be combined to obtain the following advantages :
  1. To credit an idle host 2. To regulate the traffic
- The token bucket is used first followed by the leaky bucket technique. The rate of leaky bucket needs to be higher than the rate of tokens dropped in the bucket.

6.19.6 Resource Reservation :

- The data flow is dependent on the following resources :
  1. Buffer 2. Bandwidth 3. CPU time
- The QoS can be improved by reserving these resources. The QoS model called integrated services operates on the principle of resource reservation, for improvement in QoS.

6.19.7 Admission Control :

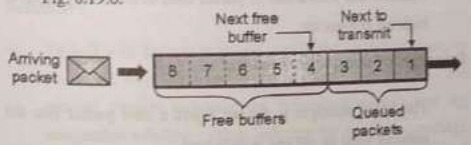
- Admission control technique is used by a router or a switch. They use this mechanism to accept or reject the data flow based on predefined parameters called flow specifications.
- Before accepting a flow for processing, a router checks the flow specifications and finds out if it is possible to take up and handle this new data flow.
- It does this by comparing its bandwidth, buffer size, CPU speed etc. with the flow specifications.

6.19.8 Queuing Disciplines :

- Each router must implement some queuing discipline which decides about how the packets are buffered when they are waiting to get transmitted.
- There are two algorithms commonly used in packet switching networks namely :
  1. First In First Out (FIFO) 2. Fair Queuing (FQ)

6.19.9 FIFO Queuing :

- The FIFO queuing is also called as First Come First Served (FCFS) Queuing. Its idea is simple and illustrated in Fig. 6.19.6.

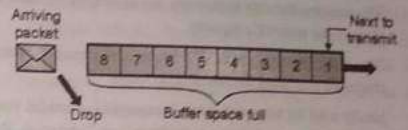


(G-485) **Fig. 6.19.6 : FIFO queuing**

- 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. 6.19.6 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. 6.19.7.

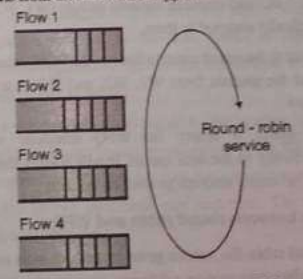


(G-486) **Fig. 6.19.7 : Dropping of a packet**

- 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.

6.19.10 Fair Queuing :

- The disadvantage of FIFO queuing is that there is absolutely no discrimination among the packets being received from different sources. All are treated equally.
- Because the entire congestion control mechanism is implemented at the sources and the FIFO queuing does not have any facility of policing the source behaviour to this mechanism, it is possible that a bad behaved source may occupy large fraction of the network capacity.
- Fair Queuing (FQ) is an algorithm which is proposed to solve this problem. It maintains a separate queue for each flow which is being currently handled by the router.
- The router then entertains these queues in the round robin manner as shown in Fig. 6.19.8.
- 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. 6.19.8 : Concept of fair Queuing (FQ) at the router**

Scanned by CamScanner

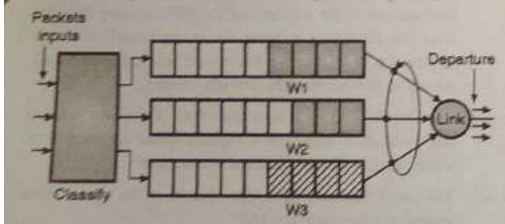
- This ensures that any source can not arbitrarily increase its share of the network's capacity.
- The main problem with FQ is that the packets being processed at a router are not of same length.
- Ideally a bit by bit round robin is expected i.e. one bit from flow-1 is transmitted, then one bit from 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.

6.19.11 Weighted Fair Queuing :

- The disadvantage of choke packet technique can be overcome with the help of the Weighted Fair Queuing (WFQ) technique.
- This queuing algorithm was proposed first in 1987. In this algorithm it is proposed that the routers have a number of queues for each output line, with one queue for each source.
- Refer Fig. 6.19.9 to understand weighted fair queuing.



(G-488) **Fig. 6.19.9 : 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.

6.20 TCP Congestion Control :

MU : May 07, Dec. 10, May 14, Dec. 14, May 15, May 16

University Questions

Q. 1 Explain how TCP controls congestion. **(May 07, Dec. 10, 10 Marks)**

Q. 2 Explain TCP congestion control. **(May 14, Dec. 14, May 16, 10 Marks)**

Q. 3 How congestion is controlled in TCP ? **(May 15, 5 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 :

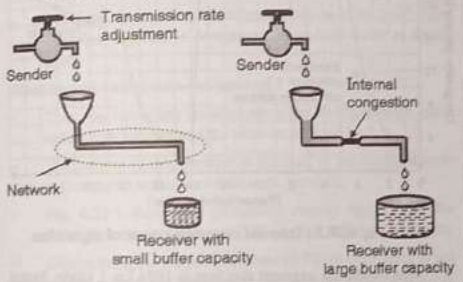
Step 1 : Detect the congestion :

- 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. 6.20.1(a), the congestion due to buffer overflow will never take place.
- Now consider Fig. 6.20.1(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. 6.20.1 : Congestion**

Conclusion :

- To prevent congestion TCP has to deal with two problems separately – receiver capacity and network capacity.

Solution :

- To deal with the two problems mentioned earlier each sender maintains two windows : the window the receiver has granted (which indicates the receiver capacity) and the **congestion window** (which indicates the network capacity). The first window that indicates the receiver capacity is called as the **flow control window.**
- The size of the congestion window is equal to the number of bytes the sender may have in the network at any time. Hence the corresponding **sending rate** is equal to the ratio of **congestion window size** and the **RTT** of the connection.
- TCP adjusts the size of window as per the AIMD rule.
- The **congestion window** is maintained in addition to the **flow control window** (Which specifies the number of bytes that the receiver can buffer).
- Both these windows are considered simultaneously. Both the windows indicate the number of bytes the sender may transmit and the number can be different. Therefore the number of bytes that may be sent by the sender is the minimum of the two windows.
- So the effective window is the minimum of what the sender and the receiver both think is all right.

Modern congestion control :

- Modern congestion control was added to TCP in 1988 through the efforts of Van Jacobson. In 1986 due to growing number of Internet users the first **congestion collapse** took place. As a response to this collapse Jacobson approximated an 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.

6.20.1 Slow Start Algorithm :

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.

Scanned by CamScanner

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. 6.20.2. 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.

6.20.2 Internet Congestion Control Algorithm :

- 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. 6.20.2.

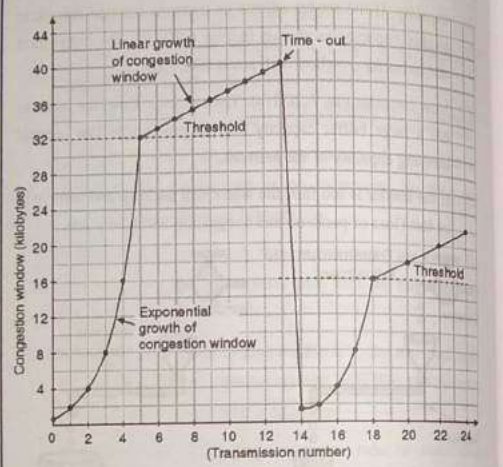
Table 6.20.1 is used to plot the graph of Fig. 6.20.2. See how the threshold point acts as the boundary of the exponential growth and linear growth of the congestion window.

(G-619(a)) **Table 6.20.1**

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. 6.20.2 : 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. 6.20.2)
- 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.

6.20.3 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. 6.20.3.

6.21 TCP Timer Management : MU : Dec. 14

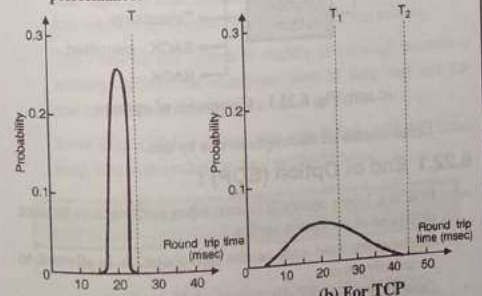
University Questions

Q. 1 Explain TCP timer management and transaction TCP. **(Dec. 14, 10 Marks)**

- 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. 6.21.1 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. 6.21.1(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. 6.21.1 Probability density of acknowledgement arrival times**

6.21.1 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,

$$SRTT = \alpha\, SRTT + (1 - \alpha)\, R \quad \text{...(6.21.1)}$$

- 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,

$$RTTVAR = \beta\,(RTTVAR) + (1 - \beta)\,|SRTT - R| \quad \text{...(6.21.2)}$$

- The typical value of $\beta = 3/4$. The retransmission timeout RTO is set by the following expression,

$$RTO = SRTT + (4 \times RTTVAR) \quad \text{...(6.21.3)}$$

- 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.

6.21.2 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.

Scanned by CamScanner

21.3 Other Timers in TCP :

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.

Keepalive timer :

- This is the third timer in TCP. It is used when a connection is idle for a long time.
- When a connection is idle for a very long time, the Keepalive timer may go off. This will cause one side to check if the other side is still there.
- If the other side does not respond, then the connection is terminated.

Timer for TIMED WAIT state :

This timer is used in the TIMED WAIT state while closing. his timer is set to a time equal to twice the maximum packet etime to ensure that after closing a connection all the packets eated by it die off.

Ex. 6.21.1 : 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.

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 :**

$$D = |RTT - M| = |30 - 24| = 6 \text{ msec}$$

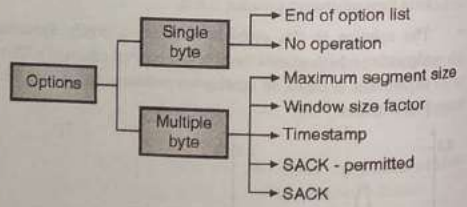
$$\therefore \text{Time out} = 30 + (4 \times 6) = 54 \text{ msec}$$

6.22 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. 6.22.1.

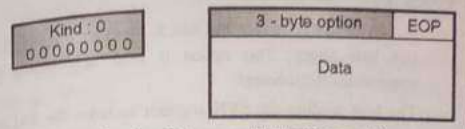


(G-2037) **Fig. 6.22.1 : Categories of options**

- Let us discuss all these options one by one.

6.22.1 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. 6.22.2.



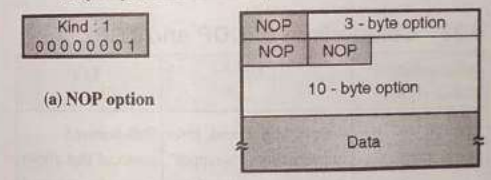
(a) End of option list **(b) Used for padding**

(G-2038) **Fig. 6.22.2 : 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.

6.22.2 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. 6.22.3. The NOP is used for aligning one 3-byte option (like window scale factor) and one 10-byte option like timestamp.



(a) NOP option

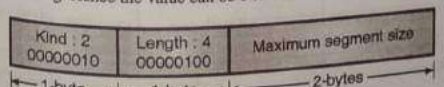
(b) Used to align beginning of an option

(G-2039) **Fig 6.22.3 : No operation option**

- From Fig. 6.22.3(b) it is evident that we can use the NOP option more than once.

6.22.3 Maximum Segment Size (MSS) :

- Fig. 6.22.4 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.
- 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. 6.22.4 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. 6.22.4 : Maximum segment size option**

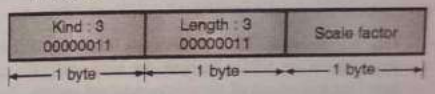
- During the TCP connection establishment, the MSS is defined by each party, for the segment it is going to receive during the connection.
- If a party does not define MSS, then its default value of 536 is used.
- The value of MSS which is fixed during the connection established cannot be changed during the connection.

6.22.4 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. 6.22.5.



(G-2041) **Fig. 6.22.5 : 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. 6.22.5, 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.

Scanned by CamScanner

6.22.5 Timestamp :

- Fig. 6.22.6 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.

Kind : 8	Length : 10
00001000	00001010
Timestamp value	
Timestamp echo reply	

(G-2042) **Fig. 6.22.6 : Format of timestamp option**

6.22.6 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. 6.22.7.

Kind : 4	Length : 2

SACK - permitted option

Kind : 5	Length
Left edge of 1st block	
Right edge of 1st block	
⋮	
Left edge of nth block	
Right edge of nth block	

SACK - option

(G-2043) **Fig. 6.22.7 : Formats of SACK-permitted and SACK options**

SACK - permitted option :

- As shown in Fig. 6.22.7, 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.

6.23 Comparison of UDP and TCP :

Characteristic / Description	UDP	TCP
General Description	Simple, high-speed, low-functionality "wrapper" that interfaces applications to the network layer and does little else.	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
Protocol Connection Setup	Connectionless; data is sent without setup.	Connection-oriented; connection must be established prior to transmission.
Data Interface To Application	Message-based; data is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure.
Reliability and Acknowledgments	Unreliable, best-effort delivery without acknowledgments	Reliable delivery of messages; all data is acknowledged.
Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.

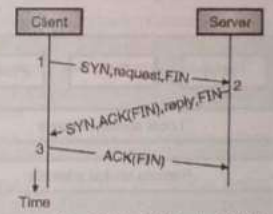
Characteristic / Description	UDP	TCP
Features Provided to Manage Flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms.
Overhead	Very low	Low, but higher than UDP
Transmission Speed	Very high	High, but not as high as UDP
Data Quantity Suitability	Small to moderate amounts of data (up to a few hundred bytes)	Small to very large amounts of data (up to gigabytes)
Types of Applications That Use The Protocol	Applications where data delivery speed matters more than completeness, where small amounts of data are sent; or where multicast/broadcast are used.	Most protocols and applications sending data that must be received reliably, including most file and message transfer protocols.
Well-Known Applications and Protocols	Multimedia applications, DNS, BOOTP, DHCP, TFTP, SNMP, RIP, NFS (early versions).	FTP, Telnet, SMTP, DNS, HTTP, POP, NNTP, IMAP, BGP, IRC, NFS (later versions).
Error control	Only checksum.	Provided.

6.24 Transitional TCP : MU : Dec. 14

University Questions

Q. 1 Explain TCP timer management and transaction TCP. **(Dec. 14, 10 Marks)**

- One of the ways to implement a client server system is to use the remote procedure call (RPC). We could also use UDP if both the request and reply are small enough to fit into single packets.
- But if these conditions are not satisfied, then UDP is no more an attractive option. The use of conventional TCP also does not prove to be a practical option due to its low efficiency.
- The disadvantage of using RPC is that even under the best working conditions we need nine packets. This number will increase in the worse cases.
- In order to overcome these problems, an experimental TCP variant was developed known as **transactional TCP or T/TCP**.
- T/TCP has the following advantages :
  1. It is very efficient.
  2. It uses only two messages.
- T/TCP is described in RFCs 1379 and 1644. The T/TCP protocol has been illustrated in Fig. 6.24.1.



(G-1417(a)) **Fig. 6.24.1 : RCP using T/TCP**

- The first packet from the client consists of the **SYN** bit, the **request** and **FIN** (finished). This means that the client says I want to establish a connection, here is the data and I have finished.
- On receiving the request, the server prepares the reply, and chooses how to respond to the clients request. If the reply fits in one packet then its reply is as shown in Fig. 6.24.1 which says, "I acknowledge your FIN, this is my reply and I have finished.".
- The client then acknowledges server's FIN and terminates the conversation. If the reply is longer than 1 packet then the server can send more than one packet before sending the FIN bit.
- T/TCP has a major disadvantage. It has major security problems due to which it has not gained a widespread popularity.

6.25 Sockets and their Programming :

MU : Dec. 03, Dec. 06, Dec. 07, May 08, Dec. 11, May 12, May 13

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 following terms : Socket. **(Dec. 06, 2 Marks)**

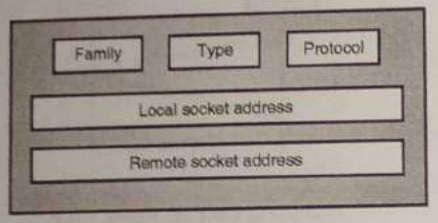
Q. 3 Explain the following with examples. : Socket. **(Dec. 07, 2 Marks, May 08, May 13, 10 Marks, Dec. 11, May 12, 4 Marks)**

Scanned by CamScanner

- 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. 6.25.1 shows a simplified socket structure.



(G-601) **Fig. 6.25.1 : 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.

6.25.1 Socket Types :

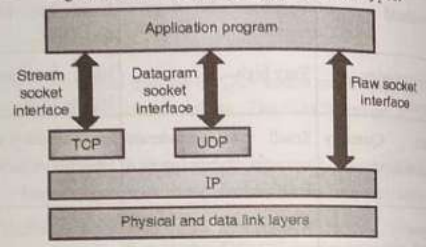
- There are three types of sockets.
  1. The stream socket
  2. The packet socket
  3. The raw socket

All these sockets can be used in TCP/IP environment. Let us discuss them one by one.

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. 6.25.2 shows the three types of socket types.



(G-602) **Fig. 6.25.2 : Type of sockets**

6.25.2 Berkeley Sockets : MU : Dec. 15, May 17

University Questions

Q. 1 Explain : Berkeley sockets. **(Dec. 15, 5 Marks)**

Q. 2 Write short note Berkeley socket. **(May 17, 5 Marks)**

- Table 6.25.1 lists various transport primitives used in Berkeley UNIX for TCP.

Table 6.25.1

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 6.25.1 are executed in the same order by the server.
- The SOCKET primitive creates a new end point and allocates table space for it within the transport entity.
- The newly created sockets do not have addresses. These are assigned using the BIND primitive.
- The LISTEN primitive allocates space to queue the incoming calls in case if several clients wish to connect at the same time.

- To block waiting for an incoming connection, the server executes an ACCEPT primitive. When a TPDU requesting for a connection arrives, the transport entity creates a new socket and returns a file descriptor for it.
- These were the primitives corresponding to server side. Now let us consider the client side.
- On the client side also a socket needs to be created first using the SOCKET primitive, however the BIND is not required.
- The CONNECT primitive blocks the caller and initiates the connection process.
- When it completes (which is indicated by an appropriate TPDU received from the server), the client process is unblocked and the connection is established.
- After this both the sides can use SEND and RECEIVE primitives to send and receive data.
- In order to release the connection, both sides have to execute a CLOSE primitive.

6.25.3 Steps Followed for Socket Programming :

- The steps followed for the socket programming are as follows :

Server side :

1. Server creates a socket and checks for errors using SOCKET.
2. Assign address to the newly created socket using BIND.
3. Use the LISTEN to allocate space for the queue which is used for the incoming calls.
4. Execute an ACCEPT for blocking the waiting incoming connections.

Client side :

1. Create a socket using SOCKET.
2. Use CONNECT to initiate connection process.
3. Establish the connection.

6.25.4 Connectionless Iterative Server (Datagram Socket) :

- 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.

6.25.5 Connection Oriented Concurrent Server (Stream Socket) :

- 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.

Scanned by CamScanner

4. **Repeat :** The server repeats the steps given below infinitely.
   (a) **Create a child :** When a child requests a connection, the operating system creates a temporary child process and assigns the duty of serving the client to the child. The parent process is then free for listening to new clients.
   (b) **Create a new socket :** A new socket is created which is to be used by the child process.
   (c) **Repeating :** The child repeats the following steps as long as it has requests from the client.
   1. Read 2. Process
   3. Write 4. Destroy socket.

Client functions :

The client performs the following functions :

1. Create a socket
2. Connect
3. Repeat the write and read operations
4. Destroy : Close the connection.

Client and server program :

Client-server programs are written in the languages such as C, C + +, Java. It requires advanced knowledge of the particular language.

6.26 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.

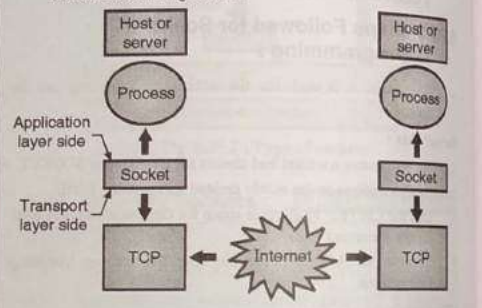
So when developing a proprietary application, the developer should not use one of the well known port numbers defined in the RFCs.

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 :

- The processes running on different machines communicate with each other by sending messages into sockets. This is demonstrated in Fig. 6.26.1.

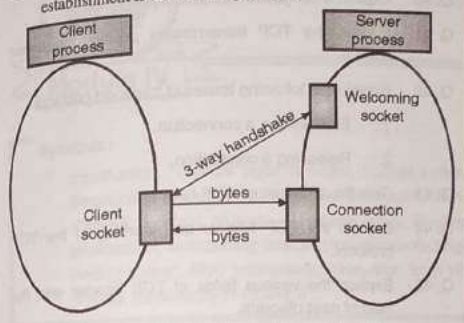


- Processes are controlled by application developers
- TCP is controlled by the operating system
- UDP can be used in place to TCP

(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.

- 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.



(G-1247) **Fig. 6.26.2 : Different types of sockets**

- During the three way handshake the client process knocks on the welcoming socket of the server process.
- The server process responds to this knocking by creating a new socket called **connection socket** which is dedicated to that particular client.
- In the last phase of the three way handshake a TCP connection is established between the client socket and the connection socket as shown in Fig. 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 :

- 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.

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 ?

Scanned by CamScanner

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 :

Q. 1 Describe a scenario in which a TCP connection request is received by a TCP end point, but there is infact no corresponding TCP end point who wishes to establish communication with receiver.

Ans. : This situation is similar to receiving the duplicate of an old request which is not existing at present. The TCP reacts to this situation as explained in **section 6.13.1.**

Q. 2 What is interprocess communication ? Explain its role in network based communication system.

(May 2009, 7 Marks)

Ans. : The transport layer is meant for process to process (interprocess) communication. **Refer section 6.3.1.**

□□□

CHAPTER 7

Module IV

Network Layer

Syllabus :

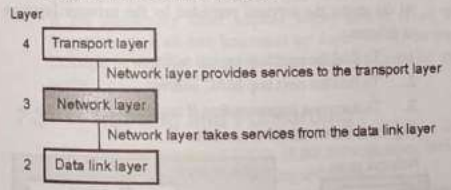
Introduction, Network layer services, Packet switching, Network layer performance, Network layer congestion, Structure of a router, Network layer protocols : IPv4 datagram format, IPv4 addresses, Forwarding of IP packets ICMPv4, Unicast routing : General idea, Routing algorithms, Unicast routing protocols, Multicast routing : Introduction, Multicasting basics, Intradomain routing protocols, Interdomain routing protocols, Next generation IP, Packet format, IPv6 addressing, Transition from IPv4 to IPv6, ICMPv6, Mobile IP; Addressing, Agents, Three phases, Inefficiency in mobile IP.

7.1 Network Layer :

- The network layer is responsible for carrying the packet from the source all the way to destination. In short it is responsible for host-to-host delivery.
- The network layer has a higher responsibility than the data link layer, because the data link layer is only supposed to move the frames from one end of the wire to the other end.
- Thus network layer is the lowest layer that deals with the end-to-end transmission.

Position of network layer :

- Fig. 7.1.1 shows the position of network layer in the 5 layer internet model. It is the third layer.



(G-433) **Fig. 7.1.1 : Position of network layer**

- It receives services from the data link layer and provides services to the transport layer.
- The network layer was designed to solve the problem of delivery through several links. The network layer is also called as the **Internetwork** layer.
- In addition to the host-to-host delivery the network layer is also responsible for **routing** the packets through the router.
- As a pure concept we can imagine that the Internet is a black box which connects a very large number of computers in the entire world together.
- But the Internet also is not a single network. It is infact the network of many networks or links.
- That means the Internet is an **internetwork** which is actually a combination of LANs and WANs.
- All these LANs and WANs are connected to each other via a connecting device such as a **router** which acts as a switch.

Routers :

Routers have many ports or interfaces. When it receives a packet at one of its ports, it forwards the packet through another port to the next switch or the final destination.

7.2 Network Layer Services :

- The duty of the network layer in TCP/IP is to provide the host-to-host delivery of datagrams.
- In this section we are going to discuss the services that are expected from the network layer.
- At the sending end, the network layer will accept a packet from its transport layer, encapsulate the packet into datagram and will deliver the packet to the data link layer.
- At the destination, exactly opposite process takes place. That means, at the destination the received datagram is decapsulated to extract the packet from it and the packet is delivered to the transport layer.

7.2.1 Logical Addressing :

- The two computers in communication with each other should have some universal identification system which is called as the **network layer address or logical address.** Thus the sending and receiving computers must have two network-layer addresses for them to communicate.

7.2.2 Services Provided at the Source Computer : MU : Dec. 14, Dec. 16

University Questions

Q. 1 What are the three main functions performed by network layer ? What is routing ? Explain distance vector counting. **(Dec. 14, 10 Marks)**

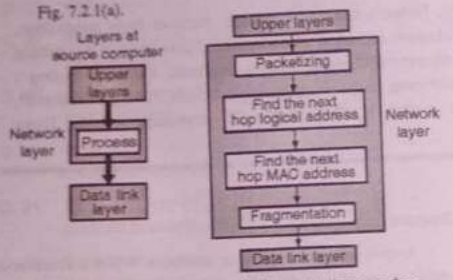
Q. 2 What are three main function of network layer ? What is routing ? Explain distance vector routing. **(Dec. 16, 10 Marks)**

- The following four services are provided by the network layer at the source computer :
  1. Packetizing.
  2. To find the logical address of the next hop.
  3. To find the physical or MAC address for the next hop.

Scanned by CamScanner

4. Fragmentation of the datagram if necessary.

- These services are as shown in Fig. 7.2.1(b).
- The upper layers (transport and application) take services of the network layer. For this the upper layers send several pieces of information.
- The network layer processes these pieces of information and creates fragmented datagrams alongwith the next hop MAC address to finally deliver it to the data link layer as shown in Fig. 7.2.1(a).



(a) Network layer process (b) Network layer services

(G-1999) Fig. 7.2.1

1. Packetizing :

- **Packetizing** is the first duty of the network layer in which it encapsulates the payload (data received from the transport layer) in a packet at network layer at the source. Then at the destination the decapsulation process takes place.
- In this way the network layer is doing the job of a postal service in delivering the packages from source to destination.

At the source :

At the sending end the events take place in the following sequence :

1. The payload (data) from the upper layer is received.
2. A header containing the source and destination address and some other information is added to the payload.
3. This packet is then delivered to the data layer.
4. If the payload is too large, then the host carries out **fragmentation** on it. Otherwise the host is not allowed to modify the contents of the payload.

2. Finding the logical address of the next hop :

- The datagram prepared with packetizing contains the source and destination addresses of the packet.
- The datagram is to be delivered to the next router. But the source and destination addresses in the datagram do not give any information about the logical address of the next hop.
- The network layer at the source computer finds the logical address of the next hop by consulting a routing table.

3. Finding MAC address of next hop :

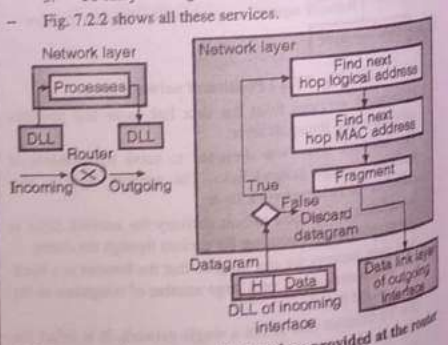
- Note that it is the duty of data link layer (and not of network layer) to actually deliver the datagram to the next hop.
- And to do this the data link layer needs the physical or MAC address of the next hop.
- The network layer uses another table to map the logical address of next hop into the corresponding MAC address of next hop.
- However generally an auxiliary protocol called as ARP (Address Resolution Protocol) is used for this purpose.

4. Fragmentation :

- The datagram at this stage may not always be ready to be given to the data link layer. The LANs and WANs can carry the data of a limited size in a frame.
- If the data is longer than the maximum specified size for LANs and WANs then it is not possible to fit it in one frame.
- In such circumstances, the datagram should be **fragmented** 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.

7.2.3 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. 7.2.2 shows all these services.



(a) Process at the router (b) Services provided at the router

(G-2000) Fig. 7.2.2

- Before providing the services mentioned above the router checks the validity of the incoming datagram with the help of checksum.
- In checking the validation, the following two things are checked :
  1. Whether the datagram header is corrupted.
  2. Whether the datagram is delivered to the correct router.
- If the incoming datagram fails the validation test then it is simply discarded as shown in Fig. 7.2.2(b).

7.2.4 Services Provided at the Destination Computer :

- The sequence of events taking place at the destination is as follows :
  1. The network layer packet is received from the data link layer.
  2. The received packet is decapsulated and the payload is delivered to the upper layer protocol.
  3. If a large packet is fragmented by either the source host or a router, then the responsibility of the network layer at the destination is to wait until all fragments are received, reassemble them and deliver them to the upper layer protocol.
- The network layer at the destination computer is much simpler than that at the source computer or router.
- Before providing any service, the received datagram should be subjected to validation. If it passes the validation test then all the services mentioned above should be provided. Otherwise the datagram is discarded.
- The network layer also sets a reassembly timer when it receives fragments of a datagram that are to be reassembled.
- If the reassembly timer expires before arrival of all the fragments, then all data fragments are destroyed and an error message is sent that the entire fragmented datagram be sent again.

7.3 Routing and Forwarding :

- The other two important duties of the network layer, which are related to each other are routing and forwarding.

7.3.1 Routing : MU : Dec. 14, Dec. 16

University Questions

Q. 1 What are the three main functions performed by network layer ? What is routing ? Explain distance vector counting. **(Dec. 14, 10 Marks)**

Q. 2 What are three main function of network layer ? What is routing ? Explain distance vector routing. **(Dec. 16, 10 Marks)**

- The responsibility of the network layer is to route the packets from its source to destination. The physical network through which the packets travel consists of LANs, WANs and routers.
- Due to this the source and destination are connected to each other via more than one routes.
- It is the responsibility of the network layer to find the best route out of all the possible routes.
- In order to achieve this goal, the network layer must have some concrete strategy for defining the best route.
- In the modern days, this is done by running an appropriate routing protocol which helps the routers to coordinate their knowledge about the neighbouring routers and prepare routing tables which can be used on the arrival of a packet.
- These routing protocols should be run before commencement of any communication.

7.3.2 Forwarding :

- We can define the process of forwarding as the action taken by a router when it receives a packet at one of its interfaces.
- A router takes such an action with the help of the decision making tables called as **forwarding table** or **routing table.**
- When a packet arrives at one of the interfaces of a router from one of the attached network, the router has to forward it to another attached network.
- The router has to make this decision with the help of a piece of information present in the packet header.
- This piece of information can be the **destination address** or a **lable.** The router can use this information to find the corresponding output interface number in the **forwarding table.**

7.4 Other Services :

- The other services expected from the network layer are as follows :
  1. Error control.
  2. Flow control.
  3. Congestion control.
  4. Quality of service (QoS).
  5. Security.
- Let us discuss them one by one.

7.4.1 Error Control :

- Eventhough it is possible to implement the error control at the network layer level, the design engineers have neglected this issue.
- One possible reason for this is that the packets may get fragmented at every router due to which the error checking becomes inefficient.
- However a **checksum** field has been added to the datagram in order to control any corruption in the header only. The error control is not applicable to the whole datagram.
- Thus there is no direct error control provided by the network layer in the Internet. But an auxiliary protocol ICMP is used by the Internet for providing some error control to the datagram.

7.4.2 Flow Control :

- The purpose of providing the flow control is to regulate the data rate of the source so as to avoid the receiver getting overwhelmed.
- The receiver will be overwhelmed if the upper layers at the sending end are producing data at a rate which is higher than the rate at which the upper layers at the destination can consume it (data).

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.

7.4.3 Congestion Control :

MU - Dec. 05, Dec. 07, Dec. 15, May 17

University Questions

Q. 1 Write short note on : Congestion control. **(Dec. 05, Dec. 15, 8 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 control and what are the causes of congestion ? **(May 17, 6 Marks)**

- This is another important issue to be handled at the network layer. **Congestion** will take place if the source computer sends more datagrams than the capacity of the network or routers.
- In this situation, the routers will drop some of the received packets.
- But this will make the congestion worse because the error control mechanism present at the upper layers will retransmit the packets dropped by the routers.
- Sometimes the congestion becomes so bad that the system collapses and no datagrams are delivered at the destination.
- The congestion control at the network layer is never implemented in the Internet.

7.4.4 Quality of Service (QoS) :

- The quality of service in the Internet has become more important since new applications like multimedia communication have been introduced.
- The Internet has grown as it successfully provides the quality of service to support all the modern day applications.
- However the QoS provisions are not implemented in the network layer. They are mostly implemented in the upper layers.

7.4.5 Security :

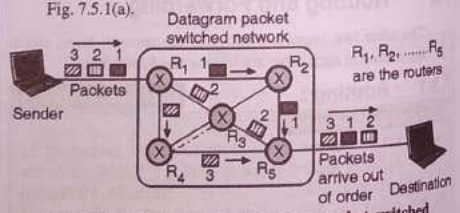
- During the early days of the Internet, security was not a major design concern due to limited (small) number of users. Hence the network layer was designed without any security provisions.
- But security has become a big concern now. But network layer is connectionless. Hence to provide security at the network layer we need to have another virtual level in order to change the connectionless service to connection oriented one.
- The virtual layer is known as IPsec.

7.5 Packet Switching :

- In the previous section we have discussed about routing and forwarding which implies that some kind of **switching** takes place at the network layer.
- A router is basically a switch which connects its input port with an output port or a number of output ports.
- The two types of switching techniques used in data communication are :
  1. Circuit switching and
  2. Packet switching.
- But at the network layer, only the **packet switching** is used because at this layer the unit of data is packet.
- The data received from the upper layers is divided into packets of manageable size and these packets are then sent through the network, one by one sequentially.
- The destination computer receives these packets one by one but not necessarily sequentially.
- When all the packets are received, they are delivered in the form of a message to the upper layers at the destination.
- **Router** is generally the switching device used in packet switched networks. These routers decide the route for each packet to travel from source to destination over the network.
- The two different approaches used for routing the packets are :
  1. The datagram approach. 2. The virtual circuit approach.

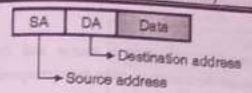
7.5.1 Datagram Approach : Connectionless Service :

- Initially the Internet was made simple by designing the network layer to provide a connectionless service.
- Each network layer protocol treats each packet independently with no relation with any other packet.
- In the datagram packet switching, the packets belonging to the same message also may not take the same route while travelling from source to destination as shown in Fig. 7.5.1(a).



(G-2219) **Fig. 7.5.1(a) : A connectionless packet-switched network**

- Each packet (datagram) has a header in which it contains the source and destination addresses as shown in Fig. 7.5.1(b).
- No dedicated connection is established between the sender and receiver.
- When a switch (router) receives a packet, it has to wait if there are any other packets being processed. This will increase the delay.



(G-2220) **Fig. 7.5.1(b) : Packet format**

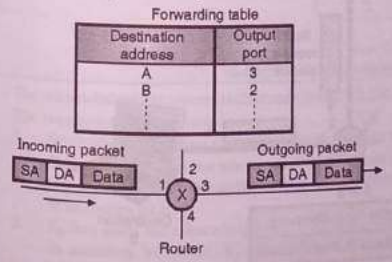
- A connectionless packet switched circuit is shown in Fig. 7.5.1(a).
- In this circuit, three packets are to be delivered from the sender to receiver. The switches in the datagram network are called as **routers.**
- All the three packets (datagrams) belong to the same message in this circuit however actually they can get originated from any computer.
- The three datagrams, as shown in Fig. 7.5.1(a) may travel different paths to reach the destination. Due to this the packets may arrive out of order at the destination.
- The delay associated with each packet will be different as a result of the different paths followed by them. The datagrams may get lost or dropped out due to lack of resources.
- The upper layer protocols are supposed to reorder the received datagrams or ask for the retransmission 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.

7.5.2 Forwarding Process in a Datagram Network :

- In packet switched networks, each packet switch has a routing table.
- The routing tables are dynamic and their information is updated on periodic basis. The routing table consists of destination address and the corresponding output port over which the packet is to be forwarded as shown in Fig. 7.5.2.

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.

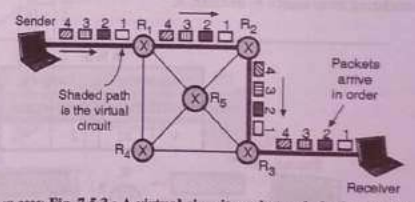


(G-2221) **Fig. 7.5.2 : Forwarding process in a connectionless datagram network**

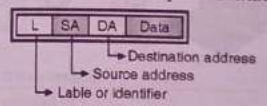
- For example in the routing table of Fig. 7.5.2, if the destination address on the received packet is B then it will be forwarded through port 2.
- In the connectionless datagram network, a router will make the forwarding decision of a packet on the basis of its destination address.

7.5.3 Virtual Circuit Approach : Connection Oriented Service :

- The connection oriented service at the network layer is also called as the virtual circuit approach.
- 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).**
- Here all the packets will follow the same path which was established before communication.
- When the connection is opened, the virtual circuit is also terminated. In the connection oriented service, each packet carries an identifier. This identifier can tell us about the virtual circuit (VC) that this packet belongs to.
- Refer Fig. 7.5.3 in which the sender has established connection-1 with the destination.
- It has been shown with shading in Fig. 7.5.3. The format of each packet being sent on the virtual circuit is as shown in Fig. 7.5.4. As shown it consists of a source address (SA), a destination address (DA), and a flow lable (L) which is a virtual circuit identifier which tells us about the virtual circuit path that this packet is going to follow.



(G-2222) **Fig. 7.5.3 : A virtual circuit packet switched network**



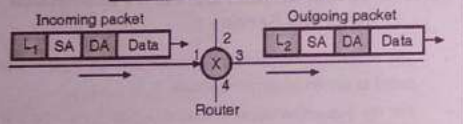
(G-2223) **Fig. 7.5.4 : Packet format for virtual circuit packet switched network**

- At each router in Fig. 7.5.3, each packet is forwarded on the basis of its lable. The **lable** is also called as the **virtual circuit identifier (VCI).** Fig. 7.5.4(a) illustrates the principle of forwarding process on the basis of the lable or VCI.
- When a packet arrives at port-1 of the router, the router checks its forwarding table which shows that this packet is to be sent out on port-3 with a lable number L_2 which is different than the lable of the incoming packet i.e. L_1.

Scanned by CamScanner

Forwarding table

Incoming		Outgoing	
Port	Lable	Port	Lable
1	L_1	3	L_2
2	L_3	4	L_4
⋮	⋮	⋮	⋮



(G-2224) **Fig. 7.5.4(a) : Forwarding process in the virtual circuit network**

Three phases of communication :

- A source and destination have to undergo three phases to communicate between each other in the connection oriented service.
- The three phases are :

  1. Set up 2. Data transfer 3. Teardown

Set up phase :

In this phase the source and destination use their addresses. This will help routers to make table entries for the connection oriented service.

Data transfer :

The data transfer is the second phase in which the packets are transferred from source to destination.

Teardown :

- In the teardown phase both source and destination will communicate the routers to erase the corresponding entry.
- Let us discuss these phases one by one.

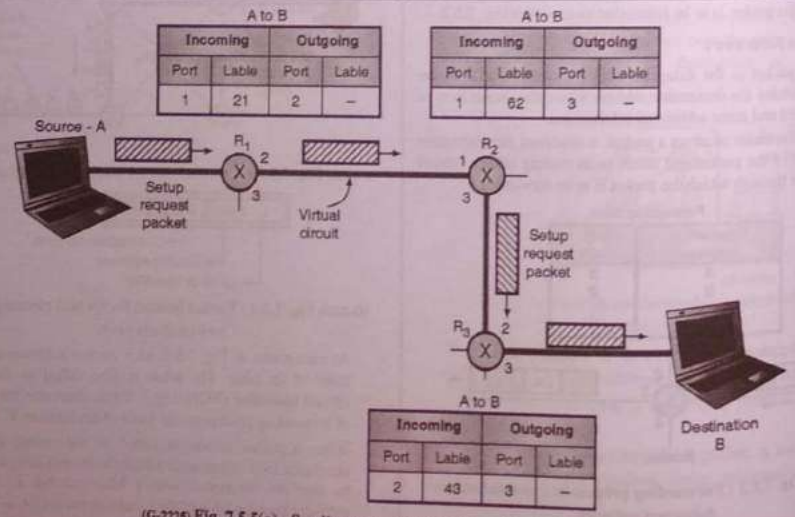
Set up phase :

- The source sends a set up request packet to the destination via various routers as shown in Fig. 7.5.5(a).
- The events take place in the following sequence after that :

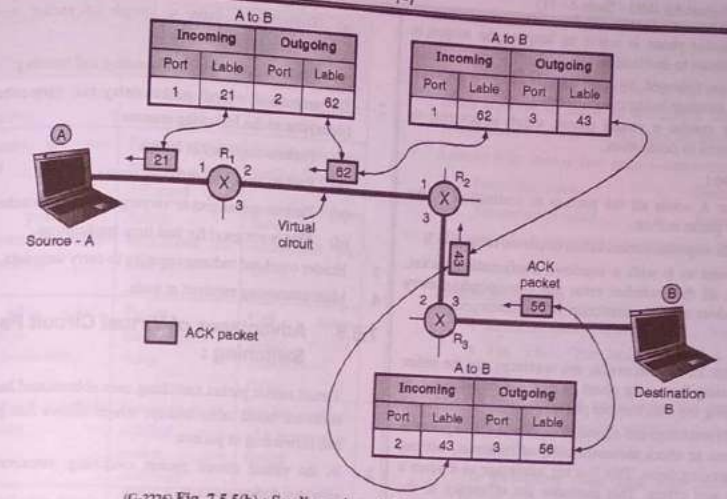
  1. The source A sends a set up packet to router R_1.
  2. Router R_1 has a routing table which is different from the switching table. The router creates an entry in its table for this virtual circuit but it can fill up only 3 columns out of 4, namely incoming port 1, VCI 21 and outgoing port 2. It does not know the outgoing VCI because it is found in the acknowledgement step. The set up packet is forwarded to router R_2.
  3. R_2 receives the set up request packet and same events will take place as those happened at R_1. Three columns are filled : incoming port 1, VCI 62 and outgoing port 3.
  4. Now R_3 receives the set up request packet from R_2. Here also the three columns are filled as : incoming port 2, VCI 43 and outgoing port 3.
  5. Destination B receives the set up request packet. If it is ready to receive packets from source, then a VCI is assigned to the packets coming from the source A. In this case the VCI A is 56. This VCI is an indication that packets come from and not from any other source.

Acknowledgement :

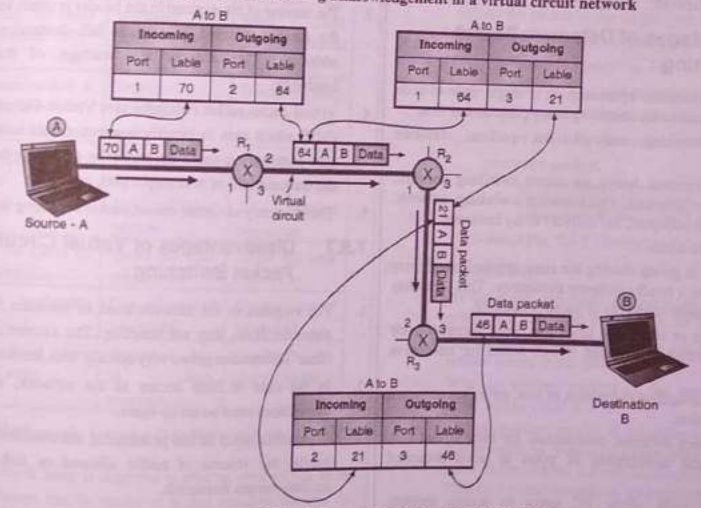
- The acknowledgement packet is sent from the destination B to source A via the three routers. This completes the entries in the tables.



(G-2225) **Fig. 7.5.5(a) : Sending request packet in a virtual circuit network**



(G-2226) **Fig. 7.5.5(b) : Sending acknowledgement in a virtual circuit network**



(G-2227) **Fig. 7.5.5(c) : Source A to destination B data transfer**

- The acknowledgement process is illustrated in Fig. 7.5.5(b).
- The sequence of events is as follows :

  1. Destination B sends an acknowledgement packet to R_3. This packet contains the source and destination address and VCI 56. R_3 fills this number into the fourth column of its routing table.
  2. R_3 then sends the acknowledgement to R_2 that contains its incoming VCI = 43. R_2 fills this into its table as outgoing VCI as shown in Fig. 7.5.5(b).
  3. R_2 sends an acknowledgement to R_1 which contains its incoming VCI = 62. R_1 fills this into its switching table as outgoing VCI.
  4. R_1 sends the acknowledgement which contains its incoming VCI = 21.
  5. Source A uses it as the outgoing VCI for all the data packets directed to destination B.

Source to destination data transfer :

- Fig. 7.5.5(c) shows the actual data transfer taking place between source A and destination B.
- It shows how the VCI of a packet is changed by each switch for routing it from source to destination.

Scanned by CamScanner

- The data transfer phase is active as long as the source is sending its frames to destination.
- The procedure followed by each switch is same for each frame of the message being communicated.
- This process creates a virtual circuit which is not real to connect a source to destination.

Teardown phase :

- When source A sends all the packets to destination B, the data transfer phase is over.
- Then A sends a special packet called teardown request to B.
- B will respond to it with a teardown confirmation packet, after which all the switches erase the corresponding entry from their tables and the connection will be destroyed.

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.

7.5.4 Advantages of Datagram 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.
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.

7.5.5 Disadvantages of Datagram 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.

7.5.6 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.

7.5.7 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.

7.5.8 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

7.6 Network Layer Performance :

- The network layer is expected to give an ideal service to the upper layers but in reality it is not possible because the network layer is not perfect.
- The three factors that determine the performance of a network are as follows :
  1. Delay.
  2. Throughput.
  3. Packet loss.
- In this section we will define these factors and then study their effect on the network performance.

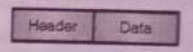
7.6.1 Delay :

- The latency or delay is defined as the time required for an entire message to reach its destination from the instant at which the first bit was sent out from the source.
- Latency is the sum of four delay components viz :
  1. Processing delay
  2. Queueing delay
  3. Transmission delay
  4. Propagation delay.
- The sum of all these delays amounts to the total delay or latency.

1. Processing delay :

- A packet consists of a header and a data field as shown in Fig. 7.6.1. The header contains the destination address.
- The time required to examine the packet header and deciding the direction in which the packet is to be sent is a part of the processing delay.
- The processing delay may also include some other factors such as the time required to check the errors, deliver the packet to the output port (in case of a router) or delivering the packet to the upper layers etc.
- The processing delay is of the order of few microseconds or less, but it is not the same for all the packets. Hence normally it is calculated as an average.

∴ **$Delay_{pr}$ = Time taken by the router or destination host to process a packet.**



(G-696(a)) **Fig. 7.6.1 : Format of a packet**

2. Queueing delay :

- At the queue, the packets experience a queueing delay, when they wait to get transmit on the links.
- The queueing delay depends on the number of packets arrived earlier in the queue.
- With no waiting packets in the queue, the queueing delay will be equal to zero.
- Queueing delays can be of the order of microseconds or milliseconds in practice. These delays normally take place in the routers. As will be discussed later on in this chapter, a router consists of an input queue and an output queue.
- The queueing time for a packet can be defined as the time for which a packet waits in the input and output queue of a router.

∴ **$Delay_{qu}$ = Waiting time for a packet in the input and output queue of a router.**

3. Transmission delay :

- The packets are transmitted on the first come first served basis. So a particular packet can get transmitted only after all the earlier packets are transmitted.

Scanned by CamScanner

- Transmission delay is also called as store and forward delay. It is the time required to push (transmit) all the packet bits into the link.
- Typically, the transmission delay is of the order of microseconds or milliseconds in practice.

$$\text{Delay}_{Tr} = \text{Transmission delay} = \frac{\text{Packet size}}{\text{Transmission rate}}$$

- This means that the transmission delay increases with increase in the packet size at a constant transmission rate. And the transmission delay decreases with increase in the transmission rate.

Ex. 7.6.1 : Find the transmission delay for a LAN which has a packet of 10,000 bits and its transmission rate is 100 million bits/sec.

Soln. :

$$\text{Delay}_{Tr} = \frac{\text{Packet size}}{\text{Transmission rate}} = \frac{10{,}000 \text{ Bits}}{100 \times 10^6 \text{ Bits/sec}} = 100 \times 10^{-6} \text{ sec or } 100\ \mu\text{S}. \quad \text{...Ans.}$$

Conclusion : This means that the given LAN needs 100 μsec. to put all the 10,000 bits in a packet on the line.

4. Propagation delay :

- The time required for the packet bits to reach from point A of the link to point B on the same link called as propagation delay.
- The signals travel at a speed which is slightly less than that of light.
- So propagation delay is the ratio of the distance to be travelled by the signal to the speed of propagation.
- Practically the propagation delays are of the order of few milliseconds.

$$\text{Delay}_{Pg} = \text{Propagation delay} = \frac{\text{Distance}}{\text{Propagation speed}}$$

- The factors affecting the value of propagation delay are as follows :
  1. Propagation speed of signal.
  2. Distance to be covered.
  3. Propagation delay of each network.

Ex. 7.6.2 : Find the propagation delay of the bits that are travelling at a speed of 2×10^8 m/s. over a point to point cable link of 2000 metres length.

Soln. :

$$\text{Delay}_{Pg} = \frac{\text{Distance}}{\text{Speed}} = \frac{2000 \text{ m}}{2 \times 10^8 \text{ m/s}} = 1 \times 10^{-5} \text{ sec or } 10\ \mu\text{sec} \quad \text{...Ans.}$$

Total delay :

- By assuming equal delays for all senders, routers and receivers in a network, the total delay for a packet from source destination is given by,

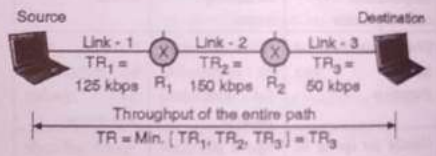
$$\text{Total delay} = (n + 1)\,[\text{Delay}_{tr} + \text{Delay}_{pg} + \text{Delay}_{pr}] + n\,\text{Delay}_{qu}$$

Where n = Number of routers.

- If there are "n" routers, then there will be (n + 1) links. Therefore there will be (n + 1) transmission delays related to n routers and the source, then (n + 1) propagation delays for (n + 1) links, (n + 1) processing delays corresponding to n routers and a receiver and n queuing delays corresponding to n routers.

7.6.2 Throughput (T) :

- The throughput is a parameter that is used to know the speed of data transmission over a network.
- The throughput of a system is defined as the actual rate at which the information is sent over the channel. It is measured in bits/second or frames/second.
- Throughput is a measure of performance of any network.
- However the throughput is not the same at every point in the network. It can have different values at different points.
- There we can define the throughput at any point of the network as the number of bits passing through that point per second.
- A packet passes through several links (networks) while travelling from a source to destination. Each link can have a different transmission rate as shown in Fig. 7.6.2.



(G-2228) **Fig. 7.6.2 : Throughput of a path**

- In such situations, the throughput of the entire path will be equal to the minimum of the transmission rates of different links.
- For Fig. 7.6.2, the throughput of the entire path is equal to 50 kbps i.e. the data rate of link-3.
- In general, the throughput of a path having "n" links in series is given by,

Throughput = Minimum $[TR_1, TR_2, \ldots\ldots TR_n]$

- The definitions of bandwidth and throughput appear to be the same but they are not. They are different.
- If B is the bandwidth and T is the throughput of a network then T is always less than and at the most equal to B.
- Thus bandwidth is the theoretical measurement while throughput is the actual measurement of how fast data can be sent.

Ex. 7.6.3 : A network has a bandwidth of 20 Mbps. It can pass 15,000 frames per minute and each frame contains 10,000 bits. Calculate the throughput. Comment on the result.

Soln. :

Given : $B = 20 \times 10^6$ bps, Number of frames = 15000 per min, Number of bits per frame = 10,000.

Throughput T = Number of frames per sec. × Number of bits per frame

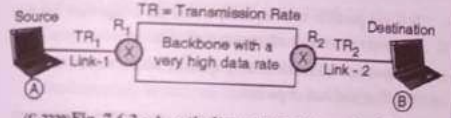
$$= \frac{15000}{60} \times 10{,}000 = 3.5 \text{ Mbps.} \quad \text{... Ans.}$$

Comment :

The value of B = 20 Mbps shows the potential of the network and T = 3.5 Mbps shows the actual capability.

Real life situation-1 :

- In Fig 7.6.3, we have shown the calculation of throughput of a path made of three links.
- But the real life situation in the Internet as demonstrated in Fig. 7.6.3 is different. Here the data passes through two access networks and an Internet backbone.



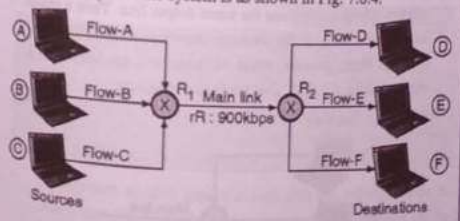
(G-2229) **Fig. 7.6.3 : A path through the Internet backbone**

- The transmission rate of the Internet backbone is extremely high, typically a few Gbits/sec, as compared to the transmission rates TR_1 and TR_2 of the two links in Fig. 7.6.3.
- Therefore the throughput of the end to end path (A to B) is equal to the minimum transmission rate of the two access links.

$$\therefore \text{TR} = \text{Minimum } [TR_1, TR_2]$$

Real life situation – 2 :

- Another real life situation in which we need to calculate the throughput of the system is as shown in Fig. 7.6.4.



(G-2230) **Fig. 7.6.4 : Effect of throughput in shared links**

- Multiple sources (A, B, C) are connected to router R_1. Similarly router R_2 distributes the flow among various destinations (D, E, F).
- The link between the two routers R_1 and R_2 is called as the main link which has a transmission rate of 900 kbps.
- Because the main link shares flows between three sources, the transmission rate of the main link while calculating the throughput will be considered as only 300 kbps i.e. (900/3) and not equal to 900 kbps.

7.6.3 Packet Loss :

- The performance of a network is dependent on one more factor, i.e. the number of packets lost during the communication.
- When a packet arrives at a router, when some other packet is being processed, the recently arrived packet is stored in the input buffer of the router and waits for its turn.
- But the size of input buffer is however finite. Therefore, a time may come when it will become full and the next packet arriving at the rotor input has to be dropped.
- The lost packets need to be retransmitted by the source, this may result in overflow of the input buffer and more loss of packets.
- Network designers have put in lots of time and efforts for design of queues for preventing the overflow and reducing the packet loss.

7.7 Network Layer Congestion :

MU : May 10, Dec. 15

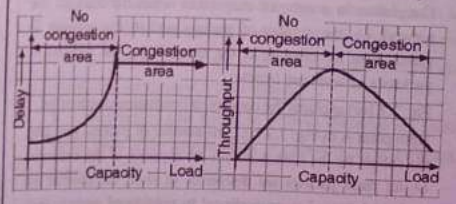
University Questions

Q. 1 What is congestion and what are the causes of congestion ? **(May 10, Dec. 15, 10 Marks)**

- 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. 7.7.1(a) and (b) respectively.



(a) Variation of delay with load **(b) Variation of throughput with load**

(G-2231) **Fig. 7.7.1 : Packet delay and throughput as function of load**

Scanned by CamScanner

1. Variation of packet delay with load :

- Consider Fig. 7.7.1(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.
- 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 :

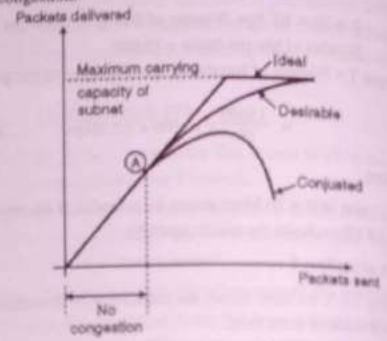
- Now refer Fig. 7.7.1(b) which shows that the throughput increases with increase in load as long as the load is less than the network capacity.
- It is expected that for any load beyond the capacity, the throughput should remain constant. Instead it decreases sharply as the load exceeds the capacity 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.

7.7.1 Congestion : MU : May 08

University Questions

Q. 1 What is congestion ? Explain how it can be avoided. (May 08, 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. 7.7.1(c) explains the concept of congestion graphically.
- Upto point A in Fig. 7.7.1(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. 7.7.1(c) : Concept of congestion

7.7.2 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).

7.7.3 Causes of Congestion : MU : May 10, Dec. 15, May 17

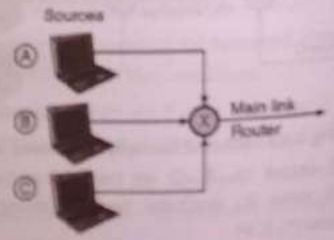
University Questions

Q. 1 What is congestion and what are the causes of congestion ? (May 10, Dec. 15, 10 Marks)

Q. 2 What is congestion control and what are the causes of congestion. (May 17, 6 Marks)

- Some of the causes of congestion are as follows :

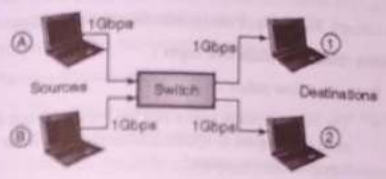
1. If suddenly a flow of packets start coming on three or four senders which all needing the same output line. Then a queue will become long. If the memory capacity is not sufficient to hold all these packets, some of them will be lost. This is shown in Fig. 7.7.2(a). This leads to congestion.



(G-2232) Fig. 7.7.2(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. 7.7.2(b), if both the sources begin to send to destination 1 at their maximum rate, congestion will occur at the switch. Higher speed links can make the congestion condition in the switch worse.



(G-2233) Fig. 7.7.2(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.

7.7.4 Difference between Congestion Control and Flow Control : MU : Dec. 09, Dec. 07

University Questions

Q. 1 Compare congestion control and flow control. (Dec. 09, 5 Marks)

Q. 2 What is congestion control ? How it is different from flow control ? Explain various congestion prevention techniques. (Dec. 07, 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.

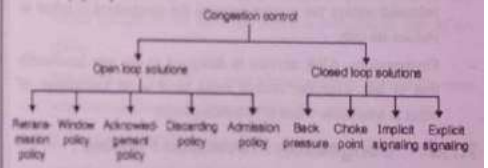
7.7.5 Principle of Congestion Control : MU : Dec. 05, May 09

University Questions

Q. 1 Write short note on : Congestion control. (Dec. 05, 8 Marks)

Q. 2 Explain general principles of congestion control. (May 09, 5 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. 7.7.3 shows the classification of congestion control schemes and various policies used in open loop and closed loop groups.



(G-474) Fig. 7.7.3 : 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.

Scanned by CamScanner

- A closed loop control is based on the following three steps :
  1. Detect the congestion and locate it by monitoring the system.
  2. Transfer the information about congestion to places where action can be taken.
  3. Adjust the system operations to correct the congestion.
- Two examples of closed loop control are :
  1. TCP flow control.
  2. BR rate control for an ATM network.

Open loop versus closed loop :

- Open loop approaches do not need end-to-end feedback, one of the examples of this type are prior-reservation and hop-to-hop flow control.
- In closed-loop approaches, the source can adjust its cell rate on the basis of the feedback information received from the network.
- Some people feel that closed loop congestion control schemes are too slow in 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.

7.7.6 Congestion Prevention Policies :

MU : Dec. 07, May 08, May 11

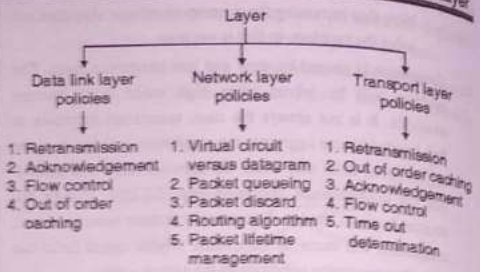
University Questions

Q.1 What is congestion control ? How it is different from flow control ? Explain various congestion prevention techniques. **(Dec. 07, 10 Marks)**

Q.2 What is congestion ? Explain how it can be avoided. **(May 08, 10 Marks)**

Q.3 Explain different congestion prevention policies. **(May 11, 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. 7.7.4 lists various policies corresponding to different layers for avoiding congestion.



(G-477) **Fig. 7.7.4 : Policies affecting the congestion**

Policies related to data link layer :

1. **Retransmission policy :**
   - The retransmission policy and the retransmission timers must be designed to optimise efficiency and at the same time prevent congestion.
   - The retransmission policy deals with how fast a sender times out. If a sender times out early then it will retransmit all the packets and such a retransmission can lead to congestion.
   - By designing the retransmission policy we can avoid this and prevent congestion.
2. **Out of order caching policy :**

   If the receivers routinely discard all the packets which are out of order, then retransmission of these packets will take place. This will increase the load and result in congestion. So a selective repeat (retransmission) should be adopted to avoid congestion.
3. **Acknowledgement policy :**
   - If each received packet is promptly acknowledged then the acknowledgement packets will increase the traffic.
   - If the acknowledgement is delayed (piggybacking) then there is a possibility of time out and retransmission.
   - So a tight flow control has to be exercised to avoid congestion.
4. **Window policy :**

   The type of window at the sender may also affect congestion. The selective repeat window is better than the Go Back N window.

Policies related to network layer :

1. **Choice between virtual circuit and datagrams :**

   This choice at the network layer will affect the congestion because many congestion control algorithms work only with virtual circuit subnets.
2. **Packet queuing and service :**
   - This policy is related to whether the routers have one queue per input line and one queue per output line or both.

   - This policy is also related to the order in which the packets are processed e.g. round robin or priority based etc.
3. **Discard policy :**
   - This policy lays a rule which tells the routers about which packet is to be discarded.
   - A good discard policy can prevent congestion and a bad one will worsen the situation.
4. **Routing algorithms :**

   The routing algorithms can spread the traffic over all the lines. By doing so it is ensured that none of the lines are overloaded. This will certainly avoid congestion.
5. **Package lifetime management :**
   - This policy decides the maximum time for which a packet may live before being discarded.
   - This time should be of adequate value so that congestion can be avoided.

Policies related to transport layer :

- The policies at the transport layer are same as those at the data link layer.
- But at transport layer determining the time out interval is more difficult.
- If it is too short then extra packets are sent unnecessarily whereas if it is too long, congestion will reduce at the cost of increased response time (network will become slow).

Traffic shaping :

- One of the important reason behind congestion is the bursty nature of the traffic. If the traffic has a uniform data rate then congestion would not happen every now and then. But due to bursty traffic it can happen regularly.
- Traffic shaping is an open loop control. It prevents the congestion by making the packet transmission rate to be more predictable (bursty traffic is unpredictable).
- Thus traffic shaping will regulate the average rate or the burstiness of data transmission.
- Monitoring a traffic flow is called as **traffic policing**.
- Check if a packet stream (connection) is as per its descriptor, and if it is not as per its descriptor, then give penalty !
- In order to achieve this the network may want to monitor the traffic flow during the connection period. The process of monitoring and enforcing the traffic flow is called traffic policing.
- The types of penalties enforced are as follows :
  1. Drop packets that violate the descriptor.
  2. Give low priority to the packets violating the descriptor.

7.7.7 Congestion Control In Virtual Circuit Subnets :

- All the congestion control techniques discussed till now were open loop techniques.
- Now let us discuss a dynamic technique called **admission control.**

Admission control principle :

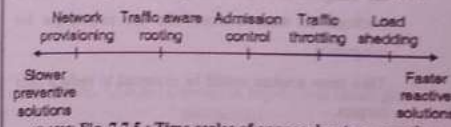
- This technique is used to keep the congestion which has already begun to a manageable level and does not allow it to worsen any further.
- Its principle is as follows : Once congestion has been detected, do not set up any more virtual circuits until the congestion is cleared.
- The advantage of this technique is that it is a simple and easy to carry out control.

Alternative approach :

- An alternative approach to admission control allows the virtual circuits to set up even when a congestion has taken place.
- But carefully route all the new virtual circuits around the area where congestion is already present.

7.7.8 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. 7.7.5 : Time scales of approaches to congestion control**

1. **Network provisioning :**
   - The fundamental way of avoiding congestion is to build a network that is properly matched to the traffic that it is going to carry.

Scanned by CamScanner

- 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.

7.7.9 Congestion Control in Datagram Subnets : MU : Dec. 04, May 10

University Questions

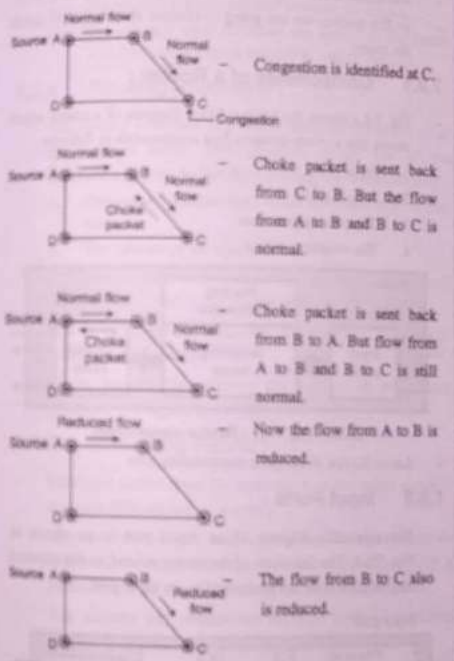
Q. 1 Give one approach of Congestion Control in Datagram subnets. (Dec. 04, 10 Marks)

Q. 2 How one can control congestion in datagram subnet ? Explain. (May 11, 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.).

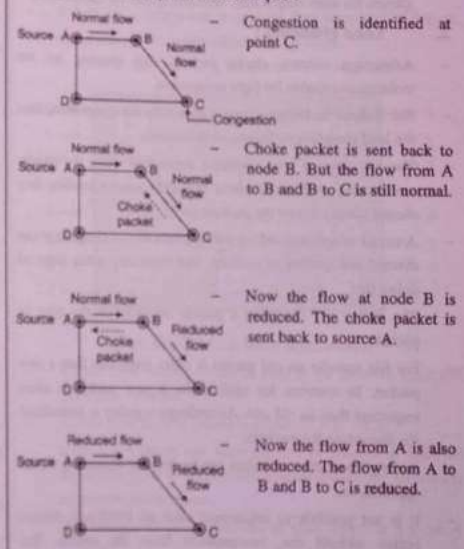


- Congestion is identified at C.
- Choke packet is sent back from C to B. But the flow from A to B and B to C is normal.
- Choke packet is sent back from B to A. But flow from A to B and B to C is still normal.
- Now the flow from A to B is reduced.
- The flow from B to C also is reduced.

(G-478) Fig. 7.7.6(a) : Choke packet mechanism

- If the value of "u" goes above the threshold then that output line will enter into a "warning" state. The router will check each newly arriving packet to see if its output line is in the "warning state".
- If it is in the warning state then the router will send back a **choke packet** signal to the sending host.
- The sender host will not generate any more data packets. This will reduce the congestion.
- Different congestion control algorithm have been proposed, depending on the value of thresholds.
- Depending on the threshold value, the choke packets can contain a mild warning, a stern warning or an ultimatum.
- Another algorithm may use the queue lengths or buffer utilization instead of using the line utilization as a deciding factor.
- The general concept of choke packet mechanism is demonstrated in Fig. 7.7.6(a).
- Fig. 7.7.6(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 :



- Congestion is identified at point C.
- Choke packet is sent back to node B. But the flow from A to B and B to C is still normal.
- Now the flow at node B is reduced. The choke packet is sent back to source A.
- Now the flow from A is also reduced. The flow from A to B and B to C is reduced.

(G-479) Fig. 7.7.6(b) : Concept of hop-by-hop choke packet mechanism

- The problem associated with the general choke packet mechanism can be overcome by using another technique called as hop-by-hop choke packet technique.
- This is demonstrated in Fig. 7.7.6(b). In this approach, the choke packets are used at each hop between the destination and source.

Scanned by CamScanner

- 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. 7.7.6(b) shows how the transmission rate is reduced at every hop in response to the choke packets.

Disadvantage :

The problem with choke packet technique is that the action to be taken by the source host on receiving a choke packet is not compulsory. The host may reduce its transmission rate or ignore the choke packets.

Weighted fair queuing :

- The disadvantage of choke packet technique can be overcome with the help of the weighted queuing technique.
- The queuing algorithm was proposed first in 1987. In this algorithm it is proposed that the routers have a number of queues for each output line, with one queue for each source.

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.

7.8 Structure of a Router : MU : May 04

University Questions

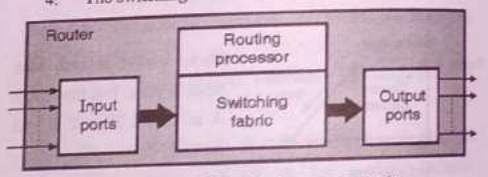
Q. 1 What does routing mean and how does it works ? **(May 04, 5 Marks)**

We know that the principle of operation of a router is as follows :

- A router receives a packet at one of its input ports (also called as an interface), then takes help of the routing table to decide upon the output port from which the packet is to be forwarded and finally sends the packet from the appropriate output port.
- In this section, we are going to discuss about what is inside the router.

7.8.1 Components of a Router :

- Fig. 7.8.1 shows the internal block diagram of a router which shows that a router contains four components as follows :
  1. Input ports.
  2. Output ports.
  3. The routing processor.
  4. The switching fabric.

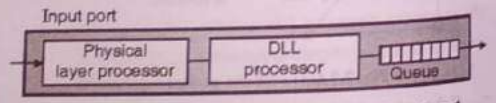


(G-2078) **Fig. 7.8.1 : Router components**

- Let us discuss about these components now.

7.8.2 Input Ports :

- The schematic diagram of an input port is as shown in Fig. 7.8.2. The functions of the router related to the physical and datalink layer are performed by its input port.

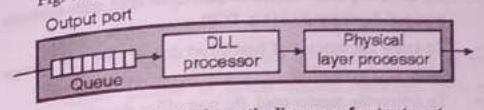


(G-2079) **Fig. 7.8.2 : Schematic diagram of an input port**

- The functions performed by the input port are as follows :
  1. It constructs bits from the received signal.
  2. It decapsulates packet from the frame.
  3. It detects and corrects the errors.
  4. The packet is ready to be forwarded.
  5. The buffers will hold the ready to forward packets before directing them to switching fabric.

7.8.3 Output Ports :

- The functions performed by the output port are same as those performed by the input port but in the reverse order.
- The schematic diagram of an output port has been shown in Fig. 7.8.3.



(G-2080) **Fig. 7.8.3 : Schematic diagram of output port**

- The functions of the output port are as follows :
  1. The outgoing packets are buffered or queued.
  2. The packets are encapsulated to create the frames.
  3. The physical layer functions are applied to the frame. This will create signals that can be sent on the line.

7.8.4 Routing Processor :

- The routing processor in a router performs the functions of the network layer. This processor makes use of the destination address to find the following two simultaneously :
  1. Output port number from where the packet is to be sent out.
  2. The address of the next hop.
- The routing processor carries out the above mentioned activities by accessing the routing table.
- Due to this reason, the activity of the routing processor is called as **table lookup.**
- In the modern day routers, the function of the routing processor is assigned to the input port.

7.8.5 Switching Fabric :

- Moving a packet from the input queue to the output queue is the most difficult task in a router.
- The size of the input / output queue and the overall delay in delivering a packet are dependent on the speed at which a packet is moved from the input queue to the output queue.
- The modern day routers use different types of switching fabrics. We will discuss some of them in brief.

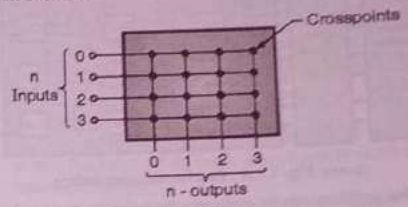
7.8.6 Types of Switching Fabrics :

Some of switching fabric types used by the routers are as follows :

1. Crossbar switch.
2. Banyan switch.
3. A batcher-banyan switch.

7.8.7 Crossbar Switch :

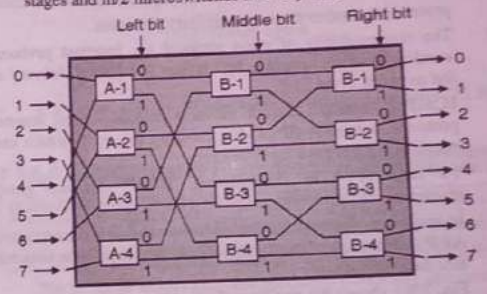
- The simplest type of switching fabric is the cross bar switch, the construction of which is as shown in Fig. 7.8.4.
- The crossbar switch uses electronic microswitches at each crosspoint and connects n inputs to n outputs in a grid, using the switches.



(G-2081) **Fig. 7.8.4 : A crossbar switch**

7.8.8 Banyan Switch :

- This switch is named after the banyan tree. It is a multistage switch with microswitches used at every stage as shown in Fig. 7.8.5.
- If there are m inputs and m outputs, then there will be $\log_2 m$ stages and m/2 microswitches in every stage.



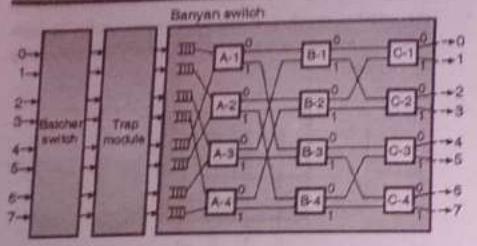
(G-145) **Fig. 7.8.5 : A three layer switch**

- A three layer banyan switch is used at the network layer and it is a kind of router.
- A three layer banyan switch is shown in Fig. 7.8.5.
- It has n = 8 inputs and same number of outputs. A three bit number is used to decide the internal path over which the input is passed to output.
- The number of microswitches at each stage is n/2 i.e. 4 switches.
- The first stage routes the cell based on the high order bit in the binary bit string.
- The second stage routes the cell based on the middle bit and last stage routes it based on the low order bit.
- Note that number of stages = $\log_2 (n) = \log_2 8 = 3$.

7.8.9 Batcher Banyan Switch :

- The banyan switches have a problem that there is a possibility of collision even when two packets are not headed for the same output port.

Scanned by CamScanner

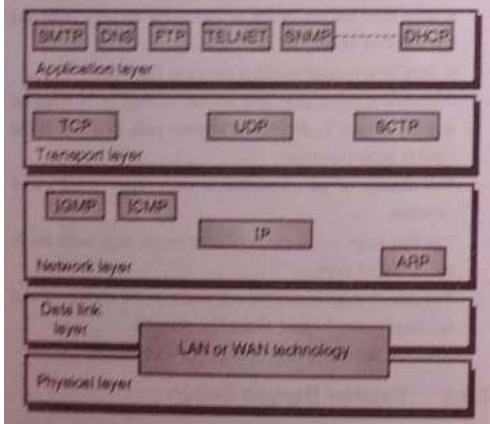


(G-146) **Fig. 7.8.6 : Batcher banyan switch**

- This problem can be overcome by using the batcher banyan switch of Fig. 7.8.6. This switch sorts the incoming packets according to their final destination.

7.9 Network Layer Protocols :

- The main protocols corresponding to the network layer in the TC/IP suite as well as Internet layer are : ARP, IP, ICMP and IGMP.
- Out of these protocols the network layer in version 4 is main protocol and other three are auxiliary protocols.
- The responsibility of main protocol i.e. **Internet protocol version 4** is packetizing, forwarding and packet delivery at the network layer.
- **ICMPv4** (Internet control message protocol) helps Internet protocol version 4 (IPv4) for handling the errors which can occur in the network layer delivery.
- To help IPv4 in multicasting, **IGMP** (Internet group management protocol) is used.
- In mapping of network layer addresses to link layer addresses **ARP** (address resolution protocol) is used to join the network and data link layers.
- Fig. 7.9.1 shows the position of network layer protocols in the TCP/IP protocol suite.



(G-2234) **Fig. 7.9.1 : Position of network layer protocols in TCP/IP protocol suite**

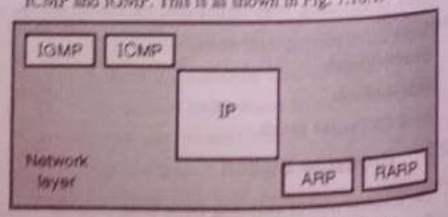
- IPv4 is connectionless and unreliable datagram protocol. It is also known as **best-effort delivery service.**
- The meaning of best-effort is that IPv4 packet can be lost, corrupted, arrive out of order or delayed and IPv4 can create network congestion.
- For reliability there should be pairing of IPv4 with a reliable transport layer protocol (e.g. TCP).
- To know the concept of best effort delivery we can take an example of post office.
- To deliver the regular mail, the post office does its best but it will not succeed always.
- In case of loss of unregistered letter, the post office will not take responsibility. To find out the loss and solve the problem is upto the sender or would-be recipient. The post office will not take any record or track of letter and in case of loss or damage it cannot send any notification to a sender.
- For packet switched network IPv4 is a connectionless protocol which uses datagram approach. That means, handling of each datagram is independent and to the destination each datagram can follow a different route. This implies that datagram could arrive out of order if it is sent by the same source to the same destination.
- During transmission also some datagram could be lost or corrupted.
- To handle and to take care of all these problems, IPv4 relies on a high-level protocol.

7.10 Internet Protocol Version 4 (IPv4) :

- We have already discussed the addressing mechanism, delivery and forwarding for the IP packets.
- Now we will discuss the format of IP packet in the next few sections.
- In the discussion we will see that an IP packet consists of a base header and options which are sometimes useful in controlling the packet delivery.

7.10.1 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. 7.10.1.



(G-824) **Fig. 7.10.1 : Protocols at network layer**

- Out of these protocols IP is the most important protocol. It is responsible for host to host delivery of datagrams from a source to destination. But IP needs to take services of other protocols.
- IP takes help from ARP in order to find the MAC (physical) address of the next hop.
- IP uses the services of ICMP during the delivery of the datagram packets to handle unusual situations such as presence of an error.
- IP is basically designed for unicast delivery. But some new Internet applications as well as multimedia need multicast delivery.
- So for multicasting, IP has to use the services of another protocol called IGMP.
- IPv4 is the current version of IP whereas IPv6 is the latest version of IP.

7.10.2 Internet Protocol (IP) :

- The Internet Protocol is the host to host delivery protocol which belongs to the network layer and is designed for the Internet.
- IP is used as the transmission mechanism by the TCP / IP protocols. That means the TCP or UDP packets are encapsulated in the IP packet and the IP carries it from source to destination.
- IP is a connectionless datagram protocol with no guarantee of reliability.
- It is an unreliable protocol because it does not provide any error control or flow control.
- IP can only detect the error and discards the packet if it is corrupted.
- If IP is to be made more reliable, then it must be paired with a reliable protocol such as TCP at the transport layer.
- Each IP datagram is handled independently and each one can follow a different route to the destination.
- So there is a possibility of receiving out of order packets at the destination. Some packets may even be lost or corrupted.
- IP relies on a higher level protocol to take care of all these problems.
- The version of IP that we are going to discuss is called as IPv4 i.e. IP version 4.
- IP is also called as a **best effort delivery protocol.** The meaning of the term best effort delivery is that the IP packet can get lost or corrupted or delayed. They may arrive out of order at the destination or may create congestion in the network.

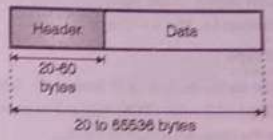
7.10.3 Datagrams : MU : Dec. 12, Dec. 15

University Questions

Q. 1 Explain IPv4 datagram format. **(Dec. 12, 10 Marks)**

Q. 2 What is IP addressing ? Explain IPv4 datagram format. **(Dec. 15, 10 Marks)**

- Packets in IP layer are called datagrams. Fig. 7.10.2 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-825) **Fig. 7.10.2 : IPv4 datagram format**

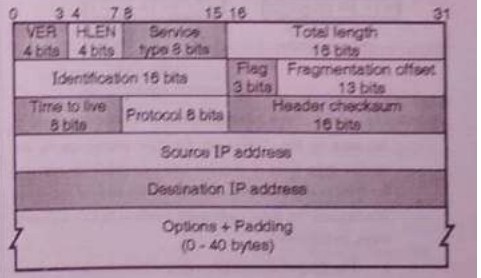
- It is a custom in TCP/IP to show the header in 4-byte (32 bit) sections.

7.10.4 IPv4 Header Format : MU : May 12

University Questions

Q. 1 Explain IPv4 header. Also discuss the need for fragmentation of IP packet. **(May 12, 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. 7.10.3.



(G-2002) **Fig. 7.10.3 : 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.

Scanned by CamScanner

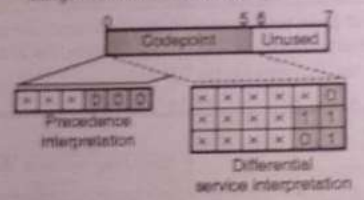
- This field will indicate the IP software running on the processing machine that this datagram belongs to IPv4 version.
- If the processing machine is using some other version of IP, then the datagram will be discarded.

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 x 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 x 4 = 60 bytes.

3. Service type :

- In the earlier designs of IP header, this field was called as **Type of Service** (TOS) field and its job was to define how the datagram should be handled.
- At that time, a part of this field used to define the precedence of datagram and the remaining part used to define the type of service out of different possible services such as low delay, high throughput etc.
- But now the interpretation of this field has been changed by IETF. This field is now supposed to define a set of **differential services.** Fig. 7.10.4 illustrates the new interpretation of the **service type** field.



(G-2083) **Fig. 7.10.4 : New interpretation of service type field**

- As seen in Fig. 7.10.4, 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 lower precedence (0) will be discarded first.

Differential service interpretation :

- When the three rightmost bits are not all zeros, the 6 bit codepoint subfield is used for differential service interpretation.
- In that case these 6 bits can be used for defining a total of 56 (64 – 8) services, on the basis of the priorities assigned by the Internet or local authorities as per Table 7.10.1.

Table 7.10.1 : Values of codepoints

Category	Codepoint	Assigning authority
1.	××××× 0	Internet
2.	×××× 1 1	Local
3.	×××× 0 1	Temporary or Experimental

- The first, second and third categories contain 24, 16 and 16 service types respectively.
- The Internet authorities assign the first category. The local authorities assign the second while the third one is temporary and can be used for experimental purposes.

4. Total length :

- This 16 bit field is used to define the total length of the IP datagram. The total length includes the length of header as well as the data field.
- The field length of this fields is 16 bits so the total length of the IP datagram is restricted to $(2^{16} - 1) = 65535$ bytes out of which 20 to 60 bytes constitute the header and the remaining bytes are reserved to carry data from upper layers.
- This field allows the length of a datagram to be upto 65,535 bytes, although such long datagrams are impractical for most hosts and networks.
- All hosts must be prepared to accept datagram of upto 576 bytes, regardless of whether they arrive whole or in the form of fragments.
- The hosts are recommended to send datagram larger than 576 bytes only if the destination is prepared to accept larger datagram.
- We can find the length of data by subtracting the header length from the total length.
- As stated earlier the header length can be obtained by multiplying the contents of HLEN field by four.

  ∴ 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 ?

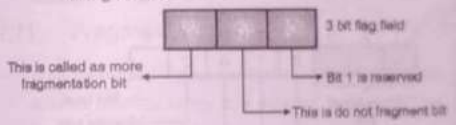
- We might feel that the **total length** field is not at all required because the host or router will drop the header and trailer when it receives a frame. Then why to include this field ?
- The answer to this question is that in many situations we do not need this field at all.
- But in some special 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.

6. Flags :

- **Flags :** This is a three bit field. The 3 bits are as shown in Fig. 7.10.5.

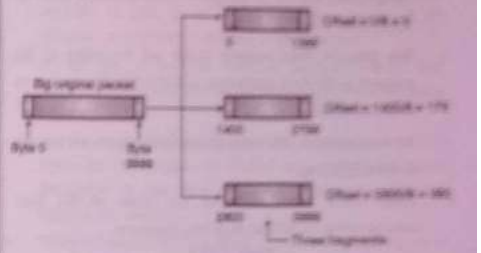


(G-527) **Fig. 7.10.5 : Flag bits**

- First bit is reserved, and it should be 0.
- The second bit is known as the "Do Not Fragment" bit. If this bit is "1" then machine understands that the datagram is not to be fragmented.
- But if the value of this bit is 0 then the machine should fragment the datagram if and only if necessary.
- The third bit is known as "More Fragment Bit" (M). M = 1 indicates that the datagram is not the last fragment and M = 0 indicates that this is the last or the only fragment.

7. Fragmentation offset :

- This is a 13 bit field which is used to indicate the relative position of this fragment with respect to the complete datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.
- To understand this refer Fig. 7.10.6.
- 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. 7.10.6.
- 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. 7.10.6 : 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.**

Scanned by CamScanner

- The TTL field is also used to **limit the journey of a packet intentionally.** For example if a packet is to be confined to a local network only then a 1 is stored in the TTL field of this packet.
- As soon as it reaches the first router, then TTL field value is decremented from 1 to 0 and the packet will be discarded.

9. Protocol :

- This is an 8-bit field which is used for defining the higher level protocol which uses the services of IP layer.
- The data from different high level protocols can be encapsulated into an IP datagram. These protocols could be UDP, TCP, ICMP, IGMP etc.
- The protocol field contents would tell the name of the protocol at the final destination to which this IP datagram is to be delivered.
- At the destination, the value of this field helps in the process of demultiplexing.
- Table 7.10.2 shows some of the values of this field corresponding to different high level protocols.

Table 7.10.2

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 :

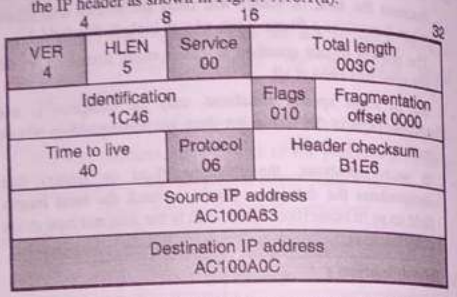
Options are not required for every datagram. They are used for network testing and debugging. We have discussed all the options in detail, later in this chapter.

Ex. 7.10.1 : A IP header from an IP packet received at destination 4500003c1c4640004006b16ac 100a63 ac100a0c. Map these values to IP header and explain all bits.

Dec. 14, 10 Marks

Soln. :

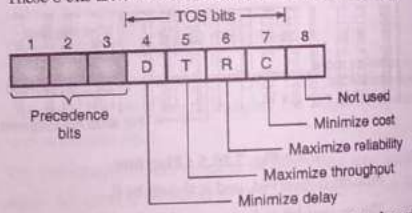
- The IP packet data received at the destination is in the form of hexadecimal digits (4 bits each).
- The IP header is as shown in Fig. P. 7.10.1(a). In the received IP packet data there are 40 hex digits (4 bits each) or 20 bytes. The received data has been placed in various fields of the IP header as shown in Fig. P. 7.10.1(a).



(G-1780) **Fig. P. 7.10.1(a) : IPv4 header format**

Explanation :

1. **Version (VER)** = 4. Therefore the version is IPv4.
2. **Header length (HLEN)** = 5. Therefore the header length is $5 \times 4 = 20$ bytes.
3. **Service** = 00. This field indicates differentiated services. These 8 bits are bifurcated as shown in Fig. P. 7.10.1(b).



(G-1781) **Fig. P. 7.10.1(b) : Service type or differentiated services**

From Fig. P. 7.10.1(b),

Precedence bits are 000, which shows that this packet has the least priority in the event of congestion.

TOS bits are 0000 which indicates that the type of service is normal service or default service.

4. **Total length** = 003C. This defines the total length of the IPv4 datagram (header + data) in bytes.

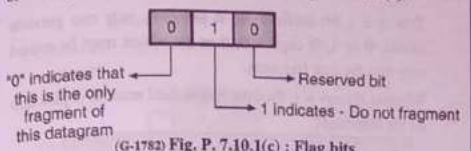
Total length = 003C

= 36 bytes (header + data)

∴ Number of data bytes = 36 – 20 (header bytes) = 16 bytes.

5. **Identification :** This is a 16 bit field. Its value here is 1C46. It is the identification number of this datagram. If it is fragmented, then this number will be copied into all the fragments. At the destination the same number will be used to reassemble all the fragments of this datagram.

6. **Flags :** The contents are as shown in Fig. P. 7.10.1(c).



(G-1782) **Fig. P. 7.10.1(c) : Flag bits**

7. **Fragmentation offset :**

This is a 13 bit field and they are all zeros in this case. So the number of the first byte obtained by multiplying offset value by 8 will be 0.

8. **Time To Live :** TOL = 40 in this case.

This value is approximately twice the maximum number of routers between any two hosts. When this datagram passes through a router it will decrement this number by 1. When TOL becomes 00 the router will discard this datagram.

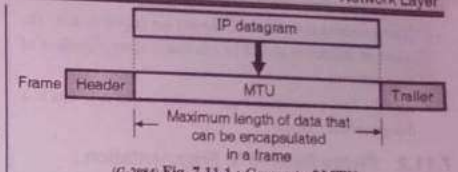
9. **Protocol** = 06. That means the higher level protocol which uses the services of the IP layer is TCP.
10. **Checksum** = B1E6 This is used at the destination to verify if the header has been received without any errors.
11. **Source IP address** = AC100A63 it is a 32 bit address.
12. **Destination IP address** = AC100A0C it is also a 32 bit address.

7.11 Fragmentation :

- In the Internet, a datagram sent by a host has to travel through different networks before it is delivered to the destination host.
- At every router, the received frame is decapsulated, the IP datagram is extracted and processed and encapsulated in another frame.
- The size and format of the frame received by a router depends on the protocol used by the previous physical network to the router.
- As an example, imagine that a router connects a LAN to a WAN. Then the frame received by the router is in the LAN format and the one forwarded by it is in the WAN format.

7.11.1 Maximum Transfer Unit (MTU) :

- The frame format of each data link layer protocol is different in its own way. One of the important field in the frame format is the **maximum size of data field.**
- Therefore when we encapsulate an IP datagram in a frame, the datagram size should be less than the maximum data size specified by the maximum size field.
- The concept of MTU has been illustrated in Fig. 7.11.1.



(G-2084) **Fig. 7.11.1 : 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.

Scanned by CamScanner

- The remaining fields in the IP header are copied as it is. The value of checksum should be calculated again regardless of fragmentation.
- And the final point about fragmentation is that only data in a datagram is fragmented.

7.11.2 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.

.12 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.

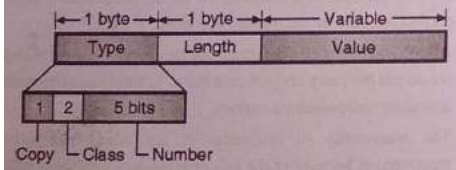
Options as the name suggests are not required for a datagram. Their main application is for network testing and debugging.

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.

.12.1 Format :

The format of an option has been shown in Fig. 7.12.1. 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. 7.12.1 : Option format**

Let us discuss these fields one by one.

Type :

As shown in Fig. 7.12.1, 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 7.12.1.

Table 7.12.1

Number	Type of option
00000	End of option.
00001	No option.
00011	Loose source route
00100	Timestamp
00111	Record root
01001	Strict source route

- We will discuss these later in this chapter.

2. Length :

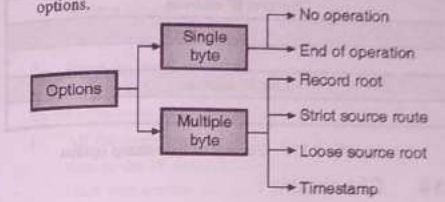
- This 8-bit field is used for defining the total length of the option with the type field and the length field included.
- The length field will not be present in all the option types.

3. Value :

- This is variable length field which contains the specific data which is required by that option.
- Similar to the length field, the value field also will not be present in all the option types.

7.13 Option Types :

- As we started earlier, only six options are being used currently. Fig. 7.13.1 shows the classification of these options.

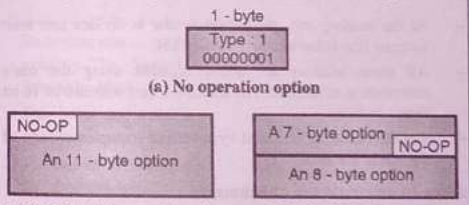


(G-2086) **Fig. 7.13.1 : Categories of options**

- Options are classified into two option types i.e. single byte options and multiple byte options.
- There are two single byte options which do not require the data or length fields.
- The remaining four options are multibyte options which require the data and length fields.
- Let us now discuss these options one by one.

7.13.1 No Operation Option :

- This is a **single byte** option which is being used as a **filler** between options.
- As shown in Fig. 7.13.2, we can use the no operation option to align the next option on a 16 bit or 32 bit boundary.



(a) No operation option

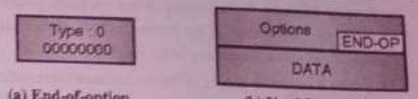
(b) NO-OP is being used to align beginning of an option

(c) NO-OP is being used to align the next option

(G-2087) **Fig. 7.13.2 : No operation option**

7.13.2 End of Option Option :

- The second one byte option is the **end of option** option. It finds its application in **padding** at the end of the option field.
- Two important points about this option are as follows :
  1. We can use it only as the last option.
  2. We can use only one end of option. That means after this option, the receiver should expect the **payload data** to arrive.
- There if we need more than 1 byte to align the option field, then we must use more than one **no-operation** options and after that only one end-of-operation option as shown in Fig. 7.13.3.



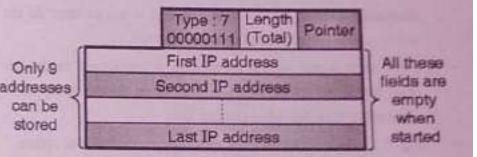
(a) End-of-option

(b) Used for padding

(G-2088) **Fig. 7.13.3**

7.13.3 Record-Route Option :

- The record route option is a multiple byte option and it is used for recording the Internet routers which handle the datagram.
- Since the maximum size of the header is 60 bytes, including 20 bytes of base header, this option can list upto 9-IP addresses of the routers.
- So actually only 40 bytes are left for the option part. The format of the record-root option is as shown in Fig. 7.13.4. The source creates fields that are to be filled by each router visited by the datagram.



(G-2089) **Fig. 7.13.4 : Round trip option**

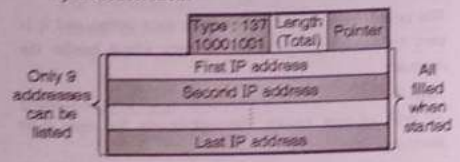
- The pointer field is an offset integer field which contains the byte number of the first empty entry. That means it points towards the first available entry.
- All the empty fields for the IP address are empty when the datagram leaves the source. The value of pointer field is 4 which points to the first empty field.
- When the datagram starts travelling, each router visited by this datagram, will insert its outgoing IP address in the next empty field and increments the value of pointer by 4.

7.13.4 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.

Scanned by CamScanner

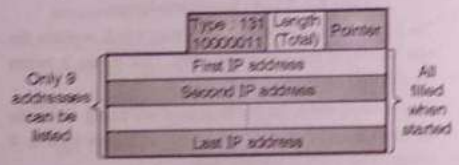
- However the strict source routing is not generally preferred even by the regular users of the Internet, as they are not much aware of the physical topology of the Internet.
- Fig. 7.13.5 shows the format of the strict source route option. You will see that it is very similar to the format of the **record-root option** that we have discussed earlier with one exception that all the nine IP addresses of routers are entered by the sender itself.



(G-3090) **Fig. 7.13.5 : Format of strict source root option**

7.13.5 Loose-Source-Root Option :

- This option is similar to the strict source root option discussed earlier. However this option is not as strict as the strict source root option, it is more relaxed.
- Here each router whose IP address is mentioned in the list must be visited by the datagram as before but the datagram is allowed to visit the other routers also.
- Fig. 7.13.6 shows the format of the loose-source-root option.

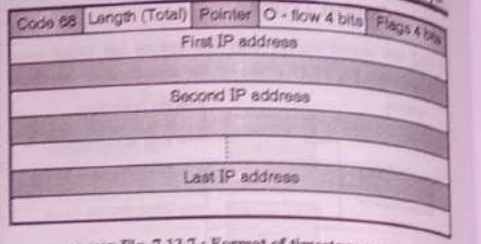


(G-3091) **Fig. 7.13.6 : Format of loose-source root option**

7.13.6 Time Stamp Option :

- The time stamp option is a multiple byte option and it is used for recording the time of datagram processing by a router, i.e. the time instant at which the datagram is processed by a router.
- This time is measured from midnight universal time and expressed in milliseconds.
- The users and managers can use the time of processing a datagram to track the behavior of the router in the Internet.
- With the help of the time stamp option, we can estimate the time taken by a datagram to travel from one router to the other.

However this option is not used by most of the Internet as they are not aware of the physical topology of the Internet. Fig. 7.13.7 shows the format of the time stamp option.



(G-3092) **Fig. 7.13.7 : Format of timestamp option**

7.14 Checksum :

- Most TCP/IP protocol use the error detection method which is called as **checksum.** The purpose of using the checksum is to protect the packet from the corruption that may happen when the packet travels from source to destination.
- Checksum does not carry any information. Therefore it is the **redundant** bits added to the packet.
- The sending machine calculates the checksum and send its value with the packet. At the receiver the same calculation is performed on the whole packet including the checksum.
- The receiver will accept the packet if the result of the calculation is **satisfactory.** Otherwise the packet will be rejected.

7.14.1 Checksum Calculation at the Sender :

- At the sending end, the packet header is divided into n-bit sections (the value of n is generally 16).
- All these sections are added together using the one's complement arithmetic. The addition (sum) will also be 16 bit long.
- The **checksum** is obtained by inverting (complementing) all the bits in the sum.

Steps to calculate the checksum :

1. Divide the packet into K sections with each section containing n-bits.
2. Add all the K-sections together using one's complement arithmetic.
3. Complement the final result of addition to obtain the checksum.

7.14.2 Checksum Calculation at the Receiver :

- The receiver receives the packet and divides it into K sections and then adds all the sections.
- The result of addition is then complemented. The packet is accepted if the final result is zero, otherwise it is rejected.

Checksum in the IP packet :

- If we want to implement the checksum in an IP packet then we should follow the same principle discussed earlier in this section.

- The stepwise procedure for calculating the checksum is as follows :
  1. Set the value of the checksum field to 0.
  2. Divide the entire header into 16 bit sections and add all of them together.
  3. Complement the result (sum).
  4. Insert the complemented result into the checksum field.
- In the IP packet, the checksum covers only the header and not the data due to the following three reasons :
  1. All the high level protocols, which encapsulate their data in the IP datagram have a checksum field which takes into account the whole packet. Therefore the IP datagram need not consider the encapsulated data again while calculating its own checksum.
  2. The second reason is that when an IP packet visits a router, only its header changes but there is no change in data. Therefore, the checksum should take into account only that part which changes i.e. the header.
  3. If the data were included in the checksum calculation, then each router would have to recalculate the checksum for the whole packet which would increase the **processing time.**

7.15 IPv4 Addresses : MU : May 17

University Questions

Q. 1 Explain IP address and subnet mask. (May 17, 5 Marks)

- Each computer connected to the Internet should be identified uniquely. The identifier used for this purpose is called as the **Internet address** or IP address.
- The hosts and routers on the Internet have unique IP addresses.
- The current version of IP (Internet Protocol) is IPv4 whereas the advanced version is IPv6.
- The IPv4 address is a 32-bit address and it is used for defining the connection of a host or router to the Internet. **Thus an IP address is an address of the interface.**

7.15.1 Uniqueness of IP Addresses :

- The IP address is **unique** and **universal.** That means each IP address defines only **one connection** to the Internet.
- At any given time, no two devices connected to the Internet can have the same IP address.
- But if a device is connected to the Internet via two connections through two different networks, then it can have two different IP addresses.
- All the IPv4 addresses are 32 bit long and they are used in the source address and destination address fields of the IP header.
- The IP addresses for hosts are assigned by the network administrator. For Internet it has to be obtained from the network information center.

7.15.2 Address Space :

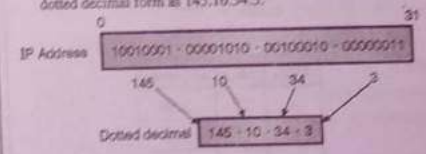
- The IPv4 protocol has an address space. It is defined as the total number of addresses used by the protocol.
- If N number of bits are used for defining an address then the address space will be 2^N addresses.
- For IPv4, N is 32 bits. Hence its address space is 2^{32} or 4, 294, 967, 296 (more than 4 billion). So theoretically more than 4 billion devices could be connected to the Internet.
- Thus **the address space** of IPv4 is 2^{32}.

7.15.3 Notation :

- The IPv4 addresses can be shown use three different notations as follows :
  1. Binary notations (base 2).
  2. Dotted decimal notation (base 256).
  3. Hexadecimal notation (base 16).
- Out of these the **dotted decimal** notation is most commonly used.

Dotted decimal notation :

- This notation has become popular because of the two advantages it offers. This notation makes the IPv4 address more compact and easy to read.
- The 32 bit IPv4 address is grouped into groups of 8-bits each separated by decimal points (dots).
- Each 8-bit group is then converted into an equivalent decimal number as shown in Fig. 7.15.1.
- 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 1001 0001.00001010 00100010 00000011 is denoted in the dotted decimal form as 145.10.34.3.

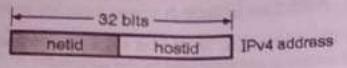


(G-3091) **Fig. 7.15.1 : Dotted decimal notation**

7.15.4 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. 7.15.2 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.

Scanned by CamScanner



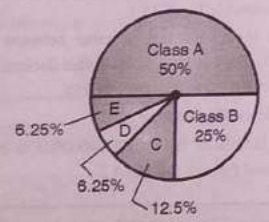
(G-2002) **Fig. 7.15.2 : IPv4 address format**

7.16 Classful Addressing :

- The concept of IP addresses is few decades old. It uses the concept of **classes**. This architecture is called as the **classful addressing.**
- Later on in mid 1990s a new architecture of addressing was introduced which was known as **classless addressing.** This new architecture has superseded the original architecture.
- In this section we are going to discuss the classful addressing.

7.16.1 IPv4 Address Classes :

- In the classful addressing architecture, the IP address space has been divided into five classes : A, B, C, D and E.
- Fig. 7.16.1 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. 7.16.1 : Classful addressing occupation of address space**

7.16.2 Formats of Various Classes :

MU : Dec. 05, Dec. 06, Dec. 07, May 08, May 09, Dec. 09, May 10, May 11, Dec. 11, May 12, May 15

University Questions

Q. 1 Describe the classification of IP-addresses in IPv4. **(Dec. 05, 5 Marks)**

Q. 2 Explain IP address. **(Dec. 06, May 08, 10 Marks)**

Q. 3 Explain IP address with examples. **(Dec. 07, 2 Marks)**

Q. 4 What are different classes of IP addresses ? Give the format of each class. **(May 09, Dec. 09, 5 Marks)**

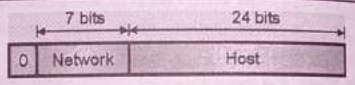
Q. 5 Explain IPv4 protocol and differentiate with IPv6 protocol. **(May 10, 10 Marks)**

Q. 6 Write short note on IP Addresses. **(May 10, 5 Marks)**

Q. 7 What are different types of IP address ? Give the total number of Networks and total number of Host for each type of IP address. **(May 11, May 12, 5 Marks)**

Q. 8 Explain IP address with example. **(Dec. 11, May 12, 2 Marks)**

Q. 9 Explain the different classes of IP addresses and need of subnetting with the help of example. **(May 15, 10 Marks)**



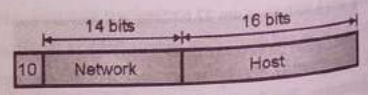
(G-531) **Fig. 7.16.2(a) : Class A IPv4 address formats**

Class A format :

- The formats used for IPv4 address are as shown in Fig. 7.16.2. The IPv4 address for class A networks is shown in Fig. 7.16.2(a).
- The network field is 7 bit long as shown in Fig. 7.16.2(a) and the host field is of 24 bit length. So the network field can have numbers between 1 to 126.
- But the host numbers will range from 0.0.0.0 to 127.255.255.255.
- Thus in class A, there can be 126 types of networks and 17 million hosts.
- The "0" in the first field identifies that it is a class A network address.

Class B format :

- The class B address format is shown in Fig. 7.16.2(b).
- The first two fields identify the network, and the number in the first field must be in the range 128 - 191.

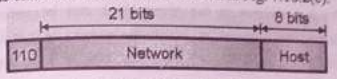


(G-532) **Fig. 7.16.2(b) : Class B format**

- 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. 7.16.2(c).



(G-533) **Fig. 7.16.2(c) : Class C format**

- The first block in class C covers addresses from 192.0.0.0 to 192.0.0.255 and the last block covers addresses from 223.255.255.0 to 223.255.255.255.

Class D format :

- The class D address format is shown in Fig. 7.16.2(d).

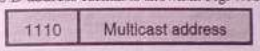


Fig. 7.16.2(d) : Class D format

- The class format allows for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

Class E address format :

- Fig. 7.16.2(e) shows the address format for a class E address. This address begins with 11110 which shows that it is reserved for the future use.

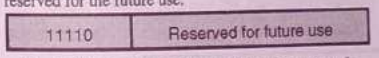
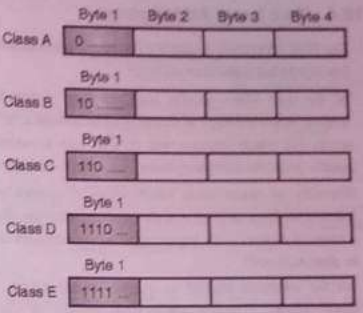


Fig. 7.16.2(e) : IPv4 address for class E network

- The 32 bit (4 byte) network addresses are usually written in dotted decimal notation. In this notation each of the 4-bytes is written in decimal from 0 to 255.
- So the lowest IP address is 0.0.0.0 i.e. all the 32 bits are zero and the highest IPv4 address is 255.255.255.255.

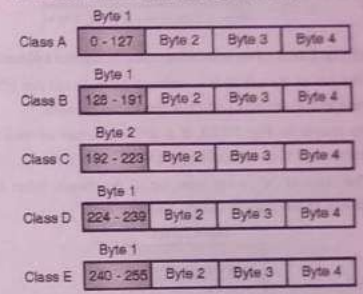
7.16.3 How to Recognize Classes ?

- When an IPv4 address is given to us either in the binary or dotted decimal notation, we can find the class of the address.
- If the given address is in the binary notation then we can identify its class by inspecting the first few bits of the address. This is as shown in Fig. 7.16.3(a).



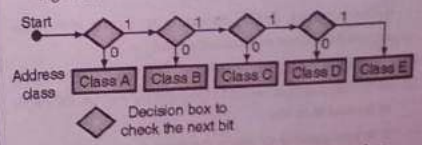
(G-2004) **Fig. 7.16.3(a) : Finding the address class**

- If the given address is in the dotted decimal notation then we can identify the address class by inspecting the first byte of the address. This is as shown in Fig. 7.16.3(b).



(G-2005) **Fig. 7.16.3(b) : Finding the address class**

- It is important to note here that there are some special addresses which fall in class A or E. These special addresses are to be treated as the exceptions to the classful addressing. We have discussed them later in the chapter.
- In computers, the IPv4 addresses are generally stored in the binary notation format. Therefore it is possible to write an algorithm which can identify the address class by using the continuous checking process.
- The principle of such an algorithm has been shown in Fig. 7.16.4.

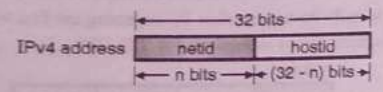


(G-2006) **Fig. 7.16.4 : Algorithm to identify address class**

Scanned by CamScanner

7.16.4 Two Level Addressing :

- The IPv4 addressing is used for defining a destination for an Internet packet at the network layer.
- At the time when classful addresses were designed, the Internet was considered as the network of networks. In other words the whole Internet was divided into a number of smaller networks with many hosts connected to each network.
- Normally an organization which wants to connect to the Internet creates a network and the Internet authorities allocate a block of address to the organization. These addresses can be in class A, B or C.
- All the addresses allotted to an organization belong to a single block. Therefore each IPv4 address in classful addressing system is made up of two parts namely **net id** and **host id** as shown in Fig. 7.16.5.



(G-2007) **Fig. 7.16.5 : Two level addressing in classful addressing**

- The job of the **net id** is to define a network and that of the **host id** is to define a particular host in that network.
- As shown in Fig. 7.16.5 if n bits define **net id** then the remaining (32-n) bits define **host id.**
- The value of "n" is not same for all the classes. Infact it is depend on the class as shown in Table 7.16.1.

Table 7.16.1

Class	Value of n
A	n = 8
B	n = 16
C	n = 24

7.16.5 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. 7.16.6.

1. Total number of addresses in the block :

The total number of IPv4 addresses in the given block will be equal to,

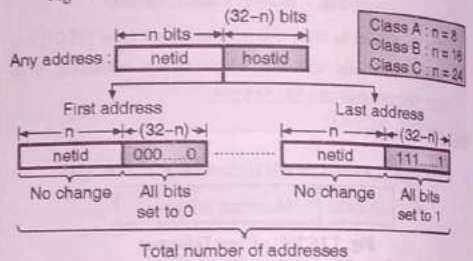
$$N = 2^{(32-n)} \quad \ldots(7.16.1)$$

2. First address in the block :

The first address in the given block can be obtained by keeping the leftmost "n" bits in the address as it is and setting all the (32 – n) rightmost bits to 0 as shown in Fig. 7.16.6.

3. Last address in the block :

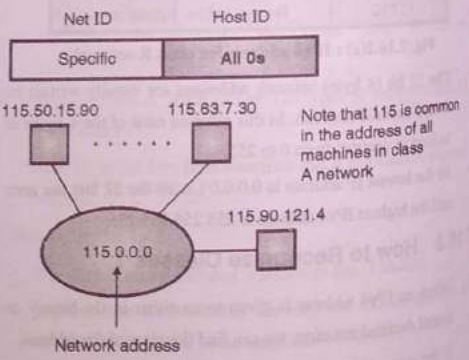
The last address in the given block can be obtained by keeping the leftmost "n" bits in the address as it is and then setting all the (32 – n) rightmost bits to 1 as shown in Fig. 7.16.6.



(G-2008) **Fig. 7.16.6 : Information extraction in classful addressing**

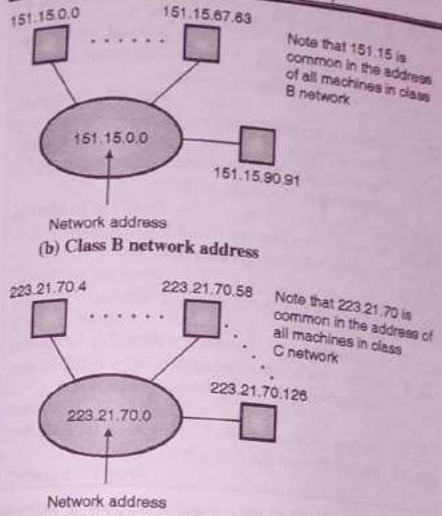
7.16.6 Network Address :

- The network address is an address that defines the network itself. It cannot be assigned to a host. Fig. 7.16.7 shows the examples of network addresses for different classes.



(a) Class A network address

(G-536) **Fig. 7.16.7 (Contd..)**



(b) Class B network address

(c) Class C network address

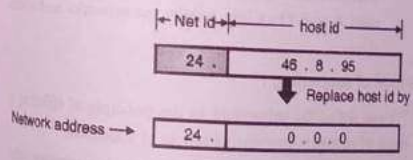
(G-536) **Fig. 7.16.7**

- The following examples will enable you to find the network address.

Ex. 7.16.1 : For the address 24.46.8.95 identify the type of network and find the network address.

Soln. :

- Examine the first byte. Its value is 24 i.e. it is between 0 and 127. So it is a class A network.
- So only the first byte defines the Net id. So we can find the network address by replacing the host id with 0s.
- The process of obtaining the network address is shown in Fig. P. 7.16.1.



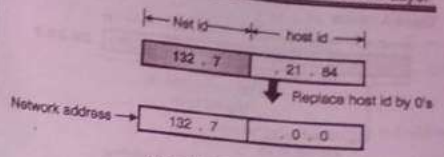
(G-537) **Fig. P. 7.16.1**

So the network address is 24.0.0.0.

Ex. 7.16.2 : For the address 132.7.21.84 find the type of network and the network address.

Soln. :

- Examine the first byte. It is 132 i.e. between 128 and 192. So it is a class B network.
- So the first two bytes define the net id. Replace the host id with 0's to get the network address as shown in Fig. P. 7.16.2



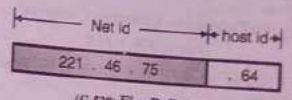
(G-538) **Fig. P. 7.16.2**

So the network address is 132.7.0.0.

Ex. 7.16.3 : Find the class of the network if the address is 221.46.75.64.

Soln. :

The first byte is 221 i.e. between 192 and 255. So this is a class C network. The net id and host id are as shown in Fig. P. 7.16.3.



(G-539) **Fig. P. 7.16.3**

What is the difference between net id and network address ?

The network address is different from a net id. A network address has both net id and host id, with 0s for the host id.

Where to use the network address ?

The network address is used to route the packets to the desired location.

7.16.7 Network Mask or Default Mask :

- Earlier we have discussed the methods for extracting different pieces of information. But all these methods are theoretical methods which are useful in explaining the concept.
- But practically these methods are not used. When a packet arrives at the input of the router in the Internet, it uses an algorithm to extract the **network address** from the destination address in the received packet.
- This can be achieved by using a **network mask.**

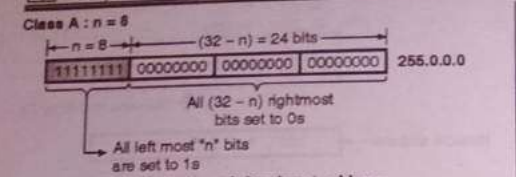
Definition of default mask :

A **network mask** or **default mask** in classful addressing is defined as a 32-bit number obtained by setting all the "n" leftmost bits to 1s and all the (32 – n) rightmost bits to 0.

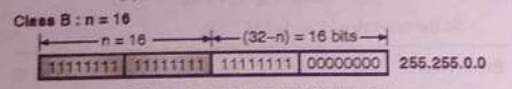
7.16.8 Default Masks for Different Classes :

- We know that the value of n is different for different classes. Therefore their default masks also will be different.
- The default masks for class A, B and C addresses are as shown in Fig. 7.16.8.

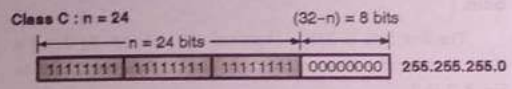
Scanned by CamScanner



(a) Default mask for class A address



(b) Default mask for class B address



(c) Default mask for class C address

(G-2009) Fig. 7.16.8

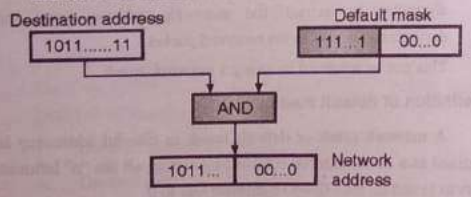
- Table 7.16.2 enlists the default masks of the three classes of IPv4 addresses.

Table 7.16.2 : Default masks

Address class	Default mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

7.16.9 Finding Network Address using Default Mask :

- The router uses the AND operation for extracting the network address from the destination address of the received packet.
- The router ANDs the destination address with the default mask to extract the network address as shown in Fig. 7.16.9.
- It is possible to use the default mask to find the number of addresses and the last address in the block.



(G-2010) **Fig. 7.16.9 : Finding a network address using the default mask**

7.16.10 Three Level Addressing : Subnetting :

MU : Dec. 06, May 08, Dec. 09, Dec. 11, May 12, May 14, Dec. 14, May 15, May 16, May 17

University Questions

Q. 1 Explain sub-netting and masking with suitable examples. **(Dec.06, 10 Marks)**

Q. 2 Explain subnetting and supernetting. **(May 08, 10 Marks)**

Q. 3 What are subnets ? Where are they used ? Explain with a detailed example. **(Dec. 09, 10 Marks)**

Q. 4 Explain subnetting and give example of subnetting of class C network. **(Dec. 11, 10 Marks)**

Q. 5 Explain need of subnet mask, with example of subnetting class C input address. **(May 12, 10 Marks)**

Q. 6 What is IP addressing ? How it is classified ? How is subnet addressing performed ? **(May 14, 10 Marks)**

Q. 7 What is IP address ? Why it is required ? What is subnet mask ? Explain subnetting and supernetting with examples. **(Dec. 14, 10 Marks)**

Q. 8 Explain the different classes of IP addresses and need of subnetting with the help of example. **(May 15, 10 Marks)**

Q. 9 Explain : Subnet mask **(May 16, 3 Marks)**

Q. 10 Explain IP address and subnet mask. **(May 17, 5 Marks)**

- As discussed earlier, the originally designed IP addresses were with two level addressing with **net id** and **host id.**
- The two level addressing is based on the principle that in order to reach a host on the Internet, we have to reach the network first and then the host.
- But very soon it became evident that the two level addressing would not be sufficient for the following two reasons :
  1. First it was needed to divide a large network of an organization (to which a block in class A or B is allotted) into many smaller **subnets** (subnetworks) for improved management and security.
  2. Second reason is more important. The blocks in class A and B were almost depleted and the blocks in class C were smaller than the needs of most organization. Therefore the organizations had to divide their allotted class A or B block into smaller subnetworks and share them.

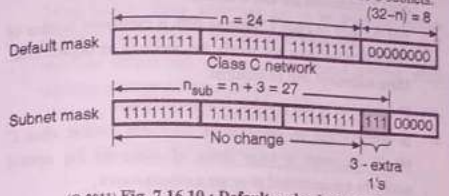
Definition of subnetting :

- We can define the **subnetting** as the principle of splitting a block of addresses into smaller blocks of addresses.
- In the process of **subnetting** we divide a big network into smaller subnetworks or **subnets.**
- Each such subnet has its own **subnet address.**

Subnet mask :

- The **network mask** or **default** mask that we discussed earlier is used when the given network is **not** to be divided into smaller subnetworks i.e. when **subnetting** is **not** to be done.
- But when the given network is to be divided into smaller subnets i.e. when subnetting is to be done, we need to create a **subnet mask** for each subnet.

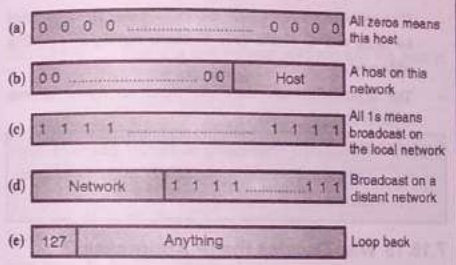
- Fig. 7.16.10 shows the format of a subnet mask. Each subnet has its own **net id** and **host id.**
- If we want to divide a network into 8 subnets then the corresponding subnet mask will have three extra 1's because $2^3 = 8$, as compared to the default mask, as shown in Fig. 7.16.10.
- In Fig. 7.16.10, we have shown the default mask and subnet mask when a class C network is to be divided into 8 subnets.



(G-2011) **Fig. 7.16.10 : Default and subnet masks**

7.16.11 Special IP Addresses :

- Fig. 7.16.11 shows some special IP addresses.



(G-540) **Fig. 7.16.11 : Special IP addresses**

- All zeros means this host or this network and all 1s means broadcast address to all hosts on the indicated network.
- The IP address 0.0.0.0 is used by the hosts when they are being booted but not used afterward.
- The IP addresses with 0 as the network number refer to their own network without knowing its number as shown in Fig. 7.16.11(b).
- The address having all ones is used for broadcasting on the local network such as a LAN as shown in Fig. 7.16.11(c).
- Refer Fig. 7.16.11(d). This is an address with proper network number and all 1s in the host field. This address allow machines to send broadcast packets to distant LANs anywhere in the Internet.
- If the address is "127. Anything" as shown in Fig. 7.16.11(e) then it is a reserved address **loopback testing.** This feature is also used for debugging network software.

7.16.12 Limitations of IPv4 :

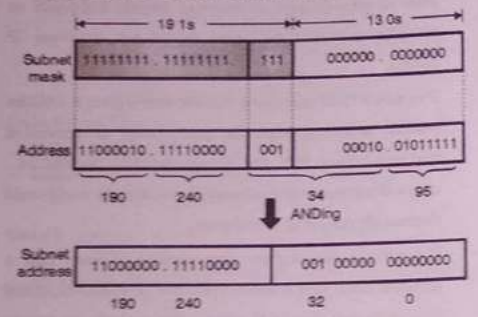
- The most obvious limitation of IPv4 is its address field. IP relies on network layer addresses to identify end-points on networks, and each networked device has a unique IP address.
- IPv4 uses a 32-bit addressing scheme, which gives it 4 billion possible addresses. With the proliferation of networked 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 $(2 \wedge 16 - 2)$, 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 $(2 \wedge 21)$, the number of available class C networks will quickly exhaust. Because of the above two reasons, a lot of IP addresses are wasted and also the available IP address space is rapidly reduced.
- Other identified limitations of the IPv4 protocol are: Complex host and router configuration, non-hierarchical addressing, difficulty in re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of Service), mobility and multi-homing, multicasting etc.
- To overcome these problems the internet protocol version 6 (IPv6) which is also known as internet protocol, next generation (IPng) was proposed.
- In IPv6 the internet protocol was extensively modified for accommodating the unforeseen growth of the internet.
- The format and length of the IP addresses has been changed and the packet format also is changed.

Ex. 7.16.4 : 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. 7.16.4.



(G-544) **Fig. P. 7.16.4**

Thus the subnet address is 190.240.32.0

7.16.13 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.

7.16.14 Supernetting : MU : May 08, Dec. 14

University Questions

Q. 1 Explain subnetting and supernetting. **(May 08, 10 Marks)**

Q. 2 What is IP address ? Why it is required ? What is subnet mask ? Explain subnetting and supernetting with examples. **(Dec. 14, 10 Marks)**

- The class A and class B addresses are almost depleted. But class C addresses are still available.
- But the size of class C address with a maximum number of 256 addresses does not satisfy the needs of an organization. More addresses will be required.
- The solution to this problem is **supernetting.**
- In supernetting an organization combines several class C blocks to create a large range of addresses i.e. several networks are combined to create a 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.

7.16.15 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.

7.16.16 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 7.16.3. These addresses are to be used for private networks and are called **unregistered addresses.**
- We can choose any of these unregistered address while building our own private network.

Table 7.16.3 : IP addresses for private networks

Class	Network address
A	10.0.0.0 through 10.255.255.255
B	172.16.0.0 through 172.31.255.255
C	192.168.0.0 through 192.168.255.255

7.16.17 Solved Examples :

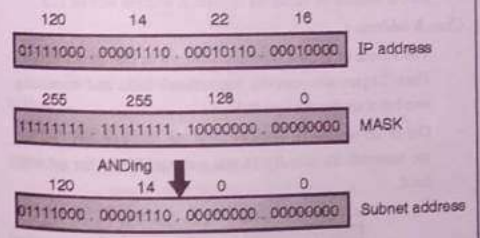
Ex. 7.16.5 : Find the sub-network address and the host id for the following :

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 :



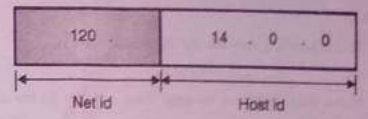
(G-553) **Fig. P. 7.16.5(a)**

So the subnet address is 120.14.0.0.

Similarly we can find the other subnet addresses.

Step 2 : Host id :

- Examine the first byte of the subnet address. It is 120 which is between 0 and 127. Hence this is a class A network.
- So only the first byte corresponds to the net id and the remaining three bytes correspond to the host id as shown in Fig. P. 7.16.5(b).



(G-554) **Fig. P. 7.16.5(b)**

So the host id is 14.0.0.

- Similarly we can find the other host id.

Ex. 7.16.6 : The IP address of a host on class C network is 198.123.46.237. Four networks are allowed for this network. What is subnet mask ? **May 12, 10 Marks**

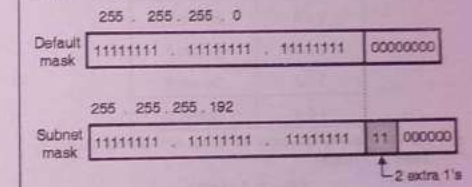
Soln. :

The default mask for a class C network is,

255.255.255.0

In order to have four networks, we must have two extra 1s.

Hence the default mask and subnet mask are shown in Fig. P. 7.16.6.



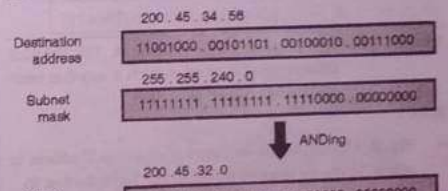
(G-555) **Fig. P. 7.16.6**

Thus the required subnet mask is 255.255.255.192.

Ex. 7.16.7 : 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. 7.16.7.



(G-556) **Fig. P. 7.16.7**

Thus the required subnet address is 200.45.32.0.

Scanned by CamScanner

Ex. 7.16.8 : A company is granted a site address 201.70.64.0. The company needs six subnets. Design the subnets.

Soln. :

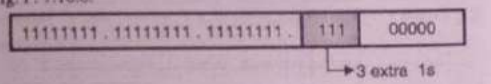
- This is a class C network. So the default mask is,

255.255.255.0

- As we need 6 subnets, we need three extra 1s. So the subnet mask is,

255.255.255.200

In the binary form the subnet mask is as shown in Fig. P. 7.16.8.



(G-557) **Fig. P. 7.16.8**

- In order to have six subnets, we can have 6 different combinations of the 3-extra 1s as shown in Table P. 7.16.8(a).

Table P. 7.16.8(a)

Combination	Subnet number
000	Subnet 1
001	Subnet 2
010	Subnet 3
011	Subnet 4
100	Subnet 5
101	Subnet 6

- So the various addresses of 6 subnets are as shown in Table P. 7.16.8(b).

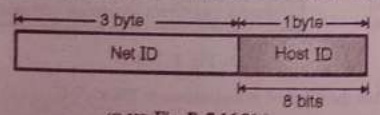
Table P. 7.16.8(b)

Subnet number	Addresses
1	201.70.64.0 to 201.70.64.31
2	201.70.64.32 to 201.70.64.63
3	201.70.64.64 to 201.70.64.95
4	201.70.64.96 to 201.70.64.127
5	201.70.64.128 to 201.70.64.159
6	201.70.64.160 to 201.70.64.191

Ex. 7.16.9 : For a given class C network 195.188.65.0 design equal subnets in such a way that each subnet has atleast 60 nodes.

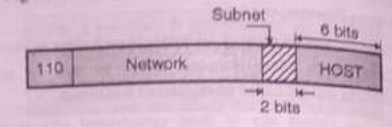
Soln. :

- Fig. P. 7.16.9(a) shows the structure of a class C address in which 3-bytes are reserved for net ID and 1-byte for host ID.



(G-558) **Fig. P. 7.16.9(a)**

- We are expected to design equal subnets such that each subnet has atleast 60 nodes (i.e. 60 users).
- In order to identify at least 60 users we need 6-bits in the host ID.
- The remaining 2-bits are assigned for subnetting as shown in Fig. P. 7.16.9(b).



(G-559) **Fig. P. 7.16.9(b)**

- This shows that there will be four equal subnets each one having at least 60 nodes.

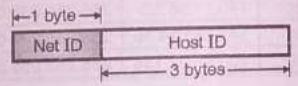
Ex. 7.16.10 : Show by calculations how many network each IP address class can have with one example ? **Dec. 06, 4 Marks**

Soln. :

Number of networks in different IP address :

Class A address :

- The format of class A address is shown in Fig. P. 7.16.10(a). Here one byte defines the network ID and three bytes define the host ID.

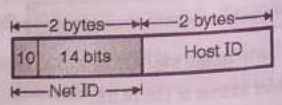


(G-560) **Fig. P. 7.16.10(a) : Class A address**

- 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. 7.16.10(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.



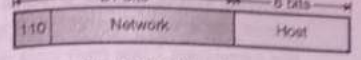
(G-561) **Fig. P. 7.16.10(b) : Class B address**

- 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. 7.16.10(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.



(G-562) **Fig. P. 7.16.10(c) : Class C address**

- So the number of networks in class C addresses is 2, 097, 152.

Ex. 7.16.11 : 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 :

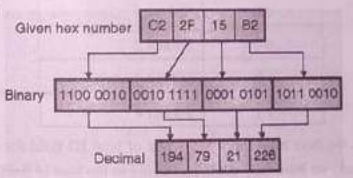
There are 2-bytes (16-bits) in the host field. So the number of hosts in class B address will be 65536 i.e. 2^{16} per network.

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. 7.16.12 : Convert the IP address whose hexadecimal representation is C22F15B2 to dotted decimal notation.

Soln. :



(G-563) **Fig. P. 7.16.12**

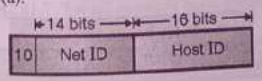
∴ The IP address in the dotted decimal notation is as follows :

194.79.21.226

Ex. 7.16.13 : A class B network on internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts per subnet ?

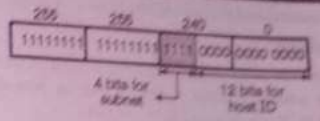
Soln. :

The structure of class B address is as shown in Fig. P. 7.16.13(a).



(G-564) **Fig. P. 7.16.13(a) : Class B address**

The given subnet mask is 255.255.2400. So it is as shown in Fig. P. 7.16.13(b).



(G-565) **Fig. P. 7.16.13(b) : Subnet mask**

Thus there are 4 extra 1s as shown in Fig. P. 7.16.13(b). So there will be 16 subnets and each subnet can have $2^{12} = 4096$ hosts.

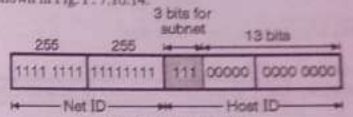
Ex. 7.16.14 : Perform the subnetting of the following IP address 160.111. X.X

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. 7.16.14.



(G-566) **Fig. P. 7.16.14**

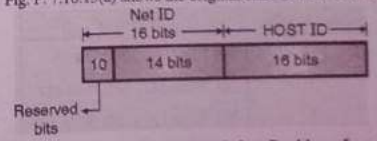
- The 3-bits reserved for subnetting will have 8 combinations from 000 to 111 out of which any six combinations can be used for 6 subnets.
- Let us decide that the combinations 000 to 001 are not to be used. Then the subnet masks for the 6 possible subnets will have the following addresses.

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. 7.16.15 : 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. 7.16.15(a) shows the original class B address format :



(G-567) **Fig. P. 7.16.15(a) : Original class B address format**

- The first two MSB bits of Net ID part are reserved. Hence, the number of bits actually available for network ID is 14.

Scanned by CamScanner

- Hence the number of class B networks = 2^{14} = 16382.

Modification :

Now with 20 bits instead of 16 being available for the Net ID part the actually available number of bits for Network part becomes 18. This is shown in Fig. P. 7.16.15(b).

∴ Number of class B networks = 2^{18} = 2, 61, 888

← Net ID →		← HOST ID →
10	18 bits	12 bits

(G-568) **Fig. P. 7.16.15(b) : Modified class B address format**

The range of IP addresses in the decimal dotted form would be 128.0.0.0 to 191.255.255.255.

Ex. 7.16.16 : 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. 7.16.16(a).

	255	255	255	0
Default mask	11111111 ·	11111111 ·	11111111 ·	00000000

(G-571) **Fig. P. 7.16.16(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. 7.16.16(b).

		← host id →
Subnet mask	11111111 · 11111111 · 11111111	11 000000

→ Two extra bits

(G-572) **Fig. P. 7.16.16(b)**

In order to have four subnets, we can have four different combinations of the two extra bits as shown in Table P. 7.16.16(a).

Table P. 7.16.16(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. 7.16.16(b).

Table P. 7.16.16(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. 7.16.17 : Consider any class – C network with default subnet mask. How many actual hosts can be connected in that network ? Divide that network into 4 equal subnets. What is the new subnet mask ? How many hosts can be connected in each subnet ?

Soln. :

- For a class C network, the default mask is

255.255.255.0

- For a class C network we can connect 2^8 = 256 total hosts.
- As we need 4 subnets, we need two extra 1s. So the subnet mask is

255.255.255.192

- In the binary from the subnet mask is as shown in Fig. P. 7.16.17.

255	255	255	192
11111111 ·	11111111 ·	11111111 ·	11 000000

2 Extra 1's

(G-574) **Fig. P. 7.16.17**

- In order to have four subnets we can have the 4 combinations of the two extra 1s as shown in Table P. 7.16.17.

Table P. 7.16.17

Combination	Subnet number
0 0	Subnet 1
0 1	Subnet 2
1 0	Subnet 3
1 1	Subnet 4

- As we have used the 2 MSB bits of host ID field for subnet mask, we have only 6 bits remaining in the host id field.

∴ No. of hosts/subnet = 2^6 = 64.

Ex. 7.16.18 : Consider any class - C network with default subnet mask. Design the subnet in such a way that each has 62 nodes. Write the range of IP addresses for all subnets.

Soln. : Refer Ex. 7.16.17.

- But we want only 62 nodes on each subnet. So 2 nodes on each subnet will be inactive.
- Let the class C address be 201.70.64.0. Then the addresses of the four subnets are as shown in Table P. 7.16.18.

Table P. 7.16.18

Subnet number	Addresses
1	201.70.64.0 to 201.70.64.61
2	201.70.64.64 to 201.70.64.125

Subnet number	Addresses
3	201.70.64.128 to 201.70.64.189
4	201.70.64.192 to 201.70.64.253

Ex. 7.16.19 : For a given C class network 210.50.60.0, how will you divide it into 4 equal subnets ? What will be the new subnet mask ? Give the network and broadcast address of each subnetwork.

Soln. :

Given : IP address : 210.50.60.0 (class C)

Step 1 : Subnet mask :

This is class C network. So default mask is given by 255.255.255.0

255 ·	255 ·	255 .	192
11111111 .	11111111 .	11111111 .	11 000000

2 extra 1's

(G-1483) **Fig. P. 7.16.19(a) : Subnet mask**

The new subnet mask is 255.255.255.192 ...Ans.

Step 2 : Find network address :

	210 .	50 .	60 .	0
IP address :	11010010 ·	00110010 ·	00111100 ·	00000000
	255 .	255 .	255 .	192
Subnet mask :	11111111 ·	11111111 ·	11111111 ·	11000000

↓ ANDing

Network address :	11010010 ·	00110010 ·	00111100 ·	00000000
	210 .	50 .	60 .	0

(G-1484) **Fig. P. 7.16.19(b)**

Network address is 210.50.60.0 ...Ans.

Step 3 : Find broadcast address :

To find broadcast address, take inverted subnet mask and perform XOR with network address.

Network address :	11010010 ·	00110010 ·	00111100 ·	00000000
Inverted subnet mask :	00000000 ·	00000000 ·	00000000 ·	00111111

↓ XORing

Broadcast address :	11010010 ·	00110010 ·	00111100 ·	00111111
	210 .	50 .	60 .	63

(G-1485) **Fig P. 7.16.19(c)**

The broadcast address is 210.50.60.63 ...Ans.

Ex. 7.16.20 : For a given class B network 144.155.0.0 with default subnet mask, how can divide it into 8 subnets ? Write the :

1. Range of each subnet.
2. Network IP for 7th subnet.
3. Broadcast IP for the 7th subnet.
4. Subnet mask in subnets.

Soln. :

Given class B network : 144.155.0.0. The default subnet mask is 255.255.0.0. In order to have 8 subnets we need to use 3 extra bits from the host id field as shown in Fig. P. 7.16.20.

		3 bits for subnet	13 bits	
255	255			
1111 1111	11111111	111	00000	0000 0000
← Net ID →		← Host ID →		

(G-566) **Fig. P. 7.16.20**

- The new subnet mask is 255.255.224.0.
- The 3-bits reserved for subnetting will have 8 combinations from 000 to 111 which can be used for 8 subnets.
- The subnet masks for the 8 possible subnets will have the following subnet masks :

Subnet	Mask
1	255.255.0.0
2	255.255.32.0
3	255.255.64.0
4	255.255.96.0
5	255.255.128.0
6	255.255.160.0
7	255.255.192.0
8	255.255.224.0

- The following is the range of subnets :

Subnet	Subnet range
1	144.155.0.0 to 144.155.31.255
2	144.155.32.0 to 144.155.63.255
3	144.155.64.0 to 144.155.95.255
4	144.155.96.0 to 144.155.127.255
5	144.155.128.0 to 144.155.159.255
6	144.155.160.0 to 144.155.191.255
7	144.155.192.0 to 144.155.223.255
8	144.155.224.0 to 144.155.255.255

- Network IP for 7th subnet is 144.155.192.0.

Scanned by CamScanner

- Broadcast IP for 7th subnet is 144.155.223.255.
- Subnet mask is 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. 7.16.21 : 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 handles can be almost 254 (28-2) host.

Ex. 7.16.22 : 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. 7.16.23 : 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 subnet address. **May 09, 4 Marks**

Soln. :

The subnet address can be obtained by ANDing the destination address with the mask as follows :

190	240	34	95	
10111110 .	11110000 .	00100010 .	01011111	IP address
255	255	224	0	
11111111 .	11111111 .	11100000 .	00000000	MASK
ANDing				
190	240	32	0	
10111110 .	11110000 .	00100000 .	00000000	Subnet address

(G-1905) **Fig. P. 7.16.23**

As shown in Fig. P. 7.16.23, the subnet address is 190.240.32.0.

Ex. 7.16.24 : The size of option field of an IP datagram is 20 bytes. What is the value of HLEN ? What is the value in binary ? **May 15, 5 Marks**

Soln. :

The size of the IP datagram header is decided rather indicated by the contents of the 4-bit HLEN (header length) field. For the IP datagram header to be of its minimum length i.e. 20 bytes the content of HLEN should be 5.

$$\text{HLEN} = 5 = (0101)_2$$

We have to multiply the contents of HLEN field by 4 to obtain the length of IP datagram header.

Ex. 7.16.25 : An IPv4, packet has arrived with the first 8 bits as shown : 01000010. The receiver discards ? Why ? **May 16, 4 Marks**

Soln. :

The first 8 bits are as follows :

0 1 0 0 0 0 1 0

Type IPv4 → HELEN $2 \times 4 = 8$

$\therefore$ Header length is 8 bytes

(G-1900)

The receiver discards this packet due to invalid length of the IPv4 header (8 bytes) which actually should be between 20 and 60 bytes.

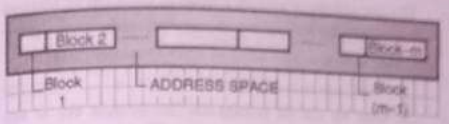
7.17 Classless Addressing in IPv4 :

- Eventhough the number of actual devices connected to Internet is much less than 4 billion, the address depletion has taken place due to flaws in the classful addressing scheme.
- We have run out of class A and B addresses. To overcome these problems, the super netting and subnetting has been tried as discussed earlier.
- But subnetting and supernetting also could not solve the problem of address depletion in IPv4.
- Due to increased number of Internet users, it was evident that a larger address space would be required as a long term solution to this problem. For this the length of the IP address should be increased which means the IP packet itself must be changed.
- A long term solution is to switch to IPv6. But a short term solution which uses the same address space has been devised for IPv4. It is known as **classless addressing.**
- In the classless addressing, there are no classes but the address generation take place in blocks.
- The classless addressing was announced by the Internet authorities in 1996 in which blocks of variable length which do not belong to any class are used.

7.17.1 Variable Length Blocks :

- Address block is defined as the range of addresses.
- In the classless addressing, when an entity wants to get connected to the internet, a block (range) of addresses is granted to it.
- The size of this block i.e. number of addresses depends on the size of the entity as well as its nature.

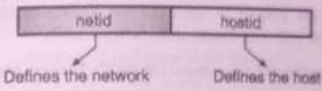
- That means for a small entity such as a household only one or two addresses will be given whereas for a larger entity like an organization, thousands of addresses can be allotted.
- Fig. 7.17.1 shows how the address space is divided into non overlapping address blocks.



(G-1904) **Fig. 7.17.1 : Variable length blocks in classless addressing**

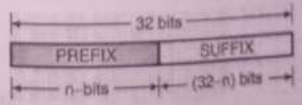
Two level addressing :

- We have discussed the two level addressing for classfull addressing which divided an address into two parts namely : net id and host id.



(G-1905) **Fig. 7.17.2 : Two layer addressing in classfull addressing**

- The **net id** and **host id** define the network and host respectively. It is possible to use the same idea in the classless addressing as well.
- A block of addresses granted to an organization is divided into two parts called as the **prefix** and the **suffix.**
- The role of prefix is same as that of the net id whereas as the role of suffix is same as that of the host id. Thus in a block granted to an organization, all the addresses will have the **same prefix** but each address will have a different **suffix.**
- Thus the prefix defines the network (organization to which the address block has been granted) while the suffix defines individual hosts on the network.
- The concept of two level addressing in classless addressing using the prefix and suffix is as shown in Fig. 7.17.1.
- 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-1906) **Fig. 7.17.3 : Two level addressing using prefix and suffix for classless addressing**

Ex. 7.17.1 : Find out the values of prefix and suffix lengths in classless addressing if all the available addresses in IPv4 is to be considered as one single block.

Soln. :

- The total addresses in IPv4 is $2^{32} = 4,294,967,296$.
- We have to consider this as one block hence the prefix length n = 0. Whereas all the hosts will have their individual addresses. So all the 32 bits will be allotted to the suffix length.

Ex. 7.17.2 : For the same data of the previous example find out the values of prefix and suffix lengths if all the available IPv4 addresses are divided into 4,294,967,296 blocks with each block having only one host.

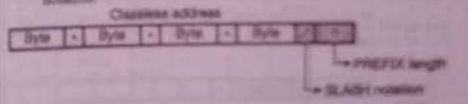
Soln. :

- Here the prefix length for each block is n = 32, and the suffix length would be (32-n) = 0. The address of the single host in each block will be same as its block address itself.

Note : The two previous examples show that the prefix number n and the number of addresses in a block are inversely proportional to each other. With increase in the value of n, the number of addresses in a block will decrease.

7.17.2 The Slash Notation (CIDR Notation) :

- If an address (classful or classless) is given to us and we want to extract information from it, then the net id in classful addressing or the prefix in classless addressing are extremely important and useful to us.
- However it is not easy to identify the prefix bits in a given classless address. It is easy to identify the net id from the given classful address.
- For a given classless address it is not possible to find the prefix length because the given address can belong to a block with any prefix length.
- Therefore, in classless addressing it is essential to include the prefix length to each address if the block of the given address is to be found.
- Hence the prefix length "n" is added to the classless address separated by a **slash** and the notation is known as the **slash notation.**
- Fig. 7.17.4 demonstrates a classless address with slash notation.



(G-1907) **Fig. 7.17.4 : Slash notation**

- The slash notation is also called as Classless Interdomain Routing or CIDR notation.

7.17.3 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.

Scanned by CamScanner

- **A network mask** in classless addressing is a 32 bit number. With its "n" left most bits (corresponding to the prefix) all set to 1s and the remaining (32-n) bits corresponding to the suffix all set to 0s.

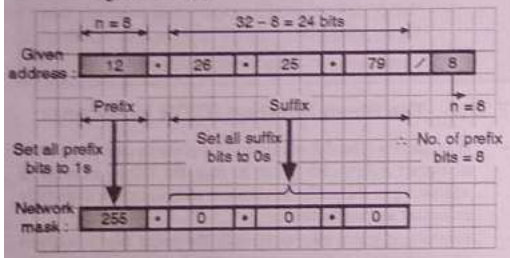
Ex. 7.17.3 : For the following addresses identify the number of prefix bits and write down the network mask :

1. 12.26.25.79 / 8
2. 130.12.230.156 / 16

Soln. :

1. Classless CIDR address : 12.26.25.79 / 8

- As per the slash notation we have n = 8 i.e. number of prefix bits is 8.
- Therefore the number of suffix bits = 32 – 8 = 24.
- In order to obtain the network mask the prefix bits all set to 1s and the suffix bits all set to zero as shown in Fig. P. 7.17.3(a).

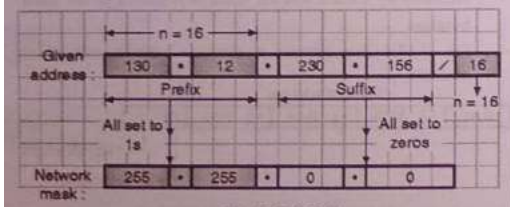


(G-1808) **Fig. P. 7.17.3(a)**

Thus the network mask = 255.0.0.0

2. Classless CIDR Address : 130.12.230.156 / 16

- As per the slash notation, n = 16 i.e. number of prefix bits is 16.
- Number of suffix bits = 32 – 16 = 16
- In order to obtain the network mask, set all the prefix bits to 1s and set all the suffix bits to 0s as shown in Fig. P. 7.17.3(b).



(G-1809) **Fig. P. 7.17.3(b)**

Thus the network mask = 255.255.0.0

7.17.4 Extracting the Block Information :

- We can extract all the required information from the given classless address in the CIDR notation. The information that we can obtain is as follows :
  1. The first address (network address)
  2. The number of addresses.
  3. The last address.
- We can obtain the number of addresses in a block as follows :

  Number of addresses in a block $N = 2^{(32-n)}$ ...(7.17.1)

  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.

  First address = (Any address) AND (Network mask) ...(7.17.2)
- 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.

∴ Last address = First address + Number of addresses in the block ...(7.17.3)

- It is also possible to obtain the last address by ORing the address with complement of the network mask.

∴ Last address = (Any address) OR [NOT (Network Mask)] ...(7.17.4)

- One more way of obtaining the last address of the block is to keep all the "n" left most bits (prefix bits) as it is and set all the (32-n) bits (suffix bits) to 1s.

Ex. 7.17.4 : 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. 7.17.4(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. 7.17.4(a).

∴ From Fig. P. 7.17.4(a) we get the first address in the block as :

First address = $\boxed{64.32.16.0}$ ...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. 7.17.4(b).

∴ From Fig. P. 7.17.4(b) we get the last address in the block as follows :

Last address = $\boxed{64.32.16.31}$

Ex. 7.17.5 : 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.

∴ n = 24 bits

∴ Prefix bits = 24, suffix bits = 32 – 24 = 8

Step 2 : Number of addresses in the block (N) :

$N = 2^{(32-n)} = 2^8 = 256$ ...Ans.

Step 3 : Find the first address :

- Refer Fig. P. 7.17.5(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

∴ Network mask = 255.255.255.0

- For ANDing write the given address and network mask in their dotted decimal notations as shown.

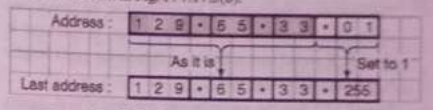
(G-1812) **Fig. P. 7.17.5(a) : First address in the block**

∴ From Fig. P. 7.17.5(a) we get the first address in the block as :

First address = $\boxed{129.65.33.0}$ ...Ans.

Step 4 : Find the last address :

To obtain the last address in the block, we have to keep the left most 24 bits in the given address as it is and set the remaining 8 bits to 1s as shown in Fig. P. 7.17.5(b).



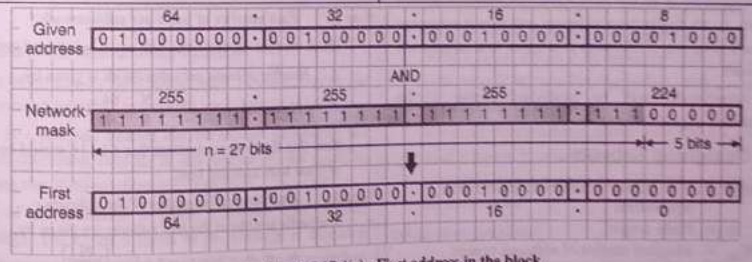
(G-1813) **Fig. P. 7.17.5(b) : Last address in the block**

- From Fig. P. 7.17.5(b) we get, the last address in the block is as follows :

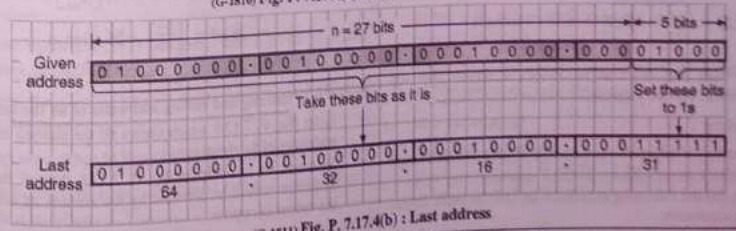
Last address = $\boxed{129.65.33.255}$ ...Ans.

7.17.5 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.



(G-1810) **Fig. P. 7.17.4(a) : First address in the block**



(G-1811) **Fig. P. 7.17.4(b) : Last address**

Scanned by CamScanner

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.

7.17.6 Relation to Classful Addressing :

- The classful addressing may be imagined as the special case of classless addressing such that the blocks of addresses in class A, B and C type addresses will have the prefix lengths $n_A = 8$, $n_B = 16$ and $n_C = 24$.
- Table 7.17.1 lists the prefix lengths for class A to F classful addresses and using this information we can change a block in classful addressing to a block in classless addressing.

Table 7.17.1 : Prefix lengths for classful addressing

Class	Prefix length	Class	Prefix length
A	/8	D	/4
B	/16	E	/4
C	/24		

7.17.7 Subnetting :

- The concept of subnetting in classless addressing domain is similar to that discussed for the classful addressing.
- The subnetting is used for creating a three level hierarchy in the classless addressing domain.
- An organization or an ISP have a block of addresses granted to them. It can divide these addresses into several subgroups and each subgroup of addresses is assigned to a **subnetwork or subnet.**
- The subnetworks may be subdivided further if the organization want it that way.

7.17.8 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 subnetwork.

$$n_{sub} = n + \log_2\left[\frac{N}{N_{sub}}\right] \quad \text{...(7.17.5)}$$

- 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.

7.17.9 Finding Information about Each Network :

- After designing the subnetworks, we can find the information about the subnets such as starting and last addresses, we can use the same procedure that was used to find the information about each network in the Internet.

Ex. 7.17.6 : 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,

$$N_1 = N_2 = N_3 = N_4 = \frac{N}{4} = \frac{64}{4} = 16 \quad \text{...Ans}$$

- Note that the first requirement that 64 / 16 should be a power of 2 has been satisfied here.

Step 3 : Find the prefix lengths of the subnets :

- The prefix lengths of the four subnets are given by,

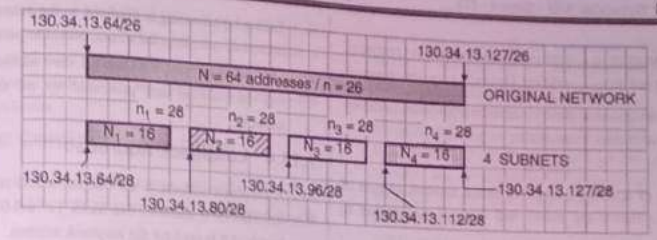
$$n_1 = n_2 = n_3 = n_4 = n + \log_2\left[\frac{N}{N_{sub}}\right]$$

$$= 26 + \log_2\left[\frac{64}{16}\right] = 26 + \log_2 4$$

$$\therefore n_1 = n_2 = n_3 = n_4 = 28 \quad \text{...Ans}$$

Step 4 : Starting and ending addresses of all the subnets :

- Refer Fig. P. 7.17.6 which shows all the starting and ending addresses of the 4-subnets.
- It should be noted from Fig. P. 7.17.6 that all the starting addresses should be divisible by the number of addresses in the subnet i.e. by 16.



(G-1814) Fig. P. 7.17.6

7.17.10 Address Aggregation :

Address aggregation is considered to be one of the advantages of CIDR architecture. As we know, ICANN assigns a large block of addresses to an ISP which is divided into smaller subnets and assigned to the customers by the ISPs. Thus many blocks of addresses are aggregated in one block and assigned to one ISP.

Ex. 7.17.7 : A router has following CIDR entries in its routing table :

Address/Mask	Next Hop
135.46.56.0/22	Interface 0
135.46.60.0/22	Interface 1
192.53.40.0/23	Router 1
Default	Router 2

For each of the following IP addresses, what does the router do if a packet with that address arrives ?

1. 135.46.63.10 2. 192.53.56.7

MU : Dec. 10, 10 Marks

SPPU : Dec. 11, 8 Marks, May 16, 5 Marks

Soln. :

CIDR – Classless Inter Domain Routing :

- IP is being heavily used for decades. However, due to the exponential growth of internet, IP is running out of addresses.
- This is a potential disaster and the internet community has begun discussion over it. In this section we are going to discuss one of the solutions to this problem.
- One of the solutions is CIDR (Classless Inter Domain Routing). The CIDR is based on the principle of allocating the remaining IP addresses in variable-sized blocks regardless of the class.
- If a site needs say 2000 addresses, then a block of 2048 addresses on the 2048 byte boundary is given to it.
- However the classless routing makes forwarding of packets more complicated.

Forwarding algorithm in the old classful system :

- The steps followed in the old classful system for forwarding packets is as follows :
  1. As soon as a packet arrives at a router, a copy of the IP address was shifted right by 28 bits to obtain a 4 bit class number.
  2. A 16-way branch then sorts packets into class A, B, C and D (if supported) with eight of the cases for class A, four of the cases for class B, two of the cases for class C and one each for D and E.
  3. The code for each class then masked off the 8–, 16–, or 24– bit network number and right aligned it in a 32 bit word.
  4. The network number was then searched in the A, B or C table.
  5. As soon as the entry was found, the outgoing line was decided and the packet was forwarded upon it.

Forwarding with CIDR :

- The simple forwarding algorithm explain earlier does not work with CIDR.
- Instead now each router table entry is extended by giving if a 32 bit mask. So now there is a single routing table for all networks (no different tables for class A, B, C, etc.) which consists of an array of triples. Each triple consists of an **IP address, subnet mask** and **outgoing line.**
- When a packet arrives at the input, the router first extracts its destination IP address. Then the routing table is scanned entry by entry to look for a match.
- It is possible that different entries with different subnet mask lengths match. In such a case the longest mask is used. For example if there is a match for a/20 mask and a/24 mask then /24 entry is used.

Solution of problem :

- Convert the IP address to bits and then AND it with the subnet mask of the interface whose address is closest to that of the IP addresses.
- The result of the ANDing will give you the network address and the interface to send the packet to.

1. **IP = 135.46.63.10 :**

The interface whose address is closest to this IP is interface 1. This interface uses a 22 bit mask. So AND the given IP address with a 22 bit mask as follows :

Scanned by CamScanner

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)

This result of ANDing does not match with the network addresses of interface 0 or 1. Hence the packet will forwarded to the default i.e. Router 2.

7.18 Special Addresses :

In the classful addressing, some addresses were reserved for special purpose. Similarly in the classless addressing as well some addresses are reserved.

7.18.1 Special Blocks :

Some address blocks have been reserved for special purpose.

7.18.2 All Zeros Address :

- The block 0.0.0.0 / 32 contains only one address. It is called as the all zero address and has a prefix length of n = 32.
- This address has been reserved for communication when a host has to send an IPv4 packet but it does not know its own address.
- In such situations, the host sends an IPv4 packet to a DHCP server using this all zero address as the source address and a limited broadcast address (all one address) as the destination address, so as to find its own address.

7.18.3 All one Address-Limited Broadcast Address :

- The block 255.255.255.255 / 32 contains only one address. It is called as an all one address and has a prefix length of n = 32.
- This all one address has been reserved for limited broadcast address i.e. if a host wants to send message to all the hosts simultaneously then the sending host can use all one address as a destination address inside the IPv4 packet.
- Such a broadcasting is confined to the network only because routers do not allow the all one packet to pass through them.
- The datagram sent with the all zero address as destination will be received and processed by all the hosts on the network.

7.18.4 Loopback Address :

- A loopback address is the address which is used to test the software on a machine. The block 127.0.0.0 / 8 with a prefix length of 8 is used for the loopback address.
- On using this address, a packet does not leave the machine at all but it returns to the protocol software. It can be used for testing the IPv4 software.

7.18.5 Private Addresses :

- The address blocks that are not recognized globally all assigned for private use are known as private addresses.
- These addresses are neither connected to nor isolated from the Network Address Translation (NAT) techniques.
- Table 7.18.1 depict such address blocks.

Table 7.18.1 : Private addresses

Block	Number of addresses	Block	Number of addresses
10.0.0.0 / 8	16,777,216	192.168.0.0 / 16	65,536
172.16.0.0 / 12	1,047,584	169.254.0.0 / 16	65,536

7.18.6 Multicast Addresses :

The block 224.0.0.0 / 4 with a prefix length of n = 4 has been reserved for the multicast IP communication.

7.18.7 Special Addresses in Each Block :

- The usage of some address in each block for special addresses has been recommended. But it has not been made mandatory. These addresses are not assigned to any host.
- One important point to be remembered is that a very small block of addresses should not be used as special addresses.

7.18.8 Network Address :

- The network address is defined as the first address (with the suffix set all to 0s) in a block. It is used for defining the network itself. It does not define any host in the network.
- With the same principle, the first address in a subnetwork is called as the subnetwork address.

7.18.9 Direct Broadcast Address :

- We can use the last address in a block or subblock (with the suffix part set to all 1s), as a **direct broadcast address** for that block or subblock.

- A router generally uses this address for sending a packet to all the hosts connected to a specific network. This address is used as the destination address in the IPv4 packet and all the hosts will accept and process the datagram which has this destination address.

7.19 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 diskless or the computer is with a disc but it is being booted for the first time.
- If a computer is diskless, 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.

7.19.1 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 9.9.9.

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.

7.19.2 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.
- 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.

Scanned by CamScanner

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.

7.19.3 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.

7.19.4 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.
   - 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.

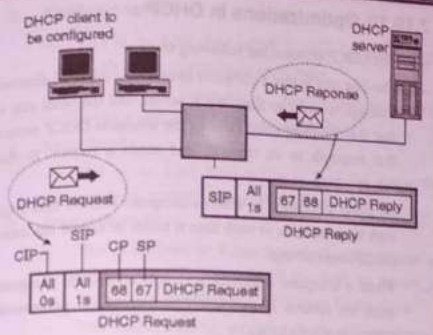
7.19.5 DHCP Operation :

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. 7.19.1.

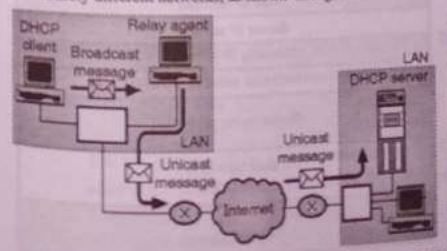


(G-1789) **Fig. 7.19.1 : Operation of DHCP when client and server are on the same network**

- 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.

7.19.6 DHCP Operation on Different Networks :

- In this situation the DHCP client and server are on two entirely different networks, as shown in Fig. 7.19.2.



(G-1790) **Fig. 7.19.2 : 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. 7.19.2. 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.

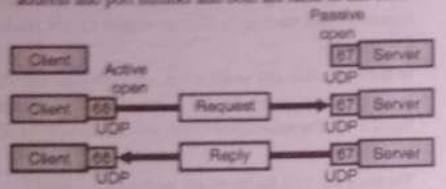
Note : In Fig. 7.19.2 only the message between the relay agent and client is it broadcast type. All the other messages are unicast types.

7.19.7 UDP Ports :

- The interaction between a client and DHCP server has been shown in Fig. 7.19.3. 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.
- 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.**

Scanned by CamScanner

- 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-1996) **Fig. 7.19.3 : 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.

7.19.8 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.

7.19.9 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.

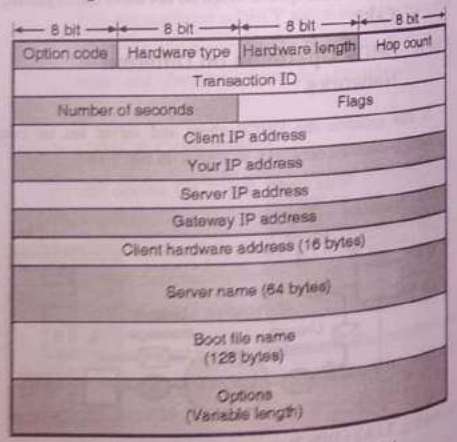
7.19.10 Optimizations in DHCP :

- 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 the 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.

7.19.11 Packet Format :

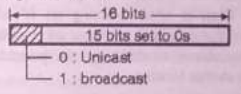
- The format of a DHCP packet has been shown in Fig. 7.19.4. Let us describe each field in the DHCP packet.

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.



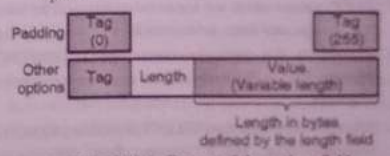
(G-1995) **Fig. 7.19.4 : DHCP packet format**

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. 7.19.5. Out of these 16 bits, only the leftmost bit is used and the remaining 15 bits are set to 0s.



(G-1996) **Fig. 7.19.5 : 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. 7.19.6 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.
    - 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. 7.19.6 : Format of the options field**

7.20 Configuration of DHCP :

DHCP is capable of providing static and dynamic address allocation.

Scanned by CamScanner

7.20.1 Static Address Allocation :

In the static address allocation capacity, the database of DHCP server would bind the physical addresses to the IP addresses.

7.20.2 Dynamic Address Allocation :

- DHCP has another database in which a pool of available IP addresses is present. This database is used by DHCP when a client requests for a temporary IP address. In response to such a request the DHCP allots an unused IP address from the pool to the requesting client for a negotiable period of time.
- The dynamic IP address allocation is required when a host moves from one network to the other or when the host is frequently getting connected or disconnected to the same network.
- The dynamic IP address is assigned temporary for a short duration. The DHCP server issues a **lease** for a specific period of time.
- The client has to renew the lease as soon as it expires or stop using the assigned IP address.

7.20.3 Transition States :

- In the dynamic address allocation mode, the DHCP client acts as a state machine. Depending on the received message it will make transitions from one state to the other.
- The transition diagram with important states has been shown in Fig. 7.20.1.

7.20.3.1 Address Acquisition States :

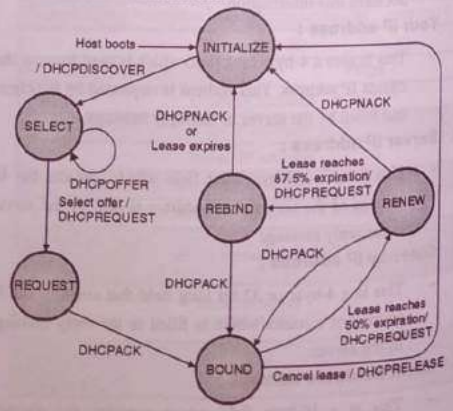
- When the DHCP is being used to obtain an IP address, a client is in one of six states. The state transition diagram in Fig. 7.20.1 shows events and messages that force a client to change state.
- When a client first boots, it enters the INITIALIZE state. In order to get an IP address, the client first contacts all DHCP servers in the local net.
- To do so, the client broadcasts a DHCPDISCOVER message and enters into the SELECT state.
- Because DHCP is an extension of BOOTP, the client sends the DHCPDISCOVER message in a UDP datagram with the destination port set to the BOOTP port (i.e., port 67). All DHCP servers which are connected to the local net receive the message, and those servers that have been programmed to respond to that particular client send a DHCPOFFER message. Thus, a client may receive zero response or multiple responses.
- When the client is in state SELECT, it collects DHCPOFFER responses from DHCP servers. Each offer contains configuration information for the client alongwith an IP address that the server is offering to lease to the client.

The client must choose one of the responses (e.g., the first to arrive), and negotiate with the server for a lease. To do so, the client sends a DHCP REQUEST message to the server, and enters the REQUEST state.

- To acknowledge the request has been received and to start the lease, the server responds by sending a DHCPACK. When of the acknowledgement is received the client to moves to the BOUND state, where the client proceeds to use the address.
- To use DHCP, a host becomes a client by broadcasting a message to all servers on the local network. The host then collects lease offers from servers, selects one of the offers, and acknowledges the acceptance with the server.

7.20.3.2 Early Lease Termination :

- We think of the BOUND state as the normal state of operation; a client generally remains in the BOUND state when it is using the IP address allotted to it.
- If a client has secondary storage (e.g., a local disk), the client can store the IP address on it and request for the same address when it restarts again.
- In some cases, however, a client in the BOUND state may discover that it does not need an IP address anymore. For example, suppose a user attaches a portable computer to a network, uses DHCP to acquire an IP address and then uses TCP/IP to read electronic mail.
- The user may not know how long reading mail will require, or the portable computer may allow the server to choose a lease period.
- In any case, the minimum lease period specified by DHCP is of one hour. If after obtaining an IP address, the user discovers that no e-mail messages are waiting to be read, the user may choose to shutdown the portable computer and move to another location.
- If the clients does not needs a lease anymore, DHCP allows a client to terminate a lease and does not for the lease to expire.
- Early termination is especially important if only a small number of IP addresses are available at the server as compared to the number of computers that attach to the network. If each client terminates its lease as soon as the IP address is no longer needed, the server will be able to assign the address to another client.



(G-582) **Fig. 7.20.1 : State diagram of DHCP**

- To terminate a lease early, a client sends a DHCPRELEASE message to the server. once an address is released the client is not allowed to use that address further.
- Thus, after transmitting the release message, the client must not send any other datagrams that use the address.
- As seen in the state transition diagram of Fig. 7.20.1 a host that sends a DHCPRELEASE leaves the BOUND state, and must start at the INITIALIZE a host state again before it can use IP.

7.20.3.3 Lease Renewal States :

- We have seen that when a client acquires an address, it moves to the BOUND state. After entering the BOUND state, the client sets three timers that control lease renewal, rebinding and expiration.
- A DHCP server can specify precise values for the timers when it allocates an address to the client; if the server does not specify timer values, the client uses the default values.
- The default value for the first timer is one-half of the total lease time. When the first timer expires, the client must attempt to renew its lease. To request a renewal, the client sends a DHCPREQUEST message to the server from which it had obtained the lease.
- The client then moves to the RENEW state and waits for a response The DHCPREQUEST contains the IP address which the client is currently using, and asks the server to extend the lease time to use the same address.
- Similar to the initial lease negotiation, a client can request its preferred period for the extension, but the actual lease time allotment is controlled entirely by the server.
- A server can respond to a client's renewal request in one of two ways: it can instruct the client to stop using the address or it can allow the client to continued use.
- If it allows the client to continue then, the server sends a DHCPACK, which causes the client to return to the BOUND state and continue using the same IP address.
- The DHCPACK can also contain new values for the client's timers. If a server does not allow the client to continue using the same address then, the server sends a DHCPNACK (negative acknowledgement), which causes the client to stop using the address immediately and return to the INITIALIZE state.
- After sending a DHCPREQUEST message that requests an extension on its lease, a client remains in state RENEW and waits for a response from the server.
- If it does not receive any response then the server that granted the lease is either down or unreachable. To handle this situation, DHCP relies on a second timer, which was set when the client entered the BOUND state.
- The second timer expires after 87.5% of the lease period, and makes the client to move from state RENEW to state REBIND. When making the transition, the client assumes the old DHCP server is not available anymore and starts broadcasting a DHCPREQUEST message to any server on the local net.
- Any server configured to provide service to the client can respond positively (i.e. to extend the lease), or negatively (i.e. to deny further use of the same IP address). If it receives a positive response, the client returns to the BOUND state, and resets the two timers.
- If it receives a negative response, the client must move to the INITIALIZE state, must immediately stop using the IP address, and must acquire a new IP address before it can continue to use IP.
- After moving to the REBIND state, a client should have asked the original server and all servers on the local net for a lease extension. sometimes a client does not receive any response from any server before its third timer, expires, the lease expires.
- The client must stop using the IP address, must move back to the INITIALIZE state, and begin acquiring a new address.

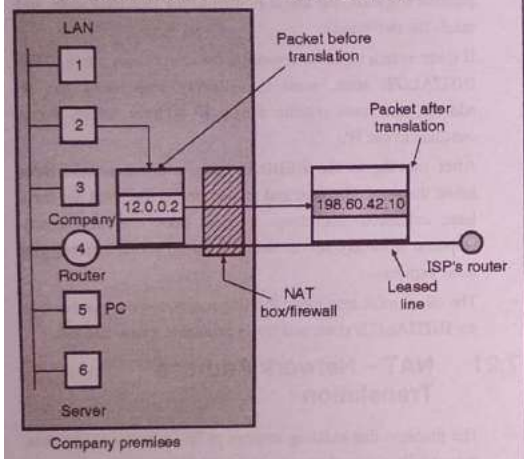
7.21 NAT – Network Address Translation :

- 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.
- 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

Scanned by CamScanner

- Generally most companies choose the addresses from the first range.
- Refer Fig. 7.21.1 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. 7.21.1 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. 7.21.1 : NAT**

7.22 Delivery and Forwarding of IP Packets :

- In this section and some of the following sections we are going to discuss the delivery and forwarding of IP packets.
- **Delivery** of IP packets can be defined as the way in which a packet is handled by the underlying networks under the supervision and control by the network layer.
- Delivery of IP packets is of two types :
  1. Direct delivery.
  2. Indirect delivery.
- **Forwarding** is defined as the manner in which an IP packet is delivered to the next station.
- Two important forwarding techniques are : first is forwarding based on the destination address of the packet and the second one is on the basis of the label attached to the packet.

7.22.1 Delivery :

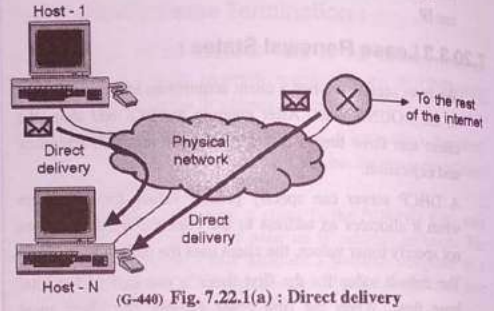
- The network layer supervises how the packets are being handled by the underlying physical networks. This handling is known as the delivery of packets.

The two different methods of delivery are :

1. Direct delivery 2. Indirect delivery.

1. Direct delivery :

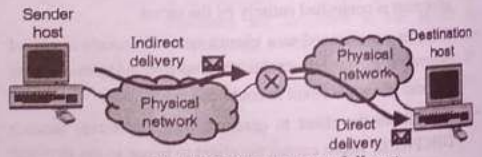
- In the direct delivery the destination host and the one who delivers the packet are in the same physical network as shown in Fig. 7.22.1(a).
- The sender can extract the network address of the destination using the mask. It then compares this address with the addresses of the networks to which it is connected. If these two addresses are identical then the delivery is direct.



(G-440) **Fig. 7.22.1(a) : Direct delivery**

2. Indirect delivery :

- In the indirect delivery of packets, the sender host and the destination host are not the part of the same physical network as shown in Fig. 7.22.1(b).
- In such a situation, the packets travel from one router to the other and are finally delivered to the destination host.
- The indirect delivery involves one direct and zero or more indirect deliveries. The last delivery is always a direct one.



(G-441) **Fig. 7.22.1(b) : Indirect delivery**

7.22.2 Forwarding :

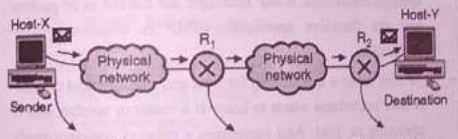
- Forwarding is defined as the process of placing the packet in its route towards its destination. Forwarding is possible only if the host or a router have a routing table of their own.
- A sender host or a router will refer to this routing table when it receives a packet and from the table they will find the root to the final destination.
- But this simple solution has practically become impossible today in the internetwork environment due to a large number of entries required to be made in a routing table.

1. Forwarding techniques :

- Many techniques have been invented and tested in order to make the size of the routing tables manageable. Some of them are as follows :
  1. Next hop method versus Route method.
  2. Network specific method versus Host specific method.
  3. Default method.

2. Next hop method versus route method :

- The Route method is the most basic method in which the information about the complete route is stored in the routing tables of hosts and routers as shown in Fig. 7.22.2(a). This makes the routing tables extremely large and difficult to manage.
- In order to reduce the size of routing tables, the next hop method is used in which the routing table contains only the address of the next hop (upto the next router) instead of information about the complete route. This is as shown in Fig. 7.22.2(a).



Routing tables at Host-X — Based on route

Destination	Route
Host Y	R_1, R_2, Host Y

Routing tables at router R_1 — Based on route

Destination	Route
Host Y	R_2, Host Y

Routing tables at router R_2 — 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

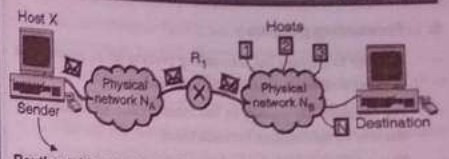
Based on next hop

Destination	Route
Host Y	–

(G-442) **Fig. 7.22.2(a) : Route method versus Next Hop method**

3. Network specific method versus host specific method :

- In the host specific method, the routing table of a host or router will specify each destination host connected to the same physical network. This increases the number of entries in a routing table and makes it large.
- But in the network specific method, we have only one entry corresponding to the destination network N_B only as shown in Fig. 7.22.2(b).



Routing tables for host - X

Host specific method

Destination	Next hop
Host - 1	R_1
Host - 2	R_2
⋮	⋮
Host - N	R_1

Network specific method

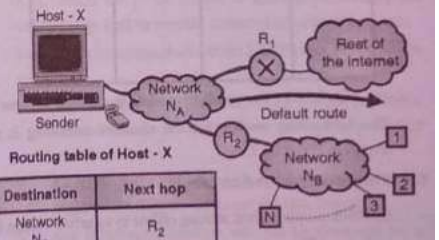
Destination	Next hop
Network N_B	R_1

(G-443) **Fig. 7.22.2(b) : Host specific method versus network specific method**

- That means we consider all hosts connected to the same network N_B as one single entry. This will reduce the routing table and simplify the searching process considerably.

4. Default method :

- This is one more method of simplifying the routing tables. Refer Fig. 7.22.2(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

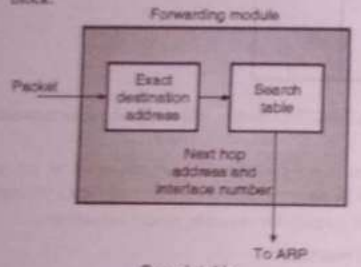
(G-444) **Fig. 7.22.2(c) : Default method**

- Router R_2 routes the packets to the hosts connected to network N_B. However router R_1 is used for the rest of the Internet.
- Hence in the routing table instead of listing all networks in the entire Internet, host X will have only one entry called as the default entry (normally defined as network address 0.0.0.0).

Scanned by CamScanner

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.



Search table

Mask	Network address	Next hop address	Interface

(G-445) **Fig. 7.22.3 : Forwarding module in classless address**

- The forwarding module for the classless addressing is as shown in Fig. 7.22.3.

6. Forwarding based on label :

- In 1980s people started making efforts to somehow change IP to behave like a connection oriented protocol, in which the routing would be replaced by switching.
- As discussed earlier, the difference between connectionless network and a connection oriented network is as follows :
- In the connectionless networks, the datagram approach is followed in which a packet is forwarded by the routers on the basis of destination address in the header of the packet.

However in the connection oriented networks the virtual circuit approach is followed in which a switch forwards a packet on the basis of the **lable** attached to the packet.

The other difference between the two types of networks is that routing involves **searching** of the routing table whereas switching involves **accessing** of the table.

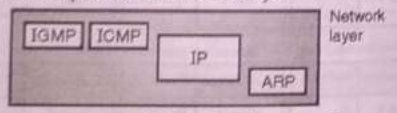
7.23 ICMPv4 (Internet Control Message Protocol) : MU : May 10, May 14, Dec. 16

University Questions

Q. 1 Explain main features of following protocol : ICMP. **(May 10, 2 Marks)**

Q. 2 Write short notes on : Internet Control protocols. **(May 14, Dec. 16, 5 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 slongwith 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. 7.23.1 shows the position of ICMP with respect to the IP and other protocols in the network layer.



(G-2102) **Fig. 7.23.1 : Position of ICMP**

- There are two versions of ICMP protocol namely ICMPv4 and ICMPv6. In the following sections, we are going to discuss ICMPv4.

7.23.1 ICMP Encapsulation :

MU : May 10, May 14, Dec. 16

University Questions

Q. 1 Explain main features of following protocol : ICMP **(May 10, 10 Marks)**

Q. 2 Write short notes on : Internet Control protocols. **(May 14, Dec. 16, 5 Marks)**

- 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. 7.23.2.

(G-2103) **Fig. 7.23.2 : 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

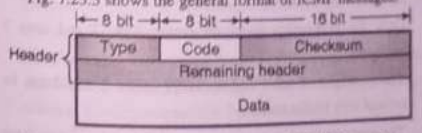
- When the destination receives the echo request message, it responds by sending an ICMP echo reply message. If a reply is not returned within a set time, ping resends the echo request several more times. If no reply arrives, ping indicates that the destination is unreachable.
- Another utility that uses ICMP is trace route, which provides a list of all the routers along the path to a specified destination.

7.23.2 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.

7.23.3 Message Format :

- Fig. 7.23.3 shows the general format of ICMP messages.



(G-2105) **Fig. 7.23.3 : General format of ICMP messages**

- As shown in Fig. 7.23.3, the header of an ICMP message is 8-byte long and the data section is of a variable size.
- 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.

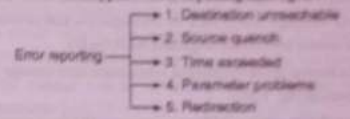
2. **Code :**

   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.

7.24 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. 7.24.1 shows different types of error reporting messages.

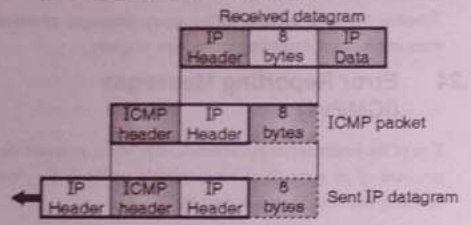


(G-2106) **Fig. 7.24.1 : Error reporting messages**

- 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.

Scanned by CamScanner

- 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. 7.24.2.



(G-2106) **Fig. 7.24.2 : Data field contents for the error message**

- Now let us discuss the ICMP error messages one by one.

7.24.1 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. 7.24.3.

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. 7.24.3 : 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.
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.

7.24.2 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. 7.24.4 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. 7.24.4 : 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.

7.24.3 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.
- The format of the time exceeded message is as shown in Fig. 7.24.5.

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. 7.24.5 : 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.

7.24.4 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. 7.24.6. 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. 7.24.6.

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. 7.24.6 : Format of parameter problem error message**

7.24.5 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.

Scanned by CamScanner

- 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. 7.24.7 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. 7.24.7 : Format of the redirection message**

- As shown in Fig. 7.24.7, 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.

7.25 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. 7.25.1.

Query
- 1. Echo request and reply
- 2. Time stamp request and reply
- 3. Address mask request and reply
- 4. Router solicitation and advertisement
- 5. Information request and reply messages

(G-2112) **Fig. 7.25.1 : 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.

7.25.1 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. 7.25.2.

	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. 7.25.2 : Echo request and echo reply messages**

- In Fig. 7.25.2, the protocol does not formally define the identifier and sequence number fields. Therefore the sender can use them in an arbitrary manner.

7.25.2 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. 7.25.3 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. 7.25.3 : Format of timestamp request and timestamp reply messages**

- As shown in Fig. 7.25.3, 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.

  Round 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.

7.25.3 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.

Scanned by CamScanner

- These messages are not being used today because their duties are done by the DHCP.

7.25.4 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.

7.26 Routing :

- Routing is a very important issue in the network layer. A router creates its routing table so as to help forwarding a datagram in the connectionless services. It also helps in creating a virtual circuit in the connection oriented service.
- In the following sections we are going to discuss about the types of routing and different routing algorithms such as distance vector routing, link state routing and hierarchical routing.

7.26.1 Types of Routing :

Routing can be broadly classified into three types :

1. Unicast routing.
2. Broadcast routing
3. Multicast routing.

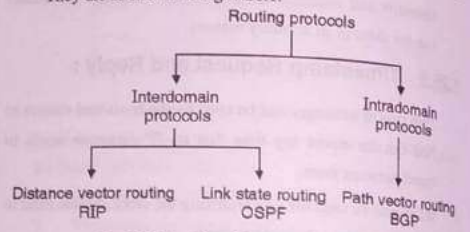
We can also classify the routing into two types as follows :

1. Intradomain routing.
2. Interdomain routing.

7.26.2 Intra and Interdomain Routing :

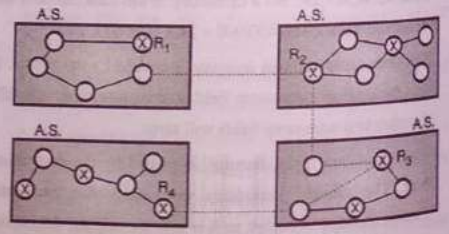
Today the size of the Internet is so big that one routing protocol cannot handle the task of updating the routing tables of all the routers.

- 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. 7.26.1.
- 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. 7.26.1.



(G-1291) **Fig. 7.26.1 : 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.

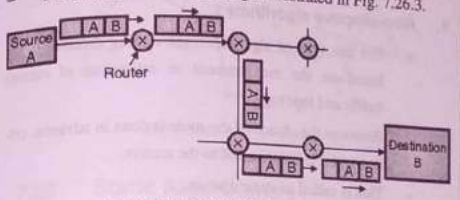


(G-1292) **Fig. 7.26.2 : Autonomous systems**

7.26.3 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. 7.26.3.



(G-448) **Fig. 7.26.3 : 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 :

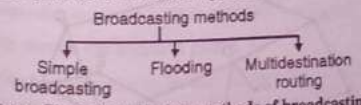
The routing that takes place inside an AS is called as interior routing.

Exterior routing :

The routing that takes place among various autonomous systems is called as exterior routing.

7.26.4 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. 7.26.4 : 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.

7.26.5 Multicast Routing : MU : May 12

University Questions

Q. 1 Write short notes on : Multicasting. **(May 12, 5 Marks)**

- 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.

7.27 Routing Algorithms :

- One of the important functions of the network layer is to route the packets from the source machine to the destination machine.

Scanned by CamScanner

- 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.

.27.1 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.

27.2 Types of Routing Algorithms :

MU : Dec. 04, May 05, May 07, May 08, May 09, Dec. 09, May 11, Dec. 12, May 13, May 14, May 16

University Questions

.1 What are the different types of Routing Algorithms ? Explain any one in detail. **(Dec. 04, May 05, May 07, 10 Marks)**

.2 Explain different types of routing algorithm. **(May 08, 10 Marks)**

.3 What are different types of routing ? **(May 09, 2 Marks)**

.4 What are different types of routing ? **(Dec. 09, 5 Marks)**

5 What are different types of routing ? With an example explain distance vector routing. **(May 11, 10 Marks)**

6 What is routing in network ? Write the difference between adaptive and non-adaptive routing. Write any one algorithm of adaptive routing. **(Dec. 12, 10 Marks)**

7 Differentiate between static routing and dynamic routing. Also explain working of RIP, problems and solution of RIP in detail. **(May 13, 10 Marks)**

Explain different categories of routing algorithms. **(May 14, 10 Marks)**

What are the different types of routing algorithms ? Explain shortest path routing algorithm in detail ? **(May 16, 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.
- 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.

7.27.3 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. 7.27.1. 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. 7.27.1, the distance metric is the number of hops. In Fig. 7.27.1(b) a sink tree for router B has been shown. The paths from B to every router with minimum number of hops.

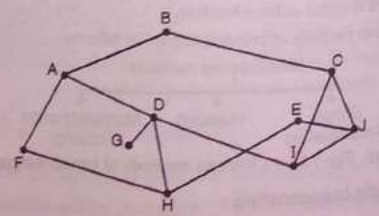
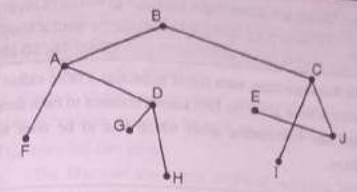


Fig. 7.27.1 (a) : A subnet



(b) A sink tree for router B

(G-450) **Fig. 7.27.1**

7.28 Static Algorithms :

MU : Dec. 05, May 13, May 14

University Questions

Q. 1 What is static routing ? What are the advantages of dynamic routing ? Explain shortest path routing in detail. **(Dec. 05, 5 Marks)**

Q. 2 Differentiate between static routing and dynamic routing. Also explain working of RIP, problems and solution of RIP in detail. **(May 13, 10 Marks)**

Q. 3 Explain different categories of routing algorithms. **(May 14, 10 Marks)**

The examples of static algorithms are :

1. Shortest path routing. 2. Flooding.
3. Flow based routing.

7.28.1 Shortest Path Routing :

MU : Dec. 04, May 05, Dec. 05, May 15, May 16, May 17

University Questions

Q. 1 What are the different types of routing algorithms ? Explain any one in detail. **(Dec. 04, May 05, 10 Marks)**

Q. 2 What is static routing ? What are advantages of dynamic routing ? **(Dec. 05, 5 Marks)**

Q. 3 What is routing in network ? Explain shortest path routing protocol. **(May 15, 10 Marks)**

Q. 4 What are the different types of routing algorithms ? **(May 16, 10 Marks)**

Q. 5 Explain shortest path routing. **(May 17, 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.**

7.29 Dynamic Routing Algorithms :

MU : Dec. 05, Dec. 12, May 13, May 14

University Questions

Q. 1 What is static routing ? What are the advantages of dynamic routing ? Explain shortest path routing in detail ? **(Dec. 05, 5 Marks)**

Q. 2 What is routing in network ? Write the difference between adaptive and non-adaptive routing. Write any one algorithm of adaptive routing. **(Dec. 12, 10 Marks)**

Q. 3 Differentiate between static routing and dynamic routing. Also explain working of RIP, problems and solution of RIP in detail. **(May 13, 10 Marks)**

Q. 4 Explain different categories of routing algorithms. **(May 14, 10 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.

Scanned by CamScanner

7.29.1 Distance Vector Routing Algorithm :

MU : May 04, Dec. 14, Dec. 16

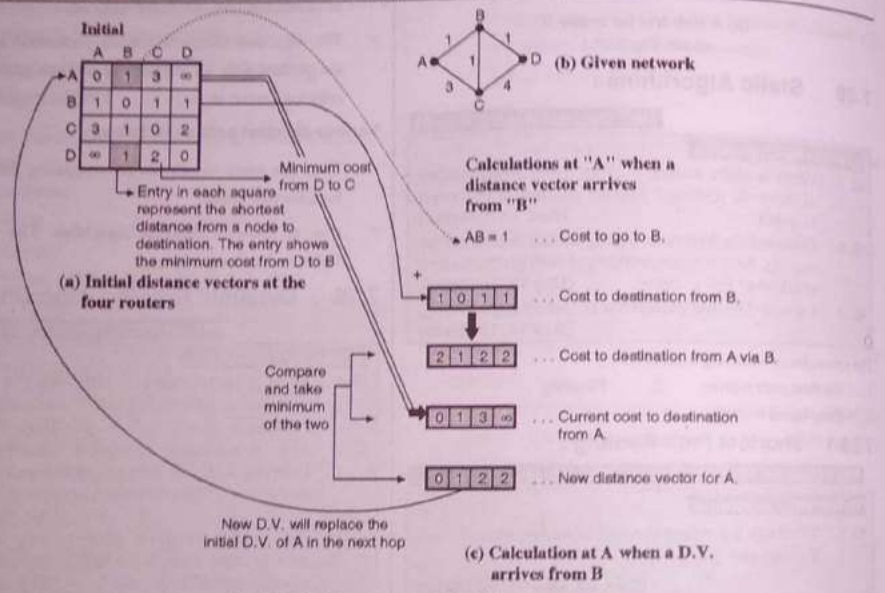
University Questions

Q. 1 What does routing mean and how does it works ? **(May 04, 5 Marks)**

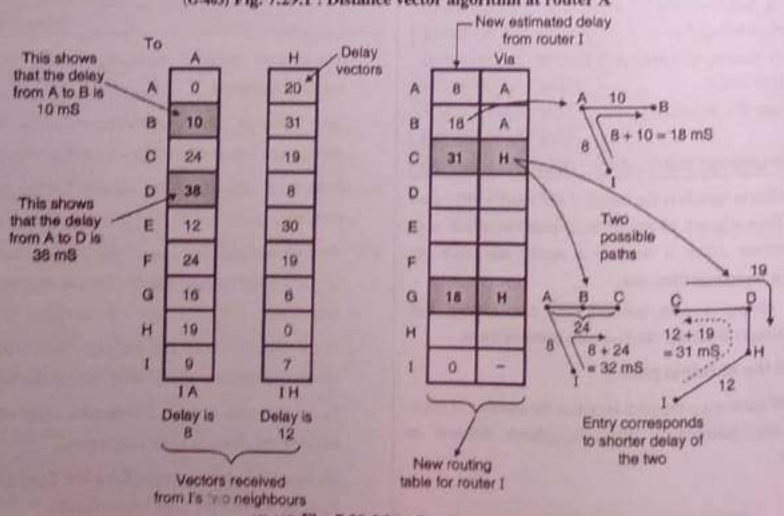
Q. 2 What are the three main functions performed by network layer ? What is routing ? Explain distance vector counting. **(Dec. 14, 10 Marks)**

Q. 3 What are three main function of network layer ? What is routing ? Explain distance vector routing. **(Dec. 16, 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.



(G-463) **Fig. 7.29.1 : Distance vector algorithm at router A**



(G-465) **Fig. 7.29.2(b) : Routing tables**

- 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 :

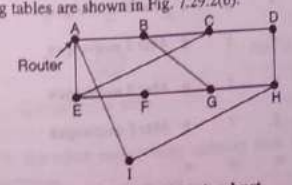
- In distance vector routing, we assume that each router knows the identity of every other router in the network, but the shortest part to each router is not known.
- A **distance vector** is defined as the list of <destination, cost> tuples, one tuple per destination. Each router maintains a distance 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. 7.29.1.
- Fig. 7.29.1 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. 7.29.1(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.

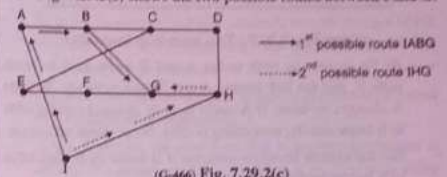
Routing procedure in distance vector routing :

- The example of a subnet is shown in Fig. 7.29.2(a) and the routing tables are shown in Fig. 7.29.2(b).



(G-464) **Fig. 7.29.2(a) : A subnet**

- The entries in router tables of Fig. 7.29.2(b) are the delay vectors. For example consider the shaded boxes of Fig. 7.29.2(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. 7.29.2(c) shows the two possible routes between I and G.



(G-466) **Fig. 7.29.2(c)**

- I knows that the reach G via A, the delay required is :

  I to A Delay = 8 mS
  A to G Delay = 16 mS } ∴ I to G Delay = 8 + 16 = 24 msec

- Whereas the delay between I and G via H (route IHG) is :

  I to H Delay = 12 mS
  H to G Delay = 6 mS } ∴ I to G Delay = 12 + 6 = 18 msec

- The best of these values is 18 msec corresponding to the path IHG. Hence it makes an entry in its routing table (I's table) that the delay to G is 18 msec and that the route to use it is via H.
- The new routing table for router I is shown in Fig. 7.29.2(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.

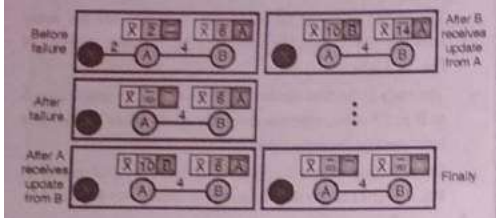
Looping in distance vector routing protocol :

- 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. 7.29.3. Note that the routing tables are shown partially for discussion.

Scanned by CamScanner



(G-1499) **Fig. 7.29.3 : Two node loop instability**

- At the beginning both nodes A and B know how to reach node X. But the link joining A and X fails suddenly. So node A changes its table. If A could send its changed routing table to B immediately, everything is okay. No problem will occur.
- But the system becomes unstable if B sends its routing table to A before receiving A's routing table.
- This is because node A receives the updated B's routing table and assumes that B has found a new path to reach node X. So A immediately updates its routing table (which is incorrect).
- Based on this update now A sends its new update to B. Now B thinks that something has changed around A and so it updates its routing table.
- Due to this process, the cost of reaching X increases gradually and finally becomes infinite. At this moment both A and B understand that now it is impossible to reach X.
- Note that during this entire time the system is unstable. A thinks that the route to X goes via B whereas B thinks that the route is via node A.
- So if A receives a packet for X, it goes to B and then again returns back to A. Similarly if B receives a packet destined for X, it goes to A and returns back to B.
- This bouncing of packets between nodes A and B is known as the **two-node loop problem.**
- This problem can be solved by using one of the following strategies :
  1. Defining infinity
  2. Split horizon
  3. Split horizon and poison reverse.
- There is a similar problem called three node loop problem present in the system using distance vector routing.

7.29.2 Count to Infinity Problem :

MU : Dec. 04

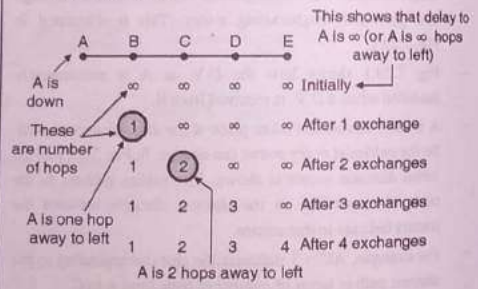
University Questions

Q. 1 Explain Count-to-infinity problem with the help of an example. It is a drawback of which algorithm. **(Dec. 04, 10 Marks)**

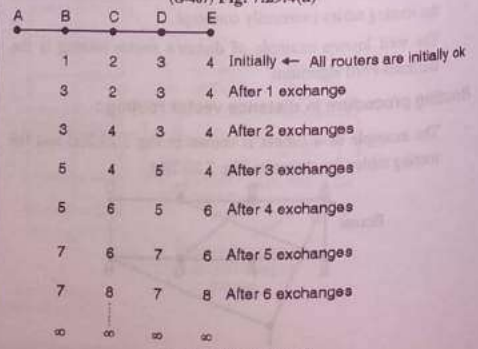
Theoretically the distance vector routing works properly but practically it has a serious problem. The problem is that we get a correct answer but we get it slowly.

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. 7.29.4 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. 7.29.4(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. 7.29.4(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.

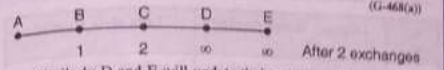


(G-467) **Fig. 7.29.4(a)**



(G-468) **Fig. 7.29.4(b)**

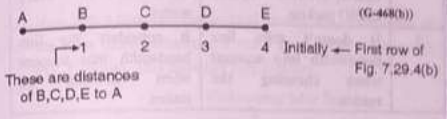
- So after the second vector exchange the entries in the third row of Fig. 7.29.4(a) are :



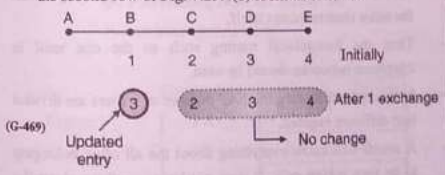
- Similarly D and E will update their routing tables after 3 and 4 exchanges respectively.
- So we conclude that the good news of A has recovered has spread at a rate of one hop per exchange.

Explanation of Fig. 7.29.4(b) :

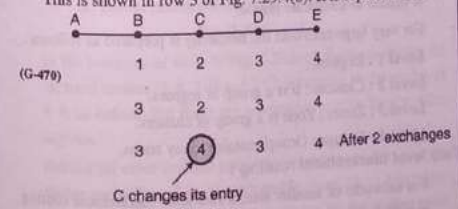
- Now refer Fig. 7.29.4(b). Here initially all routers are OK. The routers B, C, D and E have distances of 1, 2, 3 and 4 respectively to A. So the first row of Fig. 7.29.4(b) is as follows :



- 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. 7.29.4(b) looks as follows :



- 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. 7.29.4(b). It is repeated below.



- Similarly the other routers keep updating their tables after every exchange.
- It is expected that finally we should get ∞ in the router tables of B, C, D and E indicating that A is down. We do reach this state at the end in Fig. 7.29.4(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.

7.29.3 Link State Routing :

MU : Dec. 14

University Questions

Q. 1 Write short note on : Link state routing. **(Dec. 14, 5 Marks)**

- Distance vector routing was used in ARPANET upto 1979. After that it was replaced by the link state routing.
- Variants of this algorithm are now widely used.
- The link state routing is simple and each router has to perform the following five operations.

Router operations :

1. Each router should discover its neighbours and obtain their network addresses.
2. Then it should measure the delay or cost to each of these neighbours.
3. It should construct a packet containing the network addresses and the delays of all the neighbours.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

- The complete topology and all the delays are experimentally measured and this information is conveyed to each and every router.
- Then a shortest path algorithm such as Dijkshtra's algorithm can be used to find the shortest path to every other router.

Protocols :

- Link state routing is popularly used in practice.
- The OSPF protocol which is used in the Internet uses the link state algorithm.
- IS-IS i.e. Intermediate system – Intermediate system is the other protocol which uses the link state algorithm.
- IS-IS is used in Internet backbones and in some digital cellular systems such as CDPD.

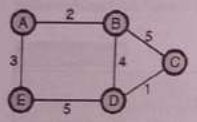
Scanned by CamScanner

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. 7.29.5(b) for the Internet shown in Fig. 7.29.5(a). The next step is creation of LSDB (which contains all the information about the Internet) at each node.



	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

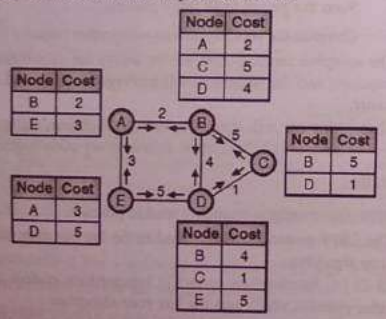
(a) Internetwork **(b) Link state database (LSDB)**

(G-2201) **Fig. 7.29.5**

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. 7.29.5(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. 7.29.5(c)**

7.29.4 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.

7.29.5 Hierarchical Routing :

- As the size of the network increases, the size of the routing tables of the routers also increases.
- As a result of large routing tables, the router memory is consumed to a great extent, more CPU time is needed to scan the tables and more bandwidth is required to send status report about the tables.
- Sometimes the network becomes so large that the size of the router table becomes excessively large and practically it becomes impossible for every router to have an entry for all the other routers except itself.
- Then the hierarchical routing such as the one used in telephone networks should be used.
- In this type of routing the total number of routers are divided into different **regions.**
- A router will know everything about the all other belonging to its own region only. It does not know anything about the internal structure of other regions. This reduces the size of the router table.
- When various networks are connected together, each network is treated as a separate region.
- For very large networks the hierarchy is prepared as follows :

  Level 1 : Regions

  Level 2 : Clusters : It is a group of regions.

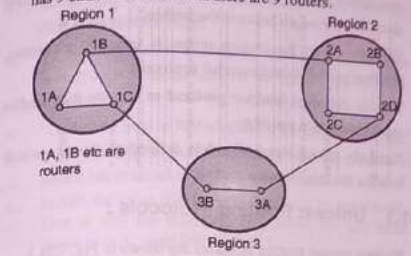
  Level 3 : Zones : Zone is a group of clusters.

  Level 4 : Groups : Group contains many zones.

Two level hierarchical routing :

- For networks of smaller size, a two level hierarchical routing is sufficient.

- Fig. 7.29.6(a) shows network containing 3 regions. Fig. 7.29.6(b) shows the full routing table of router 1A which has 9 entries because in all there are 9 routers.



(G-471) **Fig. 7.29.6(a) : A network**

- Now with a two level hierarchical routing, the routing table of the same router reduces to a much smaller size as shown in Fig. 7.29.6(c). This table has only 5 entries.

Full routing table for 1A

Destination	Line	Hops
1 A	–	–
1 B	1 B	1
1 C	1 C	1
2 A	1 B	2
2 B	1 B	3
2 C	1 B	3
2 D	1 B	4
3 A	1 C	3
3 B	1 C	2

(b) Full routing table for router 1A

Hierarchical routing table

For 1 A

	Destination	Line	Hops
Region 1	1 A	–	–
	1 B	1 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

Fig. 7.29.6

- In the hierarchical table of Fig. 7.29.6(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. 7.29.6(c). Similarly all the traffic from 1A to region 3 is routed through the line 1C-3B.
- Comparison of Figs. 7.29.6(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. 7.29.1 : 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

  $= (x-1) + (y-1) + z = x + y + z - 2$

- 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.

7.30 Unicast Routing Protocols :

- We can define the unicast communication as the communication between one sender and one receiver. In short it is a one to one communication.
- We have already discussed about how the Internet has been divided in **administrative areas** called **Autonomous Systems** which helps in handling the exchange of routing information efficiently.
- In the following sections we are going to discuss some important routing protocols.

7.30.1 Routing :

- An Internet consists of many networks connected to each other by routers. A datagram passes through different routers when it travels from the source to destination.

Scanned by CamScanner

7.30.2 Cost or Metric :

- As a router is connected to many networks it has to make a decision when it receives a packet from one of these networks, as to which network it should pass this packet to ?
- The router makes this decision on the basis of **Optimization.** That means it finds out which path is an optimum path to send the packet. But how does it define the term **optimum ?**
- One way is that a **cost** is assigned for passing through a network. This cost is also called as the **metric.**
- In connection with finding the optimum path, the network having a high cost is considered to be **bad** and to have a low cost is considered to be **good.**
- So in order to maximize the throughput the router should choose the networks (paths) having low costs.
- Similarly in order to minimize the delay, the router must choose the paths having low costs.

7.30.3 Routing Tables :

- The routing table for a host or a router consists of an entry for each destination, or a combination of destinations to route the IP packets.
- Routing tables can be of two types :
  1. Static routing tables
  2. Dynamic routing tables

1. Static routing table :

- The information in the static routing tables is entered manual. The route of a packet to each destination is entered into the table by the administrator.
- This routing table cannot update itself automatically. It has to be changed manually as and when required.
- Hence static routing table is useful only for small networks.

2. Dynamic routing table :

- The dynamic routing tables can get automatically updated by using a dynamic routing protocol such as RIP, OSPF or BGB.
- The structure of a dynamic routing table is shown in Table 7.30.1.

Table 7.30.1 : Format of dynamic routing table

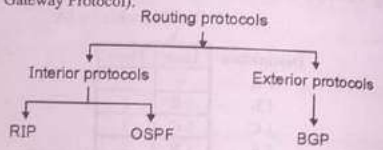
Mask	Network address	Next hop address	Interface	Flags	Reference count	Use

7.31 Routing Protocols :

- Routing protocols are designed on the basis of the demand for dynamic routing tables.
- The router in an Internet are supposed to inform each other about changes. Routing protocols combine the rules and procedures which allow the routers to exchange information about these changes between themselves.
- We can divide the routing protocols into two categories, **interior protocols** and **exterior protocols.**
- We can define an **interior protocol** as the one that handles the **intradomain routing.**
- Similarly an exterior protocol is defined as the one which handles the **interdomain** routing.

7.31.1 Unicast Routing Protocols :

- Various unicast routing protocols are shown in Fig. 7.31.1.
- The popular interior protocols are RIP (Routing Information Protocol) and OSPF (Open Shortest Path First).
- Whereas the exterior protocol used popularly is BGP (Border Gateway Protocol).



(G-497) **Fig. 7.31.1 : Unicast routing protocols**

- RIP and OSPF are used to upgrade the routing tables inside an A.S. and BGP is used for upgrading the routing tables for the routers which join multiple A.S. together.

7.32 RIP (Routing Information Protocol) : MU : May 17

University Questions

Q. 1 Write short note on : RIP (routing information protocol). **(May 17, 5 Marks)**

- RIP is used for updating the routing tables. The routing updates are exchanged between the neighbouring routers after every 30 seconds with the help of the RIP response message. These messages are also known as the RIP advertisements.
- These messages are sent by the routers or hosts. They contain a list of multiple destinations within an Autonomous System (AS).
- RIP is an interior routing protocol used inside an Autonomous System (AS). Its operation is based on distance vector routing.
- In the distance vector routing each router periodically shares its knowledge about the whole Internet with its neighbours.
- As stated earlier, RIP is a very simple intradomain or interior routing protocol which works inside an **Autonomous System (AS).**

- RIP implements the distance vector routing with the following considerations :
  1. In an A.S. it has to deal with routers and networks (links) and not the nodes.
  2. Now the destination in a routing table is a network. That is why, the network address in defined in the first column.
  3. The **metric** used in RIP is called as the **hop count** and it is very simple. It is defined as the number of links a packet has to travel to reach its destination.
  4. In RIP, the value of **infinity** is decided to be equal to 16. That is why the maximum **hop count** for any route inside an A.S. using RIP can be 15.
  5. The next node column is used to define the address of the router to which the packet is to be dispatched.

Routing table :

- A typical routing table is shown in Table 7.32.1. Every router is supposed to keep such a table with it.

Table 7.32.1 : Routing table

Destination	Hop count	Next router	Other information

- Destination column consists of the destination network address. The hop count column consists of the shortest distance to reach the destination and the next router column consists of the address of the next router to which the packet is to be forwarded.
- The other information in Table 7.32.1 may include information such as subnet mask or the time this entry was last updated.

7.32.1 RIP Updating Algorithm :

- The routing table is updated when a RIP response message is received as stated earlier.
- The updating algorithm used by RIP is as follows.

RIP updating algorithm :

1. RIP response message is received.
2. Add one hop to the hop count for each advertised destination.
3. Repeat the following steps for each advertised destination :
   - Add the advertised information to the table if the destination is not present in the routing table.
   - Replace entry in the table with the advertised one if the next hop field is same.
   - Replace entry in the routing table if advertising hop count is smaller than one in the table.
4. Return.

7.32.2 Initializing the Routing Table :

- When a new router is added to a network it initialises its routing table.
- Such a table consists of the information only about the directly attached networks and the corresponding hop counts. The next hop field which identifies the next router is empty.

7.32.3 Updating the Routing Table :

- When RIP messages are received, each routing table is updated using the RIP updating algorithm as discussed earlier.

7.32.4 RIP Operation :

- RIP work is a combination of a routing database that stores information on the fastest route from computer to computer, an update process that enables each router to tell other routers which route is the fastest from its point of view, and an update algorithm that enables each router to update its database with the fastest route communicated from neighboring routers.
- Each router on the Internet keeps a database that stores the following information for every computer in the same RIP network :
  - **IP address :** The Internet Protocol address of the computer.
  - **Gateway :** The best gateway to send a message addressed to that IP address.
  - **Distance :** The number of routers between this router and the router that can send the message directly to that IP address.
  - **Route change flag :** A flag that indicates that this information has changed used by other routers to update their own databases.
  - **Timers :** Various timers.
- At regular intervals each router sends an update message which has full information about its routing database to all the other routers that are directly connected to it. Some routers will send this message as often as every 30 seconds, so that the network will always have up-to-date information.
- RIP uses the UDP network protocol because of its efficiency and there are no problems if a message gets lost due to any reason. This is because the next update will be coming in a short time.

7.32.5 RIP Message Format :

- RIP messages can be broadly classified into two types : messages that deliver routing information and messages that request routing information.
- Both use the same format which consists of a fixed header followed by an optional list of network and distance pairs.

Scanned by CamScanner

RIP version 1

Command	Version	Reserved
Family		All zeros
Network address		
All zeros		
All zeros		
Distance		
Repeat of last 20 bytes ...		

20 bytes = Ones network

(G-1998) **Fig. 7.32.1 : RIP message format**

- The summary of the RIP packet format fields illustrated in Fig. 7.32.1, is as follows :

1. **Command :**

   Indicates whether the type of the packet i.e. a request or a response. The request asks that a router send all or part of its routing table. The response can be an unsolicited regular routing update or a reply to a request. Responses contain routing table entries. Multiple RIP packets are used to convey information from large routing tables.

2. **Version :**

   This field specifies the RIP version used. This field can signal different potentially incompatible versions.

3. **Zero :**

   This field is not actually used by RFC 1058 RIP; it was added just to provide backward compatibility with the older versions of RIP. Its name actually indicates its defaulted value: zero.

4. **Family :**

   This field is used to specify the address family used. RIP is designed to carry routing information for several different protocols. Each entry has an address-family identifier to indicate the type of address being specified. For example the value of AFI for IP is 2. Similarly different values indicate different protocols.

5. **Network address :**

- The network address field is used for defining the address of the destination network. In RIP this field is 14 bytes long, so that it can be used for any protocol.
- But the IPv4 address is only 4 byte long. Hence the remaining space in the address field is filled with zeros.

6. **Distance :**

   This field indicates the number of hops (routers) that have been traversed in the trip to the destination. This value is between 1 and 15 for a valid route, or 16 for an unreachable route.

7.33 Request and Response Messages (RIP) :

- RIP has tow types of messages namely Request and Response Messages.

7.33.1 Request Message :

- The request message is created in the following two situations :
  1. It is created by a router which has just come up.
  2. Or it is created by a router which has some time out entries.
- In a request message, information about some specific entries or all the entries is asked.
- Fig. 7.33.1(a) shows the format of the request message for one and Fig. 7.33.1(b) shows the format of request message for all.

	Com. 1	Version	Reserved
	Family		All zeros
Repeated	Network address		
	All 0s		
	All 0s		
	All 0s		

(G-2145) **(a) Format of request message (RIP) for one**

Fig. 7.33.1

	Com. 1	Version	Reserved
	Family		All zeros
Repeated	All 0s		
	All 0s		
	All 0s		
	All 0s		

(G-2146) **(b) Format of request message (RIP) for all**

Fig. 7.33.1

7.33.2 Response Message :

- Response message in RIP can be one of the following two types :
  1. Solicited response or 2. Unsolicited response.
- A **solicited response** is the one which is sent only as an answer to a request message. It carries with it the information about the destination specified in the request message.
- An **unsolicited response,** is not sent only once but it is sent periodically (every 30 seconds or so) when there is any change in the routing table. This response is also called as the update packet.

7.33.3 Timers in RIP :

- RIP uses three different timers as follows for supporting its options.
  1. The **periodic timer** to control the process of sending messages.
  2. The **expiration timer** is used for governing the validity of a route.
  3. The **garbage collection timer** is used for advertizing the failure of a route.

1. **Periodic Timer :**

- The task of the periodic timer is to control the advertizing of the update messages regularly.
- As per protocol specifications, this timer should be set to 30 sec. but practically it is set randomly between 25 and 35 sec. Each router has one periodic timer.
- This timer counts down from the set value (25 to 35 sec.) and sends an update message when its count reaches a zero. Then the timer is set once again to a random value between 25 and 35 seconds.

2. **Expiration Timer :**

- The responsibility of expiration timer is to govern the validity of a route.
- When a router gives out the update information about a route, the value of this timer is set at 180 sec or 3 minutes.
- This timer is reset, everytime a new update for that route is received, which under normal working conditions happen after every 30 sec.
- But due to some problem on the Internet, if a new update for that route is not received within 180 sec, then that route is considered expired and the hop count of that route is set to 16. This is an indication that the destination is not reachable.
- There is a separate expiration timer for each route.

3. **Garbage Collection Timer :**

- The router does not purge a particular route from its table even when the information about that route becomes invalid. Instead the router continues to advertise that route by increasing its metric value to 16 (destination is not reachable).
- At the same time, the router sets another timer called **garbage collection timer** to 120 sec. for this route.
- As soon as this count goes to zero, that route is purged from the router table, Due this timers the neighbours become aware that a particular root has become invalid, before its purging.

4. **Disadvantages of RIPv1 :**

- Some of the important disadvantages of the original RIP version i.e. RIPv1 are as follows :

1. RIPv1 only understands the shortest route to a destination, which is based on simple count of number of router hops.
2. It depend on other routers for computed routing updates.
3. Routing tables can get large and these are broadcasted every 30 seconds.
4. Distances are based on hops, not on real costs (such as the speed of link).
5. It continues to be a router to router configuration that means each router is fully depend on its next router to implement the same options.
6. If we solve one problem and other appears.

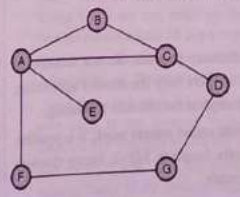
7.33.4 RIP Version 2 :

- In November 1994, RIP was modified with some additions (extensions) to overcome some of its shortcomings. RIP version 1 is still being used on many routers and continues to outnumber OSPF networks. The modified RIP is called RIP version 2 protocol.
- Version 2 is backward compatible with version 1 and contains all of the capabilities of the version 1 protocol. RIP version 2 implemented the following features :

Features :

- Authentication by means of a simple text password.
- Subnet masking used.
- Multicasting used to allow for variable-length subnet masks to be implemented.
- Route tag-to provide a method of separating RIP routes from externally learned routes.
- Compatibility switch-to allow for interoperability with version 1 routers Notice that he same format is used for RIPv1 and RIPv2.

Ex. 7.33.1 : Complete the final routing table at node A using RIP protocol for the following network. Assume the cost of hop count.



Distance	Cost	Next Hop

(G-500) **Fig. P. 7.33.1**

Soln. :

Table P. 7.33.1 : Routing table at A

Destination	Cost (hop count)	Next Hop (Next router)
B	1	B
C	1	C
E	1	E
F	1	F
D	2	C
G	2	F

Scanned by CamScanner

Message format (RIPv2) :

- The message format of RIPv2 is as shown in Fig. 7.33.2.

	Command	Version	Reserved
	Family		Route tag
Repeated	Network address		
	Subnet address		
	Next hop address		
	Distance		

(G-2147) **Fig. 7.33.2 : Message format of RIPv2**

New Fields :

- There are some new fields in the message format of RIPv2 as compared to that in RIPv1. They are as follows :

  1. Route tag 2. Subnet mask 3. Next hop address.

1. **Route tag :** This new field is useful in containing information such as autonomous system number. Using this field, we can enable RIP to receive information from an interdomain protocol.
2. **Subnet mask :** This field is 4 byte long and it contains the subnet mask or prefix. This shows that the classless addressing and CIDR is supported by the RIPv2.
3. **Next-hop address :** This new field contains the address of the next hop. This feature is useful in a situation where the same network is shared by two autonomous systems for example a backbone. With the help of this field, the message can define a router to which the packet is to be sent next. Note that this router can be a part of the same A.S. or some other A.S.

Classless Addressing :

- The most important difference between the two versions of RIP is that RIPv1 can support only the classful addressing, whereas RIPv2 can also support the classless addressing.
- Due to the additional field called **subnet mask,** it is possible to define a network prefix length in RIPv2. Hence classless addressing becomes possible.

Authentication :

- Authentication is a safety measure taken by RIPv2 to ensure the protection of message against unauthorized advertisement.
- For authentication, it is not necessary to add any extra field to the packet. Instead the authentication information is done as the first entry of the message.
- The value of $FFFF_{16}$ is entered in the family field which indicates that the entry is not the routing information but the authentication information, as shown in Fig. 7.33.3.
- The authentication field in Fig. 7.33.3 is used for defining the authentication protocol and the next field carries the actual authentication data.

Command	Version	Reserved
0x FFFF		Authentication type
Authentication data (16 bytes)		
⋮		

(G-2148) **Fig. 7.33.3 : Authentication**

Multicasting :

- In RIPv1 broadcasting is used for sending RIP message to all the neighbours. Due to broadcasting of the message, all the routers as well as hosts connected to the network would receive the RIP message.
- But in RIPv2 an all round **multicast** address is used to send the RIP messages only to the RIP routers on the network.

Encapsulation :

- The UDP is used to encapsulate the RIP messages. That means RIP message is inserted into the UDP user datagram.
- There is no field in RIP message which can indicate the length of the message. The length has to be determined from the UDP packet. The well known port 520 has been assigned to RIP in UDP.

7.33.5 Problems in RIP : MU : May 12

University Questions

Q. 1 Explain various problems in RIP. **(May 12, 5 Marks)**

RIP is the most used Internet interior routing protocols. It is based on the distance vector routing principle. RIP has many limitations. Some of them are as follows :

1. **Width restriction :** RIP uses a 4-bit metric to count router hops to the destination. For RIP infinity is defined as 16 which corresponds to 15 hops.
2. **No direct subnet support :** RIP came into existence prior to subnetting and has no direct support for it. We can use it in the subnetted environment with some restrictions.
3. **Bandwidth consumptive :** An RIP router will broadcast lists of networks and subnets it can reach after every 30 seconds. This will consume a large amount of bandwidth.
4. **Difficult to diagnos fault :** Like any other distance vector routing protocols, RIP also is difficult to debug.
5. **Weak security :** RIP does not have any security features of its own.
6. **Looping problem :** Being based on distance vector principle the RIP faces the looping (routing loop) problem.

Remedies :

Some of the above mentioned problems are overcome with RIP2 while the looping problem can be overcome by using either a link state routing protocol like OSPF or a newer distance vector routing protocol like BGP.

7.34 OSPF : MU : May 09, May 10, May 13

University Questions

Q. 1 Write short notes on : OSPF **(May 09, 10 Marks)**

Q. 2 Explain main features of following protocol : OSPF **(May 10, 2 Marks)**

Q. 3 Write short notes on : OSPF **(May 13, 5 Marks)**

- The long form of OSPF is Open Shortest Path First protocol.
- This is another interior routing protocol. It is an intradomain protocol and it is based on the link state routing. For handling the routing efficiently and in a timely manner, the OSPF divides an A.S. into areas.

Area :

Networks, hosts and routers are collectively called as an area. An autonomous system can be imagined to be made of various areas. All the networks inside an area should be connected.

Area border routers :

These are special type of routers which are used at the borders of an area. These routers summarize the information about the area and sent it to the other areas.

Backbone :

- A special area inside an autonomous system is called as backbone. All the areas inside an A.S. should be connected to the backbone.
- So backbone is the primary area and other areas are known as secondary areas.

Backbone routers :

- The routers inside the backbone are called as the backbone routers. But a backbone router can also work as an area border router.
- If the connectivity between a backbone and an area is broken, due to some problem, then the administration should create a **virtual link** between routers so that the backbone can continue to function as primary area.

Area identification :

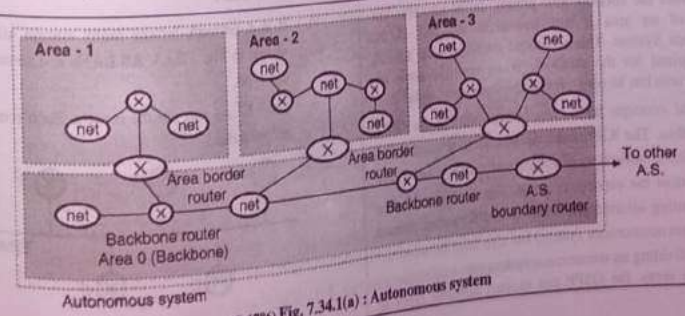
Each area has an area identification. The area identification of the backbone is zero. An autonomous system is as shown in Fig. 7.34.1(a).

Disadvantages of the RIP protocol :

- The maximum distance between any two stations (the metric, measured in router hops) is 15 hops.
- A destination (network ID) whose hop count is 16 or more is considered to be nonreachable.
- The cost to a destination network is measured in terms of number of hops. RIP determines a route based on a hop count that does not take into consideration any other criteria other than the number of routers between the source and destination networks. Due to this approach two-hop high-speed network will be ignored and a one-hop low-speed link would be used instead.
- We can make a router to take a better path by adjusting the hop-count metric on the router port, but this reduces the available diameter.
- RIP updates its entire table on a periodic basis using the broadcast address. (RIPv1; RIPv2 uses multicast or broadcast). But this would consume bandwidth.
- RIP sends its update with the help of a 576 byte datagram. If there are more entries than 512 bytes, then multiple datagrams must be sent.
- The biggest drawback of RIP is its slow convergence. In the worse case, a RIP update can take over 15 minutes end to end. This can lead to black holes, loops, etc.
- RIPv1 does not support VLSM.

Remedies (What OSPF could do) :

- The first shortest-path-first routing protocol was developed and used in the ARPAnet packet switching network all the way back in 1978. This research work was developed and used in many other routing protocol types and prototypes. One of those is OSPF .
- OSPF provides solutions to most of the drawbacks of RIP. Using OSPF we can scale up the routing architecture well beyond the maximum 16 hops supported by RIP.
- Rather than exchanging node (and network) reachability information, OSPF routers exchange link state information.
- Through the link state information, each router maintains its own copy of the network topology. From this link-state database, it is possible to find the shortest routing path.
- For those of you that are familiar with the OSI routing scheme, many of the features supported by OSPF are similar to the OSI IS-IS routing protocol.
- The original versions of OSPF are actually derived from some of the earlier versions of the IS-IS protocol.



(G-1786) **Fig. 7.34.1(a) : Autonomous system**

Scanned by CamScanner

7.34.1 Features of OSPF :

1. **Type of service routing :**

   It is possible to configure different routers to support different types of service requirements. For example, one router can be configured for high-throughput, while the other one is configured to support minimal delivery delay for some other application.

2. **Load balancing :**

   When multiple routes are available, traffic can be evenly distributed over the routes. This would obviously result in a higher network efficiency.

3. **Subdivision of autonomous systems :**

   It is possible to further divide the system into logical areas. This would improve the management of large autonomous systems.

4. **Security :**

   The data exchanges in OSPF are authenticated. Inadvertent or malicious transmissions from foreign routing nodes are disc arded. Only those hosts intended for the routing network are included. The network isn't vulnerable to the threat of having routing tables corrupted by faulty route information.

5. **Host :**

   OSPF supports specific, network and subnetwork routing.

6. **Special features are provided to support LAN environments :**

   Although the relationships between routers are maintained on a logical link basis, link state transmissions are minimized by the architecture. **Designated gateways** are responsible for transmitting the link state information for all information in their local area.

7. **OSPF is an open specification :**

   The OSPF has been published as an RFC and not defined as a defacto standard such as RIP. Therefore anyone can implement the standard, without paying royalties. This has been done to encourage many vendors to use it so that the users are not locked into a single vendor's equipment.

8. **OSPF area :**

   OSPF divides the network into groups, called an **area**. The topology of an area is not known to the rest of the Autonomous System. This techaique minimizes the routing traffic required for the protocol. When multiple areas are used, each area has its own copy of the topological database.

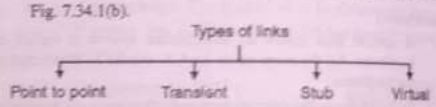
   - Several concepts have been incorporated in the OSPF algorithm. The RIP treated an autonomous system as a monolithic collection of routes and subnets, but OSPF introduces the concept of areas. The concept of hiding the routing information within a OSPF routing domain (Internet autonomous system) has also been introduced.
   - After dividing an autonomous system into a collection of logical areas, the OSPF can support different types of routing nodes (routers) such as internal routers, area border routers, backbone routers, and Autonomous System (AS) boundary routers. (See Fig. 7.34.1(a)).
   - The protocols used to support OSPF routing include database broadcast packets and link state change broadcasts. A "Hello" protocol is used to detect changes in the availability of adjacent routers.

7.34.2 Metric :

- The cost assigned to each route by an OSPF administrator is called as metric of that route. In the OSPF protocol the metric can be based on a type of service.
- A router can have multiple routing tables which are based on different types of service.

7.34.3 Types of Links :

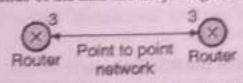
- In the OSPF protocol terminology, a connection is called as a link. OSPF defines four types of links called point to point, transient link, stub link and virtual links as shown in Fig. 7.34.1(b).



(G-501) **Fig. 7.34.1(b) : Types of links**

1. **Point to point link :**

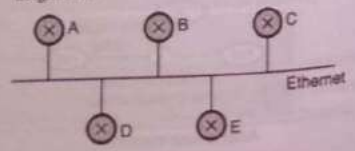
- A point to point link is defined as the link (connection) that directly connects two router without any other host or router present in between. An example of such a link is two routers connected by a telephone line.
- Each router has only one neighbour at the other side of the link. This is shown in Fig. 7.34.2. It is not necessary to assign any network address to this link. The metric are shown at the two ends of the link and they are generally the same.



(G-502(a)) **Fig. 7.34.2 : Point to point link**

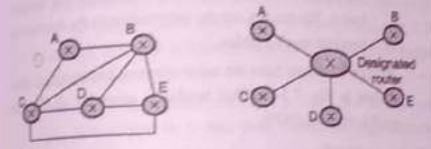
2. **Transient link :**

- It is a network having many routers attached to it as shown in Fig. 7.34.3. All LANs and some WANs are of this type.
- A, B, C ..... etc. are the routers. Each router has several neighbours.



(G-503) **Fig. 7.34.3 : Transient link**

- The relationship between the neighbouring routers is as shown in Fig. 7.34.4(a). Each router has been connected to every other neighbour. But this arrangement is extremely nonefficient and non-realistic. In order to make it more efficient and realistic, the configuration of Fig. 7.34.4(b) should be used. This is known as the transient network. The designated router is assigned to perform two tasks, one as a true router and the other as a designated router.
- Due to the realistic arrangement of Fig. 7.34.4(b) every router has only one neighbour i.e. the designated router (network), however the designated router has multiple (5 in this case) neighbours.



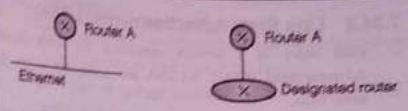
(a) **Unrealistic representation** (b) **Realistic representation**

(G-1707) **Fig. 7.34.4**

- The realistic arrangement reduces the number of announcement that each router has to make to a small number as compared to the unrealistic arrangement.
- Note that there is a metric from each node to designated router and there is no metric from the designated router to any other node.

1. **A stub link :**

- A stub link is a network that is connected to only one router as shown in Fig. 7.34.5.



(a) **Stub network** (b) **Representation**

(G-504) **Fig. 7.34.5**

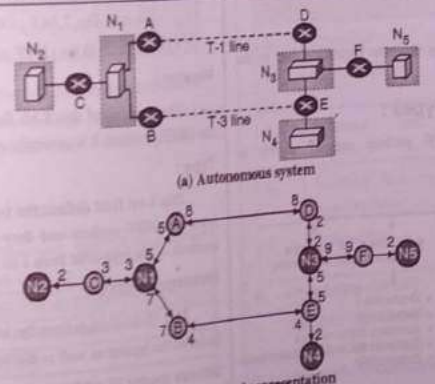
- The stub network of Fig. 7.34.5(a) is a special case of transient network. The data packets use the same link to enter and leave the network.
- This situation can be represented by using router A as a node and by replacing the network by a designated router as shown in Fig. 7.34.5(b). The link connecting router A and the designated router is unidirectional from router to network.
- When this link gets damaged the administration can create a virtual link between the two routers.

7.34.4 Virtual Link :

- The administration can create a **virtual link** between two routers, when a link between them gets broken due to some reason.
- Such a virtual link could be over a longer path which would go through many routers.

7.34.5 Graphical Representation :

- Let us now discuss about representing an A.S. graphically. Consider Fig. 7.34.6(a) which is a small A.S. with multiple networks and routers.
- There are some point to point networks, and transient as well as stub networks.
- The symbols such as N_1 and N_2 are used for the transient and stub networks. No identity should be attached to the point to point networks.
- The graphical representation of the A.S. as seen by OSPF has been shown in Fig. 7.34.6(b).



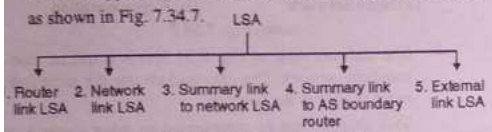
(G-2115) **Fig. 7.34.6 : A.S. and its graphical representation**

Scanned by CamScanner

34.6 Link State Advertisements (LSAs) :

Each entity in a network distributes the Link State Advertisements (LSAs). An LSA announces the states of entity links.

Different types of LSAs depending on the type of entity are as shown in Fig. 7.34.7.



(G-505) **Fig. 7.34.7 : Types of LSAs**

Router Links :

The router produced a router links advertisement for its own area. The advertisement describes the collected states of the router's links to the area. This advertisement also indicates the type of the router i.e. whether it is an area border router or an AS boundary router.

Network Links :

A network link advertisement is produced for every transit multi-access network. This advertisement is produced by the designated router for the transit network. It describes all the OSPF routers fully adjacent to the designated router.

Summary Links :

Summary Link advertisements describe a single route to a destination. The destinations described are external to the area but internal to the Autonomous System. Some condensing of routing information occurs when creating these summary link state advertisements.

AS Summary Links :

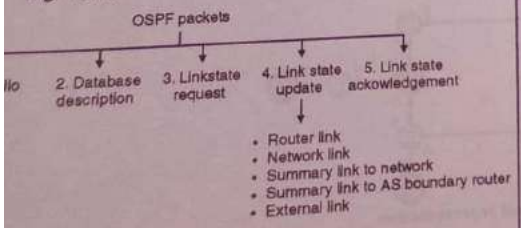
These are like summary link advertisements but they describe routes to Autonomous System boundary routers.

AS External Links :

AS external advertisements describe routes external to the Autonomous System.

34.7 OSPF Packet Types :

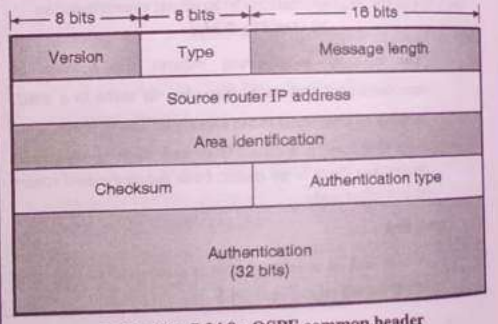
Different types of OSPF packets are as shown in Fig. 7.34.8.



(G-506) **Fig. 7.34.8 : OSPF packet types**

- The OSPF protocol runs directly over IP, and uses the assigned number 89. Each OSPF packet consists of an OSPF header followed by the body of a particular packet type. OSPF packets need to be sent to specific IP addresses in nonbroadcast multi-access networks.
- The OSPF operation consist of following stages :
  - Neighbours are discovered by means of sending The Hello messages and designated routers are elected in multi-access networks.
  - Adjacent routers are identified and link state databases are synchronized.
  - Link State Advertisements (LSA) are exchanged among the adjacent routers so as to maintain the topological databases and also to advertise interarea and interAS routes. The routers use the information in the database to generate routing tables.
- All OSPF packets have the same common header which is as shown in Fig. 7.34.9. This header is same for all the five packet types of OSPF.

Common Header :



(G-2116) **Fig. 7.34.9 : OSPF common header**

- Various fields in the OSPF packet header are as follows :

Version :

The contents of this 8-bit field tells us about the version of the OSPF protocol. It is currently version 2.

Type :

This 8-bit field defines the type of the packet. There are five types of OSPF packets and they can defined by adjusting the contents of the type field from 1 to 5.

Message length :

This 16-bit field defines the length of the total message which includes the header as well as the body.

Source router IP address :

This 32-bit field defines the IP address of the router that sends the packet.

Area identification :

This 32-bit field defines the area within which the routing takes place.

Checksum :

This field is used for error detection on the entire packet excluding the authentication type and authentication data field.

Authentication type :

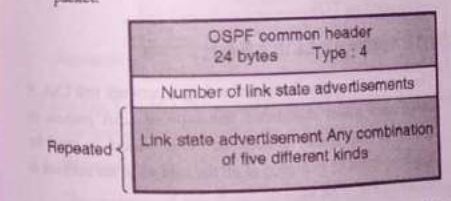
This 16-bit field defines the authentication method used in this area. At this time, two types of authentication are defined : A 0 in this field shows that no authentication is being used and a 1 represents the use of password for authentication.

Authentication :

- This 64-bit field is the actual value of the authentication data. In the future, when more authentication types would be defined, this field will contain the result of the authentication calculation.
- For now, if the authentication type is 0, this field is filled with 0s. If the type is 1, this field carries an eight-character password.

7.34.8 Link State Update Packet :

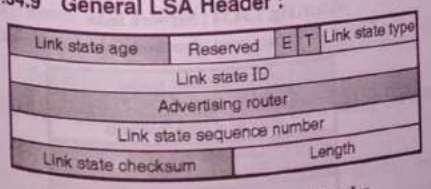
- The heart of OSPF operation is the link state update packet. So let us discuss that first. A router uses this packet, to advertise the states of its links.
- Fig. 7.34.10 shows the general format of the link state update packet.



(G-2117) **Fig. 7.34.10 : Format of link state update packet**

- Each update packet may contain many different LSAs. Fig. 7.34.11 shows the general header which is common to all five types of LSAs.

7.34.9 General LSA Header :



(G-2118) **Fig. 7.34.11 : LSA general header**

- Let us discuss various fields of LSA general header.

1. **Link state age :**
   - This field is useful in indicating the time (in seconds) elapsed from the instant of generation of this message.
   - This type of message travels from router to router which is called as flooding.
   - At the instant of creation of this message by a router, the value of this field is 0.
   - But everytime a router forwards this message, the cumulative value of this field.
2. **E Flag :**
   - This is a 1 bit flag. If E = 1 then it indicates that the area is a **stub area.** The area that is connected to the backbone by only one path is called as the stub area.
3. **T - Flag :**
   - This is also a 1 bit flag. If T = 1, then it indicates that it is possible for the router to handle multiple services.
4. **Link state type :**
   - This field is used for defining the LSA type. There are five different types of advertisements as follows :
     1. Router link
     2. Network link.
     3. Summary link to network.
     4. Summary link to A.S. boundary router.
     5. External link.
5. **Link state ID :**
   - The contents of this field are dependent on the type of link, as shown in Table 7.34.1.

Table 7.34.1

Type	Link	Link state ID
1.	Router link	IP address of router
2.	Network link	IP address of designated router.
3.	Summary link to network.	Address of the network
4.	Summary link to AS boundary router	IP address of AS boundary router.
5.	External link	Address of external Network

6. **Advertising router :**
   - The field contains the IP address of the router which advertises this message.
7. **Link state sequence number :**
   - This field contains a sequence number that is assigned to each link state update message.

Scanned by CamScanner

8. Link state checksum :

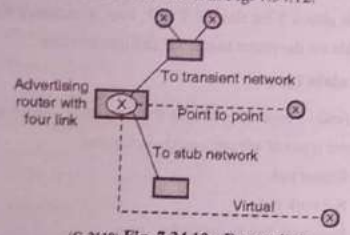
- The contents of this field is not the usual checksum. But the value of this field is calculated on a special type called as **Fletcher's checksum.** This method of calculating checksum considers the whole packet except for the age field to calculate the checksum.

9. Length :

- This field is used for defining the length of the whole packet, in bytes.

7.34.10 Router Link LSA :

- The links of a true router are defined by a router link. This advertisement is used by a true router to announce information about all its links and at the same time about the neighbours.
- A router link has been shown in Fig. 7.34.12.

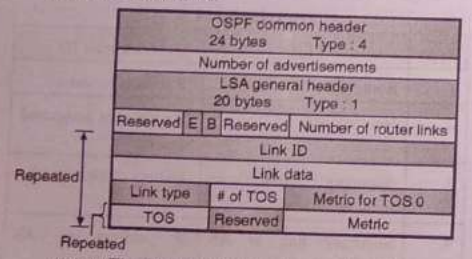


(G-2119) **Fig. 7.34.12 : Router link**

- The router link LSA is used for advertising all the links of a true router.

7.34.11 Router Link Packet :

- Fig. 7.34.13 shows the format of router link packet. Let us discuss its various fields.



(G-2120) **Fig. 7.34.13 : Format of router link LSA**

1. Link ID :

The contents of this field are dependent on the type of link. Different link identifications on the basis of link type are as shown in Table 7.34.2.

Table 7.34.2

Link type	Link identification	Link data
Type 1 : Point to point	Address of neighbor router	Interface number
Type 2 : Transient	Address of designated router	Router address
Type 3 : Stub.	Network address	Network mask
Type 4 : Virtual	Address of neighbor router	Router address

2. Link data :

The contents of this field give additional information about the link. Therefore the contents of this field are dependent on the type of link as shown in Table 7.34.2.

3. Link type :

As shown in Table 7.34.2, OSPF defines four types of links on the basis of the type of network, the router is connected to.

4. Number of types of service (TOS) :

The contents of this field are used for defining the number of types of services that are announced for each link.

5. Metric for TOS 0 :

The default type of service is TOS 0. This field is used for defining the metric for the default service.

6. TOS :

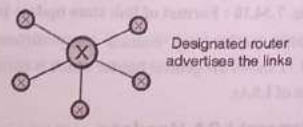
The contents of this field are used for defining the type of service.

7. Metric :

The contents of this field are used for defining the metric for corresponding TOS.

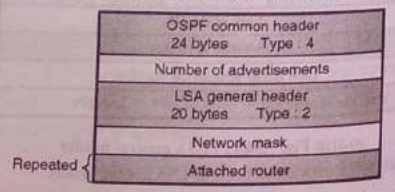
7.34.12 Network Link LSA :

- The links of a network are defined by a network link LSA. A designated router distributes this type of LSA packets on behalf of the transient network. This packet is used for announcement of existence of all the routers to the network as shown in Fig. 7.34.14.



(G-2121) **Fig. 7.34.14 : Network links**

- Fig. 7.34.15 shows the format of network link advertisement.



(G-2122) **Fig. 7.34.15 : Network link advertisement format**

- The important fields of the network link LSA are as given below.

1. Network mask :

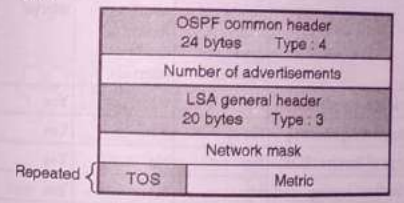
The contents of this field are used for defining the network mask.

2. Attached router :

The contents of this field are used for defining the IP addresses of all the attached routers. This field is a repeated field.

7.34.13 Summary Link to Network LSA :

- Inside an area, the router link and network link advertisements provide ample information about the router links and network links to a router.
- But this information is not enough. In addition to this, a router is also supposed to know about the network outside its area. This information is provided by the **border routers.**
- An area border router receives router link and network link advertisements and create a routing table for each area because it is simultaneously active in more than one areas.
- Fig. 7.34.16 shows the format of the summary link to network LSA.



(G-2123) **Fig. 7.34.16 : Format of summary link to network LSA**

- The important fields in this are as follows :

1. Network mask :

The contents of this field are used for defining the network mask.

2. TOS :

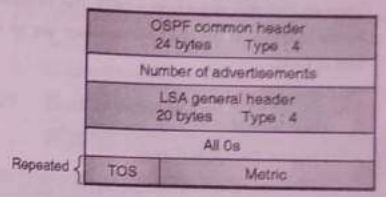
The contents of this field are used to define the type of service.

3. Metric :

The contents of this field are used for defining the metric for the type of service stated in the TOS field.

7.34.14 Summary Link to AS Boundary Router LSA :

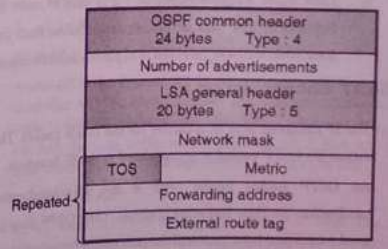
- The previous advertisement was designed to let every router know the cost to reach all the networks that belong to an A.S.
- But what if a router inside an AS wants to send a packet outside the AS ?
- In order to accomplish this, the router must know the path (route) to an autonomous boundary router.
- This information is provided by the summary link to AS boundary router.
- The area boundary routers will simply flood their areas with this information. This packet contains the information about the route to an AS boundary router.
- Fig. 7.34.17 shows the format for summary link to AS boundary router LSA. Its primary objective of this packet is to define the network to which the AS boundary router has been attached.
- The fields in this format are same as those in the summary link to the network advertisement message.



(G-2124) **Fig. 7.34.17 : Summary link to AS boundary router LSA**

7.34.15 External Link LSA :

- We have seen how the previous advertisement makes each router to know about the route to an AS boundary router.
- But only this much information is not sufficient because a router inside an AS would also like to know about the networks available outside the AS.
- This information is provided by the external link advertisement. The cost of each network outside the AS is made available (flooded) by the AS boundary router inside that AS, with the help of a routing table created by an inter domain routing protocol.
- This is accomplished by announcing one single network through an advertisement. A separate announcement is made for each network.
- Fig. 7.34.18 shows the format of external link LSA. This format is very similar to the summary link to the AS boundary router LSA but there are two additional fields.



(G-2125) **Fig. 7.34.18 : External link LSA**

Scanned by CamScanner

These two additional fields are as follows :

Forwarding address :

The contents of this field define the address of a forwarding router which is defined by the AS boundary router. This forwarding router may prove to be a better forwarding destination.

External route tag :

This field contents are used by other protocols except OSPF.

34.16 Other Packets :

There are four other packet types in OSPF. They are essential for the operation of the protocol even though they are not used as LSAs.

They are as follows :

1. Hello message.
2. Database description message.
3. Link state acknowledgement message.
4. Link state request message.

1. **Hello :** Used to discover and maintain neighbours.
2. **Database Description :** Used to form adjacencies. The router summarizes all its link state advertisements and passes this information, via database description packets to the router with which it is forming an adjacency.
3. **Link State Request :** After the database description packets have been exchanged with a neighbour, the router may think that link state advertisements it requires to update or complete the topological database. Link state request packets are sent to the neighbour in order to request for these link state advertisements.
4. **Link State Update :** It is used for transmission of link state advertisements between routers. This could be in response to a link state request packet or to flood a new or more recent link state advertisement.
5. **Link State Acknowledgment :** It is used to make the flooding of link state advertisements reliable. Each link state advertisement received is explicitly acknowledged.

34.17 Encapsulation :

The IP datagram acts as a carrier for the OSPF packet. That means the OSPF packet is encapsulated in the IP datagram.

An OSPF packet carrier with it the acknowledgement mechanism for flow and error controls. Thus OSPF does not need a transport layer protocol for provision of these services.

7.34.18 Comparison between RIP and OSPF :

MU : Dec. 11, May 12

University Questions

Q. 1 State atleast three major differences between RIP and OSPF. **(Dec. 11, May 12, 10 Marks)**

Function/Feature	RIPv1	RIPv2	OSPF
Standard number	RFC 1058	RFC 1723	RFC 2178
Link-state protocol	No	No	Yes
Large range of metrics	Hop count (16=Infinity)	Hop count (16=Infinity)	Yes, based on 1-65535
Update policy	Route table every 30 seconds	Route table every 30 seconds	Link-state changes, or every 30 [minutes]
Update address	Broadcast	Broadcast, multicast	Multicast
Dead interval	300 seconds total	300 seconds total	300 seconds total, but usually much less
Supports authentication	No	Yes	Yes
Convergence time	Variable (based on number of routers X dead interval)	Variable (based on number of routers X dead interval)	Media delay + dead interval
Variable-length subnets	No	Yes	Yes
Supports supernetting	No	Yes	Yes
Type of Service (TOS)	No	No	Yes
Multipath routing	No	No	Yes
Network diameter	15 hops	15 hops	65535 possible
Easy to use	Yes	Yes	No

7.35 Path Vector Routing :

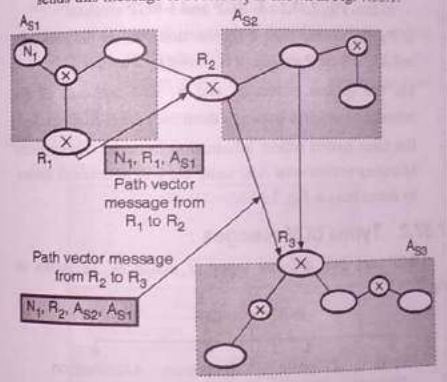
- It is different from both distance vector routing and link state routing.
- Table 7.35.1 shows the example of a path routing table. Each entry in the routing table will have the information about the destination network, the next router and the path to reach the destination.

Table 7.35.1 : Path vector routing table

Network	Next router	Path
N01	R01	AS 12, AS 21, AS 56
N02	R08	AS 20, AS 57, AS 06
.	.	.
.	.	.
.	.	.

7.35.1 Path Vector Messages :

- The autonomous boundary routers participate in path vector routing. Their job is to advertise the reachability of networks present in their A.S. to the neighbour autonomous boundary router.
- Each router that receives a path vector message verifies whether or not the advertised path is according to its policy. Such a policy is made up of rules that are imposed by the router controlling administrator.
- If yes then the router will update its routing table and will modify the message before it is sent to the next neighbour.
- In the modified message it sends its own AS number and replaces the next router entry with its own identification. This process is demonstrated in Fig. 7.35.1.
- Fig. 7.35.1 shows an internet containing three autonomous systems A_{S1} through A_{S3}.
- Router R_1 sends a path vector message to advertise that it is reachable to network N_1. Router R_2 on receiving this message will update its routing table. It then adds its own autonomous system (A_{S2}) to the path, inserts itself as the next router and sends this message to router R_3 as shown in Fig. 7.35.1.



(G-1788) **Fig. 7.35.1 : Path vector messages**

7.35.2 Loop Prevention :

- When a message is received, a router checks it to see if its autonomous system is in the path list to the destination. If it is present it indicates looping is involved which is undesirable and the message is ignored.
- In this way the looping problem and the associated instability which is present in distance vector routing is avoided in path vector routing.

7.35.3 Path Attributes :

- The path is specified in terms of attributes. Each attribute gives some information about the path. Hence the list of attributes helps the receiving router to make a better decision about when to apply its policy.
- Attributes are of two types :
  1. A well known attribute
  2. An optional attribute
- An attribute is called as a well known attribute if it is recognised by every BGP router.
- An optional attribute is the one that need not be recognised by every BGP router.
- The well known attributes are further classified into two categories :
  1. Well known mandatory attributes
  2. Well known discretionary attributes.
- The optional attributes also are classified into two types :
  1. An optional transitive attribute
  2. An optional nontransitive attribute.

7.36 Border Gateway Protocol (BGP) :

MU : Dec. 09, May 10, Dec. 10, May 15, May 16, Dec. 16

University Questions

Q. 1 Write short notes on : BGP. **(Dec. 09, Dec. 10, May 15, May 16, Dec. 16, 5 Marks)**

Q. 2 Explain main features of following protocol : BGP **(May 10, 10 Marks)**

- BGP is an exterior routing protocol. It is a unicast routing protocol. It is used for the interautonomous system routing i.e. routing among different ASs.
- It was introduced in 1989 and has four versions. BGP operation takes place on the basis of the routing method called **path vector routing.**
- This principle is used because the distance vector routing and link state routing do not prove to be much suitable for interautonomous system routing.

7.36.1 Types of Autonomous Systems :

- We have already discussed about autonomous systems. Now let us discuss about their types.
- The three categories of autonomous systems are as follows :
  1. Stub AS
  2. Multihomed AS
  3. Transit AS.

1. Stub AS :

- A stub AS is that type of AS which has only one connection to another AS. The hosts in the AS can send and receive data traffic to the hosts belonging to other AS.
- But note that data traffic cannot pass through a stub AS. In other words the stub traffic can be either a source or sink.

2. Multihomed AS :

- An AS which has more than one connection to other ASs is known as multihomed AS. But it is interesting to note that a multihomed AS is still only a source or sink for data traffic.

Scanned by CamScanner

- For a host in multihomed AS, it is possible to send and receive data traffic to from more than one AS. But it does not allow the **transient traffic.**
- That means, the multihomed AS does not allow the data traffic coming from one AS to just pass through to the other AS.

3. Transit AS :

An AS which is a multihomed AS but also allows the transient data traffic is called as **transit AS.**

7.36.2 CIDR :

- A Classless interdomain addressing is used in BGP. That means BGP makes use of the prefix (As discussed earlier) for defining a destination address.

7.36.3 Path Attributes :

- The path for a destination address can be presented as a list of **attributes.** We get some information from each attribute about the path.
- The receiving router takes the help of this list of attributes for making a better decision when applying its policies.

7.36.4 Types of Attributes :

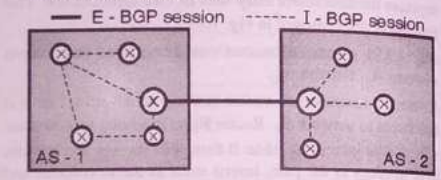
- There are two categories of attributes :
  1. A will known attribute.
  2. An optional attribute.
- Every BGP router must recognize the **well known** attribute whereas the **optional attribute** is the one which need not be recognized by every router.
- The well known attributes are further classified into two types namely **mandatory** and **discretionary.**
- We define the well known mandatory attribute as the one which must appear in the description of router.
- On the other hand a well known discretionary attribute can be defined as the one which must be recognized by each router, but it need not be included in every update message.
- We can also subdivide the optional attributes into two categories as : **transitive** and **nontransitive** optional attributes.
- We may define the optional transitive attribute as the one which should be passed to next router that has not implemented this attribute.
- Similarly an optional nontransitive attribute is defined as the one which must be discarded if the receiving router has not implemented it.

7.37 BGP Sessions :

- In a BGP **session,** the two routers using BGP exchange routing information between them. So we can define a session as **connection** which has been established between two BGP routers in order to exchange the routing information.
- In order to ensure a reliable session the BGP uses services of TCP.
- The speciality of such a connection that it lasts for a longer time until something unusual happens.
- Therefore the BGP sessions are called as the **semipermanent connections.**

7.37.1 External and Internal BGP :

- There are two types of BGP sessions as follows :
  1. External BGP (E-BGP) session.
  2. Internal BGP (I-BGP) session.
- We can use the **E-BGP** session for exchanging information between two nodes which are present in two different ASs. This is as shown in Fig. 7.37.1.

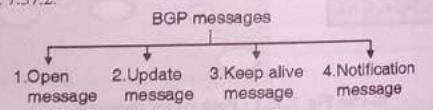


(G-2126) **Fig. 7.37.1 : E-BGP and I-BGP sessions**

- In Fig. 7.37.1, the session (connection) shown between AS_1 and AS_2 is E-BGP session. It is shown by a bold line.
- The two speaker routers A_1 and B_1 will exchange all the information which is known to them over the E-BGP session.
- But these routers collect information from the other routers belonging to their own A.S. using the I-BGP sessions shown by dotted lines in Fig. 7.37.1.

7.37.2 Types of Messages :

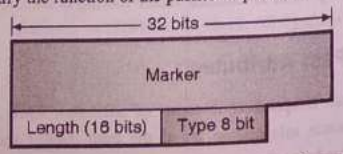
BGP uses four different types of messages, as shown in Fig. 7.37.2.



(G-508) **Fig. 7.37.2 : BGP message types**

7.37.3 Packet Format :

- All BGP message types use the basic packet header. Open, update, and notification messages have additional fields, but keep-alive messages use only the basic packet header.
- Fig. 7.37.3 illustrates the fields used in the BGP header. Each BGP packet contains a header whose primary purpose is to identify the function of the packet in question.



(G-2127) **Fig. 7.37.3 : BGP packet header format**

- Different important fields in the BGP packet header are as follows :

Marker :

This is a 32 bit field. It contains an authentication value that the message receiver can predict.

Length :

This is a 16 bit field which indicates the total length of the message in bytes. The value of the length field must be between 19 and 4096.

Type :

Type is an 8-bit field which specifies the message type as one of the following :

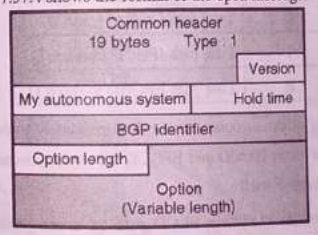
- Open
- Notification
- Update
- Keep-alive

7.37.4 Open Message :

- This message is used by a router running BGP to create a neighbourhood relationship. To do so the router opens a TCP connection with a neighbor router and sends an **open message** to it.
- If the neighbor router is interested then it responds by sending a **keepalive message** which is an indication that the relationship between these two neighbor routers has been established.

Format :

- Fig. 7.37.4 shows the format of the open message.



(G-2128) **Fig. 7.37.4 : Format of open message**

- The important fields of the open message are as follows :

1. Version :

The contents of this 1-byte long field define the version of BGP. The current version of BGP is 4.

2. My autonomous system :

The contents of this 2-byte (16 - bit) field are used to define the autonomous system number.

3. Hold time :

The contents of this 2-byte field specify the maximum amount of time in seconds that can elapse until one of the routers receives either a **keepalive** or **update** message from the other. If a router does not receive any of these messages during the hold time, then the other router is considered to be **dead.**

4. BGP identifier :

The contents of this 4-byte long field defines the router which has sent the open message.

5. Option length :

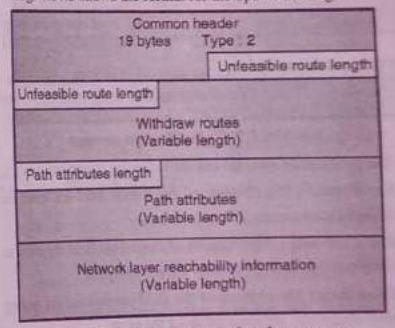
This one byte field is used for defining the length of the total option parameters. The value of this field is zero if there are no option parameters.

6. Option parameters :

This is a variable length field which contains the option parameters. The nonzero value of option parameter length field is an indication that there are some option parameters. **Authentication** is the only option parameter defined so far.

7.37.5 The Update Message :

- This is the most important message in BGP. This message is used by the routers for the following two purposes :
  1. In order to withdraw a previously advertised destination.
  2. In order to announce a route to a new destination.
- The BGP can withdraw more than one previously advertised destinations but in a single update message, it can advertise only **one** new destination.
- Fig. 7.37.5 shows the format for the update message.



(G-2129) **Fig. 7.37.5 : Format of update message**

- The important fields in the update message are as follows :

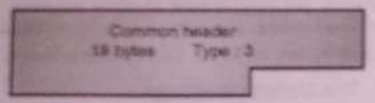
1. **Unfeasible route length :** This 2-byte long field is used for defining the length of the next field.
2. **Withdrawn routes :** The contents of this variable length field gives the list of all the previously advertised routes which should be deleted.
3. **Path attribute length :** The contents of this 2-byte long field defines the length of the next field.
4. **Path attributes :** The contents of this field are used for defining the attributes of the path (route) whose reachability is announced in this update message.

Scanned by CamScanner

5. **Network layer reachability information :** The contents of this variable length field, are used for defining the network which is actually advertised in this update message. BGP4 supports classless addressing and CIDR.

7.37.6 Keepalive Message :

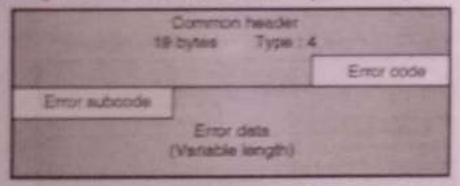
- The keepalive messages are regularly exchanged by all the routers running the BGP protocol, to tell each other that they are alive.
- The format of keepalive message is as shown in Fig. 7.37.6 which shows that it consists of only the common header.



(G-2130) **Fig. 7.37.6 : Format of keepalive message**

7.37.7 Notification Message :

- A router sends the notification message whenever it detects an error condition or when a router wants to terminate the connection.
- Fig. 7.37.7 shows the format of the keepalive message.



(G-2131) **Fig. 7.37.7 : Notification message**

- The notification message has the following important fields :

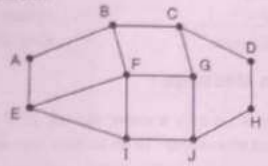
1. **Error code :** The contents of this 1-byte field are used for defining the category of error.
2. **Error subcode :** The contents of this 1-byte field are used to further define the type of error in each category.
3. **Error data :** The contents of this field can be used for giving more diagnostic information about the error.

7.37.8 Encapsulation :

- BGP messages are encapsulated in TCP segments by using the well known port 179. The error control and flow control are therefore not needed.
- After opening a TCP connection, the update, keepalive and notification messages are exchanged until a notification message is sent.

7.37.9 How does BGP Solve the Count to Infinity Problem ?

- The BGP is basically a distance vector protocol. But it is very much different from the most other protocols such as RIP.
- Instead of maintaining just the cost of each destination, each BGP router keeps track of the path used.
- Similarly instead of periodically giving each neighbour its estimated cost to each possible destination, each BGP router tells its neighbour the exact path that it is using.
- Fig. 7.37.8 shows a set of BGP routers and Table 7.37.1 shows the information that router F receives from its neighbours about "D".
- BGP can solve the count to infinity problem easily. This can be explained as follows : Suppose that the router G in Fig. 7.37.8 crashes, or if the line FG becomes faulty, then router F receives routes from the remaining three neighbours i.e. B, I and E.



(G-512) **Fig. 7.37.8 : A set of BGP router**

- As shown in Table 7.37.1, these routes are BCD, IFGCD and EFGCD.

Table 7.37.1 : Information received by F from neighbours about D

Neighbour	Information
B	I use path BCD to reach D.
G	I use path GCD to reach D.
I	I use path IFGCD to reach D.
E	I use path EFGCD to reach D.

- Looking at these routes, router F immediately understands that, the routes IFGCD and EFGCD are useless because they pass through F itself.
- So it decides to choose FBCD path as a new route. This avoids the count-to-infinity problem.

7.38 Multicast Routing Protocols :

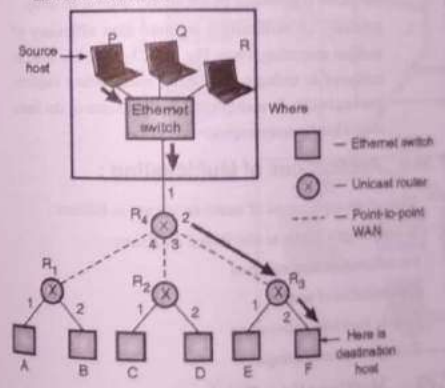
- In this section we are going to discuss multicasting and multicasting protocols.
- A message can be unicast, multicast or broadcast.

Introduction :

- We have already discussed in the previous sections that, in the datagram forwarding a datagram by a router is based on the prefix of the destination address which describes the network to which destination host is connected. In the following section we will define unicasting, multicasting and broadcasting to understand the forwarding principle.

7.38.1 Unicasting :

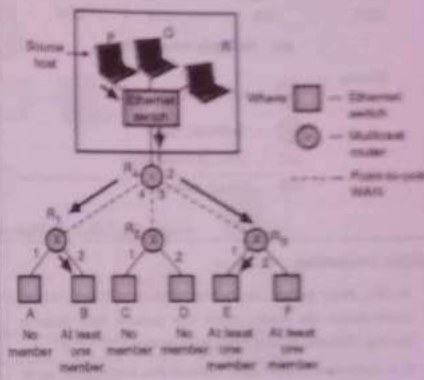
- In the unicast communication, the communication takes place between one source and one destination. That means the relation between source and destination is one-to-one.
- In the IP datagram, both the source and destination addresses are the unicast addresses assigned to the hosts.
- In unicasting when a router receives a packet it forwards the packet through only one of its interfaces. This interface is the one corresponding to the optimum path. The router may discard the packet if the destination can not be found.
- Fig. 7.38.1 shows the concept of unicasting. Delivery of unicast packet from a source computer to a destination computer is as shown in Fig. 7.38.1.
- In Fig. 7.38.1, P is a source and destination computer is attached to Ethernet switch F.
- The responsibility of router R_4 is to forward the packet only through interface 2, the responsibility of router R_3 is to forward the packet only through interface 2.
- After arrival of packet at f, the responsibility of the network is to deliver the packet to destination host. The network broadcasts it to all hosts or Ethernet switch will deliver it to the destination host.



(G-2235) **Fig. 7.38.1 : Concept of unicasting**

7.38.2 Multicasting :

- In multicast communication, the communication takes place between one source and a group of destinations i.e. the source to destination relationship is one-to-many.
- The type of source address is unicast address but the type of destination address is a group address that defines one or more destinations. The group address actually identifies all the members of a group.
- When a router receives a packet, it will forward the copies of packet to all the destinations through more than one of its interfaces, as shown in Fig. 7.38.2.
- Router R_4 sends the datagram through interface 3 and 4.
- Router R_3 sends the datagram via both its interfaces 1 and 2. As R_3 knows that there is atleast one member in subnetwork which belongs to this group in the area reached by interfaces 1 and 2.
- Router R_2 sends the datagram through interface 2. R_2 knows that there is no member interested in receiving datagram which belongs to the group in area reached by interface 1.



(G-2236) **Fig. 7.38.2 : Concept of multicasting**

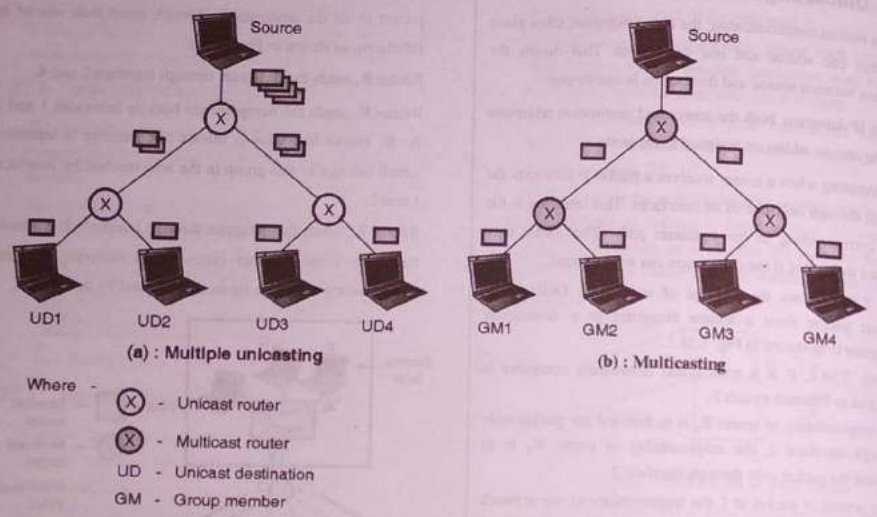
7.38.3 Broadcasting :

- In broadcast communication the source to destination relationship is of one-to-all type. That means there is only one source host and all other host act as destinations.
- On Internet the broadcasting does not take place due to the huge amount of traffic it would create and the corresponding bandwidth requirement.

7.38.4 Multiple Unicasting Versus Multicasting :

- Fig. 7.38.3 shows the concept of multiple unicasting and multicasting.

Scanned by CamScanner



(G-2237) **Fig. 7.38.3 : Multiple unicasting versus multicasting**

Multiple unicasting :

- In this, many packets starts from the source. If there are four destinations, the source sends four packets. Each packet is having different unicast destination address.
- It is important to note that, between two routers there can be several copies travelling.
- Example of multiple unicasting is e-mail. If a person want to send an e-mail to a group of people, the e-mail application software generates copies of the messages, each having a different destination address and one by one message is sent to each person.

Multicasting :

- In multicasting, single packet starts from the source and is duplicated by the routers. For all replicas, the destination address in each packet is same. It is important to note that, between any two routers only one copy of the packet travels.

7.38.5 Emulation of Multicasting with Unicasting :

- If multicasting can be emulated with unicasting, then why there is separate mechanism for multicasting. Following are the reasons for separate mechanism for multicasting :
  1. In multiple unicasting, there is relative delay between packets which are generated by the source. If there are 100 destinations there is delay between the first and last packet which is unacceptable. In multicasting, as only one packet is generated by the source there is no delay.
  2. Efficiency of multicasting is more than efficiency of multiple unicasting. From Fig. 7.38.3 it is clear that, as compared to multiple unicasting, multicasting requires less bandwidth. In multiple unicasting, some of the links should handle many copies.

7.38.6 Applications of Multicasting :

Some of the applications of multicasting are as follows :

1. In order to gain access to distributed databases.
2. For information dissemination
3. Dissemination of news.
4. So as to have teleconferencing
5. To help distance learning.

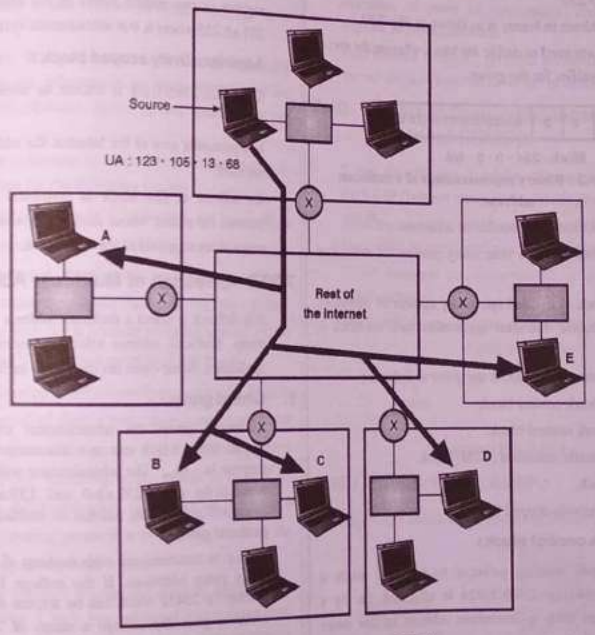
7.39 Multicasting Basics :

- We need to discuss some basics of multicasting such as multicast addressing, information collection about multicast groups and multicast optimal trees before discussing multicast routing protocols.

7.39.1 Multicast Addresses :

- In unicast communication, the source address defines the sender and the destination address defines the receiver of the packet.

- In case of multicast communication, there is only one sender and many receivers. Note that in the packet it is not able to include the addresses of all recipients.
- As discussed in the Internet protocol (IP), the destination address of packet should be only one. We need multicast address for this reason.
- A multicast address describes a group of recipients which acts as an identifier for a group.
- With some active members a new group is formed. To define this new group uniquely, an authority may assign multicast address which is unused.
- In multicast communication, the source address of packet is unicast which defines sender uniquely whereas the destination address is multicast address which defines a group of recipients.
- In such a way, host is a member of 'n' groups which has (n + 1) addresses, one unicast address which is for source or destination address in unicast communication and to receive messages sent to a group 'n' multicast addresses are used for destination addresses. The concept of multicast addresses is as shown in Fig. 7.39.1.



Where
A, B, C, D and E are members of the group 221 . 46 . 75 . 64

For A = UA : 14 · 22 · 43 · 3 MA : 221 · 46 · 75 · 64	For B = UA : 27 · 10 · 20 · 18 MA : 221 · 46 · 75 · 64 For C = UA : 27 · 10 · 20 · 19 MA : 221 · 46 · 75 · 64
For D = UA : 18 · 21 · 42 · 2 MA : 221 · 46 · 75 · 64	For E = UA : 21 · 25 · 50 · 5 MA : 221 · 46 · 75 · 64

UA - Unicast Address
MA - Multicast Address
- Ethernet switch
- Multicast delivery

(G-2238) **Fig. 7.39.1 : Concept of multicast addresses**

Scanned by CamScanner

7.39.2 Multicast Addresses in IPv4 :

- It is necessary to differentiate a router or a destination host between a unicast and multicast datagram. For this purpose a block of addresses are assigned by IPv4 and IPv6.
- In this section we will discuss the multicast addresses in IPv4.
- In IPv4, multicast addresses belongs to a huge block of addresses which are designed for this purpose.
- In classful addressing, class D was composed of multicast addresses. The same block is used by classless addressing and it was referred to as the block 224.0.0.0/4. i.e. from 224.0.0.0 to 239.255.255.255.
- A multicast address in binary is as shown in Fig. 7.39.2.
- First four bits are used to define the block whereas the rest of the bits are identifier for the group.

1	1	1	0	Group identifier (28 bits)

Block : 224 · 0 · 0 · 0/4

(G-2239) **Fig. 7.39.2 : Binary representation of a multicast address**

- In the multicast block, the number of addresses = 2^{28}.
- It is not possible to have that many number of individual groups.
- A multicast block is divided into many number of subblocks and for a particular multicast application each subblock is used.
- Some of the common subblocks are given as follows :
  1. Local network control block.
  2. Internetwork control block.
  3. Source specific multicast (SSM) block.
  4. GLOP block.
  5. Administratively scoped block.

1. Local network control block :

- To a multicasting routing protocol to be used inside a network, the subblock 224.0.0.0/24 is allocated. i.e. by a router the packet with a destination address in this range cannot be forwarded.
- The address 224.0.0.0 is reserved in this subblock and inside a network to send datagrams to all hosts, the address 224.0.0.1 is used. To send datagrams to all routers the address 224.0.0.2 is used.
- For communication, the remaining addresses are allocated to some multicasting protocols.

2. Internetwork control block :

- In the whole Internet, the subblock 224.0.1.0/24 is allocated to a multicast routing protocols which is used in the Internet. This means, in this range the packet with a destination address can be forwarded by a router.

3. Source specific multicast (SSM) block :

- For source specific multicast routing, the block 232.0.0.0/8 is used.

4. GLOP block :

- The block 233.0.0.0/8 is known as the GLOP block.
- GLOP block defines a range of addresses which can be used inside a AS (autonomous system). A 16-bit number is assigned to each autonomous system.
- To create a range of 256 multicast addresses we can add AS number as two middle octets in the block. i.e. 233.a.b.0 to 233.a.b.255 where a, b is autonomous system number.

5. Administratively scoped block :

- The block 239.0.0.0/8 is known as administratively scoped block.
- In a particular area of the Internet the addresses in this block are used.
- An address in this block is restricted to an organization because the packet whose destination address belongs to this range is not supposed to leave the area.

7.39.3 Selection of Multicast Address :

- It is difficult to select a multicast address to be allocated to a group. Multicast address selection depends on the type of application. Some cases are discussed as follows :

1. Limited group :

- In limited group, the administrator use administratively scoped block which can use autonomous system number suppose $(a \cdot b)_{256}$. The administrator will select an address between the range 239.a.b.0 and 239.a.b.255. Any other group will not use this address as multicast address for that particular group.
- For e.g. to communicate with students if professors want to create group addresses. If the college belongs to the AS number i.e. 23452 which can be written as $(91.156)_{256}$. That means it gives the college a range of 256 addresses. i.e. 233.91.156.0 to 233.91.156.255. From this range one of the address is granted to each professor. Then for the professor this can become a group of addresses through which professors can send multicast communications to their students. The packets will not be able to go beyond the college AS territory.

2. Larger group :

- The previous solution will not work if the group is spread beyond an Autonomous System region. In this case the group needs to select an address from source specific multicast (SSM) block. (i.e. 232.0.0.0/8). It is not necessary to get permission to use an address from this group. The reason is that, packet routing in SSM group is based on the source and group address are unique.

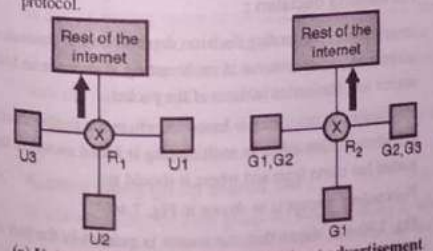
7.39.4 Collection of Information about Groups :

- Following two steps are involved in creation of forwarding tables in unicast and multicast routing.

Step 1 : A router required to know about to which destination it is connected.

Step 2 : Each router required to spread information which is obtained in step 1 to all other routers so that each router will come to know to which destination other router is connected.

- The information collection in the first step is automatic in **unicast routing.** A router needs the prefix of the network (in CIDR) and each router knows to which network it is connected.
- In the Internet, for propagation of these automatically collected pieces of information to each other router, the routing protocols distance vector or link state routing are responsible.
- The information collection in the first step is not automatic in **multicast routing** for the following reasons :
  1. In the attached network, a router does not know which host is member of a particular group. There is no relation between membership in the group and the prefix associated with the network. We have already shown that host has a separate multicast address related to the group if a host is a member of that group.
  2. The membership is not a fixed feature of a host. Even in a short period of time a host can join new groups and can leave some other groups. For this reason, a router needs help for searching active groups in each of its interfaces. After collection of information, by using a multicast routing protocol a router can broadcast the membership to any other router.
- The difference between unicast and muticast advertisement is as shown in Fig. 7.39.3. For unicasting router do not need help whereas for multicasting router needs help of another protocol.



(a) Unicast advertisement (b) Multicast advertisement

(G-2240) **Fig. 7.39.3**

Unicast advertisement :

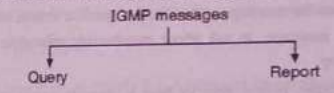
- Router R_1 knows about hosts with their prefixes U1, U2 and U3 which are connected to its interfaces and router broadcasts this information to the rest of the Internet.
- There is need of only the routing protocol inside each domain for propagation of information about a link of router.

Multicast advertisement :

- In this case, it is required for router R_2 to know that there are hosts with atleast one member who is loyal in groups G1, G2 and G3 in networks which are connected to its interfaces.
- Two protocols are required for multicasting. One protocol for collection of piece of information and second protocol required to propagate them.
- First we need to discuss protocol involved in step 1 and then we will discuss protocols involved in second step.

7.40 Internet Group Management Protocol (IGMP) :

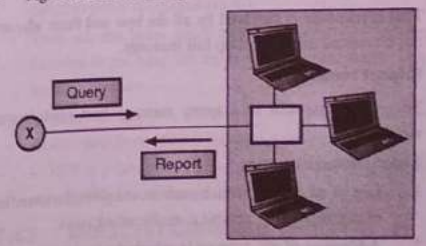
- Today, for collection of information about group membership the IGMP (Internet group management protocol) is used.
- IGMP is one of the auxiliary protocol defined at the network layer which is considered as a part of Internet protocol.
- IGMP messages are encapsulated in datagram similar to ICMP messages.
- Fig. 7.40.1 shows two types of messages in IGMP version 3.



(G-2241) **Fig. 7.40.1**

7.40.1 Operation of IGMP :

- Fig. 7.40.2 shows the operation of IGMP :



(G-2242) **Fig. 7.40.2 : 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 :

Scanned by CamScanner

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.
- 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 de
- stination address set to the corresponding multicast address the message is encapsulated in a datagram.
- This is 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.

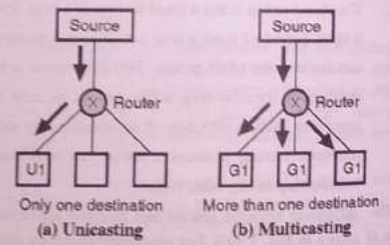
- In a datagram, the message is encapsulated with the multicast address 224.0.0.22 which is allocated to IGMPv3.
- In IGMPv3, if any host want to join a group, it will wait to receive a query message and then host sends a report message.
- If host want to leave the group then it will not respond to a query message.
- The group is eliminated from the router database if no hosts responds to corresponding message.

7.40.2 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 unicasating 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. 7.40.3. 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.

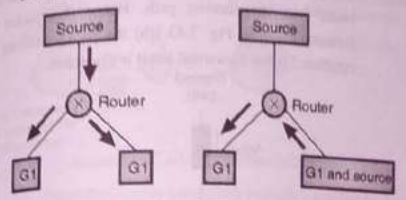


(G-2243) **Fig. 7.40.3 : Destination in unicasting and multicasting**

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. 7.40.4.
- Fig. 7.40.4(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. 7.40.4(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. 7.40.4 : Forwarding**

7.40.3 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 :

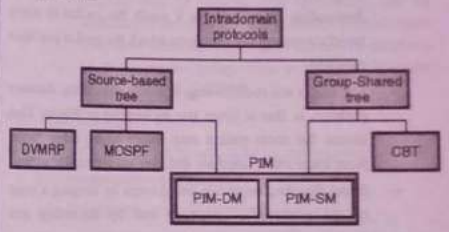
- In this approach, each router is required to generate a separate tree for each combination of source and group.
- Suppose in the Internet there are m number of groups and n number of sources. Then a router need to generate (m × n) routing trees.
- In each tree, source is the root, the members of the 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.

7.41 Intradomain Routing Protocols :

- During the recent past many new multicast routing protocols have been designed. Some of them have been obtained by extending their unicast counter parts while some are totally new.
- Fig. 7.41.1 shows the classification of intradomain routing protocols.



(G-518(a)) **Fig. 7.41.1 : Multicast routing protocols**

7.42 MOSPF :

- The long form of **MOSPF** is **Multicast Open Shortest Path First** and it is extension of the OSPF protocol.
- This protocol needs a new link state update packet to associate the unicast address of a host with group address or addresses that are sponsored by the host. Such a packet is called as group membership LSA.
- Thus only the hosts which belong to a particular group are included in the tree. All these hosts are included with their unicast addresses.
- In order to improve efficiency, the router calculates the shortest path trees when it receives a multicast packet.
- MOSPF is a data driven protocol. It uses the Dijkstra shortest path algorithm to obtain its shortest path tree.

7.43 Multicast Distance Vector : DVMRP :

- The unicast distance vector routing is simple but multicast distance vector routing is complicated. It does not allow a router to send its routing tables to the neighbouring routers.
- Instead these routers have to construct their own routing tables from scratch by using the information from the unicast distance vector tables.

Scanned by CamScanner

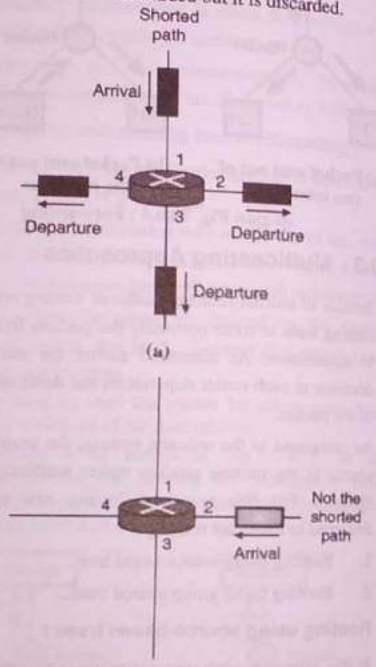
- Multicast distance vector routing makes use of the data based trees however the router actually does not prepare a routing table.
- So we can say that the shortest path tree is evanescent. After its use i.e. when the packet is forwarded, the table is destroyed.
- The multicast distance vector algorithm can achieve this by using a process based on four decision making strategies. They are as follows :
  1. Flooding
  2. Reverse path forwarding
  3. Reverse path broadcasting
  4. Reverse path multicasting.

1. Flooding :

- When a router receives a packet, without looking at the destination group address it sends the packet to every interface except the one from which the packet has been received.
- But this is not multicasting, this is broadcasting. Another problem is that it gives rise to looping problems. That means the same packet may return to the same router from some other interface and may get forwarded again.
- Some flooding protocols avoid loops by keeping a copy of the packet for sometime and by discarding any duplicates.
- This problem can be corrected by using the next strategy i.e. reverse path forwarding (RPF).

2. Reverse Path Forwarding (RPF) :

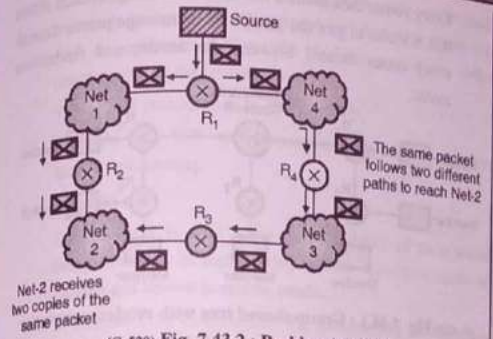
- RPF is modified flooding. It avoids looping by forwarding only one copy and dropping all others.
- In RPF, a router forwards the copy that has travelled the shortest path from the source to the router. To find if the packet has travelled the shortest path, RPF uses the unicast routing table of DVRP. Note that the unicast routing table is based on the destination address and not the source address, therefore DVMRP understands the destination address as the source address.
- Recall that a DVRP table gives the router departure information: specifically, the shortest path to the destination. In DVRMP, the router reverses the roles of the destination and the source. The router uses the source address of the packet (which is a unicast address) to find the corresponding departing interface in the routing table (as if it wants to send a packet to that address).
- If the departing interface found in the table is the same as the interface from which the packet is arriving, then it is an indication that the packet has traveled the shortest path. In other words, since the path from the router to the source is the shortest, the path from the source to the router will also be the shortest because the metrics in distance vector routing (hop counts) are symmetric.
- In Fig. 7.43.1(a), the packet arrives at interface 1 of the router from the shortest path. Hence this packet is forwarded. But in Fig. 7.43.1(b) the packet arriving at interface 2 is not forwarded but it is discarded.



(G-519) **Fig. 7.43.1 : Reverse path forwarding**

3. Reverse Path Broadcasting (RPB) :

- RPF guarantees that each network would receive a copy of the multicast packet without formation of loops. But, RPF does not guarantee that each network would receive only one copy of the intended packet i.e. a network may receive two or more copies of the same packet. The reason is that forwarding is not based on the destination address (a group address); instead it is based on the source address.
- This problem of RPF has been demonstrated in Fig. 7.43.2. In Fig. 7.43.2 the packet created by the source travels two different paths and hence two copies of the same packet reach Net-2.

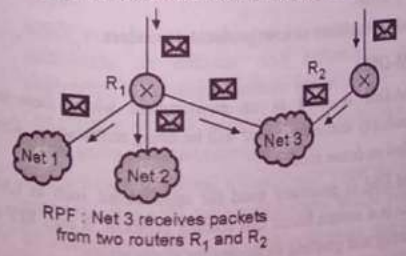


(G-520) **Fig. 7.43.2 : Problem in RPF**

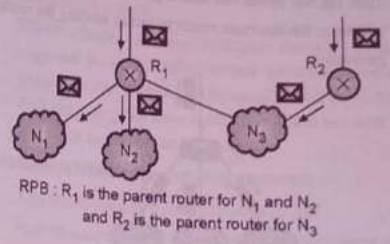
- There duplication takes place because a tree has not been made; instead of a tree we have a graph. Net-2 has two parents : routers R_2 and R_3.
- To eliminate such duplication, we must define only one parent router for each network. A network must receive a multicast packet from any source only through the designated parent router. This restriction needs to be implemented.
- Thus for each source, the router sends the packet only out of those interfaces for which it is the designated parent. This policy is called reverse path broadcasting (RPB), The RPB ensures that the packet reaches every network and that every network receives only one copy of each packet.

Comparison of RPF and RPB :

- Refer Fig. 7.43.3 which demonstrates the difference between RPF and RPB.
- The question is how to determine the designated parent router ? The answer is that the router with shortest path to the source can be the designated parent router.
- In RPB, routers send update packets to each other on the periodic basis. They can find out which neighbouring router has the shortest path to the source.
- If more than one routers qualify to be the parent router, then the router with smallest IP address is selected.



(a) RPF



(b) RPB

(G-521) **Fig. 7.43.3 : Difference between RPF and RPB**

4. Reverse Path Multicasting (RPM) :

- You must have noted that RPB broadcasts the packets. It does not multicast them. This is not an efficient way of routing. The efficiency can be increased by ensuring that the multicast packets reach only those networks which have the active members of that particular group. This is called as **Reverse Path Multicasting (RPM)**.

Path Multicasting (RPM) :

- In order to convert the broadcasting to multicasting the RPM uses two procedures as follows :
  1. Pruning and 2. Grafting
- The concept of pruning and grafting is demonstrated in Fig. 7.43.4.

Pruning :

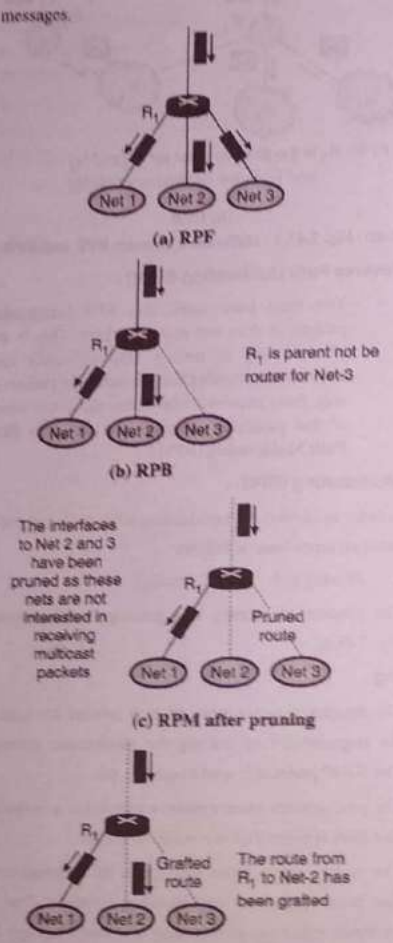
- The designated parent router of each network has been given the responsibility of holding the membership information. The IGMP protocol is used to achieve this.
- The process starts when a router connected to a network finds that there is no interest in a multicast packet.
- The router sends a prune message to the upstream router so that it can prune the corresponding interface. That is, the upstream router can stop sending multicast messages for this group through that interface.
- Now if this router receives prune messages from all downstream routers, it, in turn, sends a prune message to its upstream router.

Grafting :

- The router at the bottom of the tree is known as the leaf router.
- Assume that a leaf router sends a prune message and after sending the message it suddenly realizes that one of the networks connected to it is interested to receive the multicast packet.

Scanned by CamScanner

- Then the leaf router can send a **graft message**. This message will force the upstream router to restart sending the multicast messages.



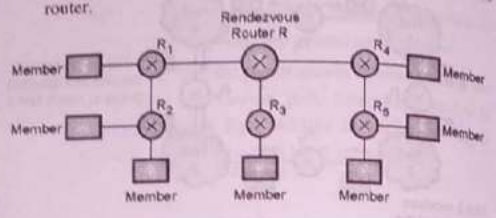
(G-522) **Fig. 7.43.4 : Concept of pruning and grafting**

7.44 Core Based Tree (CBT) Protocol :

- The CBT is a group shared protocol. It uses the core as root of the tree. The autonomous system is divided into different regions and a core router or rendezvous router is selected for each region.

Formation of the tree :

- The first step is to select the rendezvous point. After that the unicast address of the selected router is informed to all the routers.
- Every router then sends a unicast join message (which shows that it wants to join the group). This message passes through every router located between the sender and rendezvous router.



(G-523) **Fig. 7.44.1 : Group shared tree with rendezvous router**

- All these intermediate routers will extract the necessary information from the joining message sent by each sender.
- The tree is formed when the rendezvous router receives the join messages from all the senders, i.e. members of groups.
- If a router wants to leave the group then it has to send a **leave message** to its upstream router. Fig. 7.44.1 shows the group shared tree alongwith the rendezvous router.

Sending Multicast Packets :

- Once the tree is formed, any source that is belonging to the group or an outsider can send packets to all the members of the group.
- To do so, it sends the packet to the rendezvous router using the unicast address of that router.
- The rendezvous router then distributes the packet to all the members of the group.

Selection of Rendezvous Router :

- The selection of rendezvous router to optimize the process and multicasting is not a simple process.

7.45 PIM (Protocol Independent Multicast) :

- This is the name given to two independent multicast routing protocols :
  1. Protocol Independent Multicast Desne Mode (PIM-DM) and
  2. Protocol Independent Multicast, Sparse Mmode (PIM-SM).
- Both of them are unicast protocol dependent.

1. **PIM-DM :**

- PIM-DM is used in an environment where there is a possibility that each router will be doing multicasting. This is called as dense mode.
- PIM-DM is generally used for applications such as LANs. This is a source based tree routing protocol. It uses RPF and pruning and grafting strategies for multicasting.

- It works on the basis of the assumption that the autonomous system is using a unicast protocol and that each router can find an optimum path to the destination at each router interface (using the router table).
- The unicast protocol can be RIP or OSPF.
- PIM-DM uses RPF and pruning and grafting strategies to handle multicasting.

2. **PIM-SM :**

- This protocol is used when the probability of each router being involved in multicasting is very less. This mode of operation is known as **sparse mode.**
- In this working environment the broadcasting protocol can not be used. Instead a protocol like CBT is preferable.
- PIM-SM is a group-shared three routing protocol. It has rendezvous point (RP) at the source of the tree.
- One of the important characteristics of PIM-SM is that it can switch from a group shared tree strategy to a source based tree strategy as and when necessary.
- PIM-SM is similar to CBT but it uses simpler procedure.

7.46 MBONE (Multicast Backbone) :

- The need of multicasting has increased in internet due to multimedia and real time communication.
- But a very small number of internet routers are multicast routers. Therefore **tunnelling** is used to overcome this problem.
- A logical tunnel is established by encapsulating the multicast packet inside a unicast packet. The only protocol that supports MBONE and tunnelling is DVMRP.

7.47 Interdomain Routing Protocols :

- To provide multicast communication inside AS (autonomous system), three protocols DVMRP, MOSPF and PIM are designed which we have discussed in earlier section.
- Interdomain multicast routing protocols are used when the members of the group are spread among different domains.
- MBGP (Multicast Border Gateway Protocol) is commonly used interdomain multicast routing protocol which is extension of BGP which we have discussed earlier in this chapter.
- MBGP provides two paths, one for unicasting and one for multicasting. in different ASS information related to multicasting is exchanged between border routers.
- One router in each AS is selected as core router as a MBGP is shared group multicast routing protocol.
- It is not easy to inform a core router about the sources of groups in other AS is main problem with MBGP protocol.
- To inform about the presence of sources in that AS a new protocol MSDP (multicast source discovery protocol) is suggested which allocates a source core router in each AS (autonomous system).
- BGMP (Border Gateway Multicast Protocol) is another suggested protocol which allows construction of shared group trees with a single root in one of the AS i.e. In different ASS, for each group there is only one shared tree with leaves and root is located in one of the ASS.

Problems in interdomain routing protocols :

1. As a root of the tree, how to designate an AS.
2. How all sources should be informed about location of the root to tunnel their multicast packets.

7.48 IPv6 (Next Generation IP) :

MU : Dec. 07

University Questions

Q. 1 Write notes on IPv6. **(Dec. 07, 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.

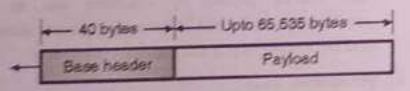
   Address space of IPv6 = (2^{128})
3. **New options :**
   - IPv6 has increased functionality due to the addition of entirely new options that are absent in IPv4.
4. **More security :**
   - IPv6 includes security in the basic specification. It includes encryption of packets (ESP: Encapsulated Security 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.

Scanned by CamScanner

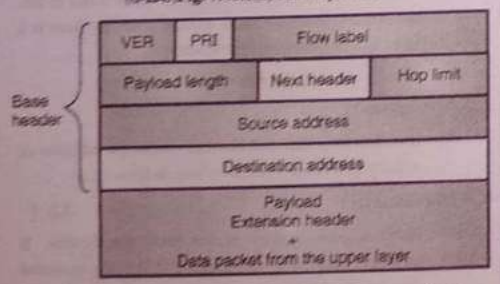
6. **Support to resource allocation :**
   - To implement better support for real time traffic (such as video conference), IPv6 includes flow label in the specification. With flow label mechanism, routers can recognize to which end-to-end flow the given packet belongs to.
7. **Plug and play :**
   - IPv6 includes plug and play in the standard specification. It therefore must be easier for novice users to connect their machines to the network, it will be done automatically.
8. **Clearer specification and optimization :**
   - IPv6 follows good practices of IPv4, and omits flaws/obsolete items of IPv4.

7.48.1 IPv6 Packet Format :

- Fig. 7.48.1(a) shows IPv6 packet. Fig. 7.48.1(b) shows the packet format (Base header) of IPv6. Each packet can be divided into two parts viz : base header and payload.
- Base header is the mandatory part and payload is an optional one. The payload follows the base header.
- The payload is made up of two parts.
  1. An optional extension headers and
  2. The upper layer data.
- The base header is 40 byte long whereas the payload consisting of the extension header and upper layer data can have information worth upto 65, 535 bytes.



(G-2245) **Fig. 7.48.1(a) : IPv6 packet**



(G-556) **Fig. 7.48.1(b) : Format of an IPv6 datagram (Base header)**

Base header :

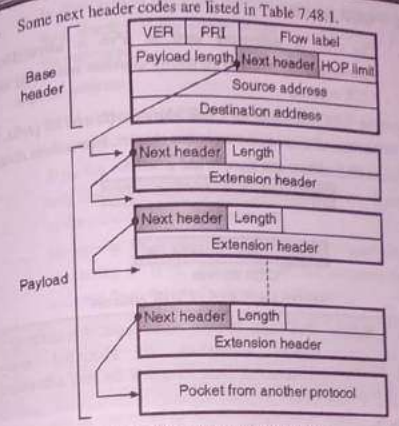
Fig. 7.48.1(b) shows the base header. It has eight fields. These fields are as follows :

1. **Version (VER) :** The contents of this 4 bit field defines the version of IP such as IPv4 or IPv6. If VER = 6, then the version is IPv6.
2. **Priority :** This 4 bit field contents defines the priority of the packet which is important in connection with the traffic congestion.
3. **Flow label :** It is a 24 bit (3 byte) field which is supposed to provide a special handling for a particular flow of data.
4. **Payload length :** The contents of the 16 bit or 2 byte length field are used to indicate the total length of the IP datagram excluding the base header. That means it gives the length of only the payload part of the datagram.
5. **Next header :** It is an 8 bit field which defines the header which follows the base header in the datagram.
6. **Hop limit :** Contents of this 8 bit (1 byte) field have the same function as TTL (time to live) in IPv4.
7. **Source address :** It is a 16 byte (128 bit) Internet address which corresponds to the originator or source which has produced the datagram.
8. **Destination address :** This is a 16 byte (128 bit) internet address which corresponds to the address of the final destination of datagram. But this field will contain the address of the next router and not the final destination if source routing is being used.

7.48.2 Payload :

- The meaning and format of payload field in IPv6 is different as compared to payload field in IPv4.
- Fig. 7.48.2 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 7.48.1.



(G-2246) **Fig. 7.48.2 : IPv6 payload**

Table 7.48.1 : Next header codes

Sr. No.	Code	Next header code
1.	00	HOP by hop option
2.	02	ICMPv6
3.	06	TCP
4.	17	UDP
5.	43	Source routing option
6.	44	Fragmentation option
7.	50	Encrypted security payload
8.	51	Authentication header
9.	59	Null (no next header)
10.	60	Destination option

7.49 IPv6 Addressing :

- IPv6 is the next generation Internet Protocol designed as the next step of the IP version 4. IPv6 was designed to enable high-performance and larger address space. This was achieved by overcoming many of the weaknesses of IPv4 protocol and by adding several new features.
- The IPv6 was developed due to the address depletion of IPv4.
- The structure of IPv6 address is fundamentally different than that of IPv4. Therefore there is absolutely no possibility of address depletion taking place in future.

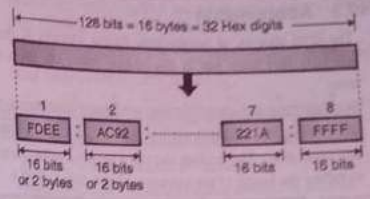
7.49.1 IPv6 Address :

MU : Dec. 07

University Questions

Q.1 Write notes on IPv6. (Dec. 07, 5 Marks)

- An IPv6 address is 128 bit long. It consists of 16 bytes as shown in Fig. 7.49.1. Thus the IPv6 address is 4 times longer than that of IPv4.



(G-545) **Fig. 7.49.1 : IPv6 address**

7.49.2 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 × 4 = 32 hexadecimal digits. These are in groups of 4 digits as shown and every group is separated by a colon as shown in Fig. 7.49.2.

AC 81 : 9840 : 0086 : 3210 : 000A : BBFF : 0000 : FFFF

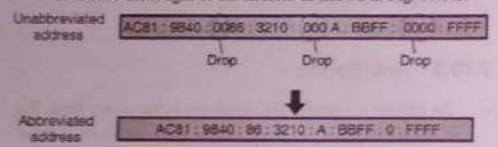
Fig. 7.49.2 : Colon hexadecimal notation

   - 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.

Scanned by CamScanner

7.49.3 Abbreviation :

- The IPv6 address, in hexadecimal format contains 32 digits and it is very long. But in this address many hex digits are zero.
- We can take advantage of this to shorten the address by abbreviating it. A section corresponds to four digits between any two colons. The leading zeros in a section can be omitted to reduce the length of the address as shown in Fig. 7.49.3.

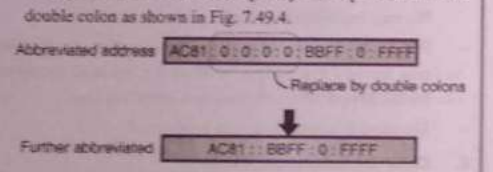


(G-546) **Fig. 7.49.3 : Abbreviated address**

- Note that only the leading zeros can be dropped but the trailing zeros can not be dropped. This is illustrated in Fig. 7.49.3. Thus due to abbreviation the length of the address has reduced to 24 hex digits from 32.

Further abbreviation :

- We can make further abbreviation if there are consecutive sections consisting of only zeros. This is known as **zero compression.**
- We can remove the zeros completely and replace them with double colon as shown in Fig. 7.49.4.



(G-547) **Fig. 7.49.4 : Further abbreviation (Zero compression)**

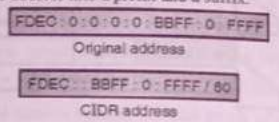
- This further abbreviation has reduced the address length to just 13 hex digits.
- It is important to note that abbreviation can be done only once per address. Also note that if there are two sets of zero sections, then only one of them can be abbreviated.

3. Mixed representation :

- Sometimes, the IPv6 address is represented using a mixed representation which combines the **colon hex** and **dotted decimal** notations.
- This notation is appropriate during the transition time during which an IPv4 address is being embedded in IPv6 address.
- In the mixed representation the rightmost 32 bits correspond to the IPv4 address Hence they are represented by the dotted decimal notation.
- Whereas the leftmost 96 bits (6 sections) are represented in colon hex notation.

4. CIDR notation :

- The type of addressing used in IPv6 is **hierarchical addressing.** Therefore IPv6 allows classless addressing and CIDR notation.
- Fig. 7.49.5 illustrates the CIDR address with a 60 bit prefix. It has been discussed later on in this chapter, how we can divide an IPv6 address into a prefix and a suffix.



(G-2132) **Fig. 7.49.5 : CIDR address**

Ex. 7.49.1 : 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

$$\therefore x = 3.4 \times 10^{38}$$

$$\therefore x = \frac{3.4 \times 10^{38}}{1 \times 10^{6}} \times 1 \text{ picoseconds}$$

$$= 3.4 \times 10^{32} \text{ picoseconds}$$

$$= 3.4 \times 10^{20} \text{ seconds}$$

$$= 9.44 \times 10^{16} \text{ hours}$$

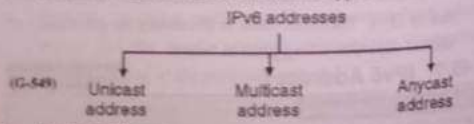
$$= 3.9352 \times 10^{15} \text{ days} = 1.0781 \times 10^{13} \text{ years}$$

7.50 Address Space :

- The address space of IPv6 contains 2^{128} addresses which is a very big number. If we compare it with the address space of IPv4, then it can be seen that, the address space of IPv6 is 2^{96} times bigger than that of IPv4.
- Therefore there is no possibility of address depletion in IPv6.

7.50.1 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.

3. Multicast addresses :

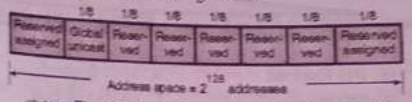
- A multicast address defines a group of computers which may or may not share the same prefix and may or may not be connected to the same physical network.
- A packet sent to a multicast address is meant to be delivered to each member of the group.
- There are no broadcast addresses in IPv6, because multicast addresses can perform the same function. The type of address is determined by the leading bits.
- All the multicast addresses start with FF (1111 1111) and all other addresses are unicast addresses.
- Anycast addresses are assigned from the unicast address space and they do not differ syntactically from unicast addresses.
- Anycast addressing is a rather new concept and there is not much experience about the widespread use of anycast addresses.
- Therefore, some restrictions apply to anycast addressing in IPv6 until more experience is gained.
- An anycast address may not be used as the Source Address of an IPv6 packet and anycast addresses may not be assigned to hosts but to routers only.
- As will be discussed later, a block is designated for multicasting in IPv6, from which the same address is assigned to the members of the group.

7.50.2 Broadcasting and Multicasting :

- In IPv6 the broadcasting is not defined at all, as in case of IPv4. In IPv6 broadcasting is considered as a special case of multicasting.

7.51 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 shown in Fig. 7.51.1.

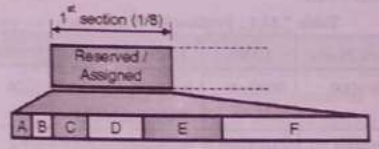


(G-2133) **Fig. 7.51.1 : Address space allocation in IPv6**

- As shown in Fig. 7.51.1, the number of addresses in each section is one eighth of the total address space. So number of addresses in each section is equal to 2^{125} addresses.

7.51.1 The First Section :

- The first section is market as Reserved/Assigned in Fig. 7.51.2. That means some address blocks in this section are reserved and the remaining are assigned as shown in Fig. 7.51.2(a).



A : 1/256 IPv4 compatible. D : 1/64 Reserved.
B : 1/256 Reserved. E : 1/32 Reserved.
C : 1/128 Reserved. F : 1/16 Reserved.

(G-2134) **Fig. 7.51.2(a) : The first section**

- As shown in Fig. 7.51.2(a), the first section is divided in six blocks of variable sizes (blocks A to F). Out of these six blocks, three blocks have been reserved and remaining three are not assigned.

7.51.2 Second Section :

- The second section is not divided into blocks. So it is considered as one single block and is used for the **global unicast** addresses.

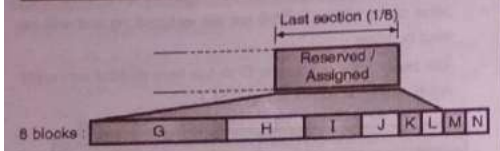
Sections three to seven :

These five sections from third to seventh are unassigned.

Last section :

- The last section in Fig. 7.51.2 which is marked as Reserved /Assigned is further divided into eight blocks of different sizes as shown in Fig. 7.51.2(b).
- Some of these blocks are not assigned while the other blocks are reserved for some special purpose as shown in Fig. 7.51.2(b).

Scanned by CamScanner



G : 1/16 Reserved.
H : 1/32 Reserved.
I : 1/64 Reserved.
J : 1/128 Unique local unicast
K : 1/512 Reserved.
L : 1/1024 Link local
M : 1/256 Reserved.
N : 1/256 Multicast.

(G-2135) **Fig. 7.51.2(b) : The last section**

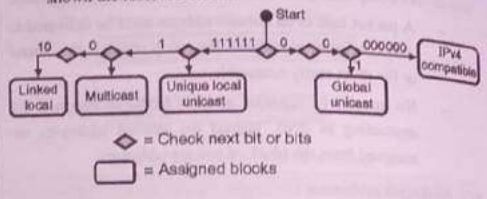
- From all this discussion it is very clear that out of the total address space of IPv6 more than 5/8th of the space is still not assigned, and only 1/8th of the address space has been assigned for the global unicast addresses for unicast communication between the users.
- The prefix for each type of address has been shown in Table 7.51.1.

Table 7.51.1 : 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

7.51.3 Algorithm :

- The diagram shown in Fig. 7.51.3 has been created to illustrate that the prefixes given in Table 7.51.1 really find the block to which the IPv6 address belongs to.
- Note that, in order to make this diagram simpler we have not shown the reserved blocks.



(G-2136) **Fig. 7.51.3 : An algorithm to find the allocated blocks**

7.51.4 Assigned or Reserved Blocks :

- In this section, we are going to discuss the purposes and characteristics of the reserved as well as assigned blocks starting from the first row of Table 7.51.1.

1. IPv4 compatible addresses :

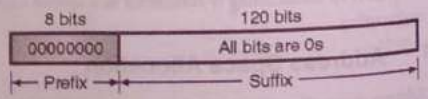
- The addresses which use the prefix (00000000) are reserved, however a part of it is used for defining some IPv4 compatible addresses.
- There are 2^{120} addresses in this block because it occupies 1/256 the fraction of the total address space.
- This block can be defined using CIDR notation as follows :

  0000::/8

- This address block is further divided into many smaller subblocks. We will discuss them later in this chapter.

7.51.5 Unspecified Address :

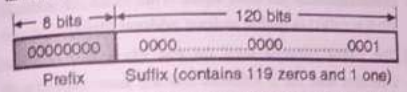
- The unspecified address is a subblock which contains only one address. By letting all suffix bits to zero, this address can be defined. That means this address is an all zeros address.
- During the bootstrapping process, when a host does not know its own address, the unspecified address is used to send an enquiry to find the unknown address of the host.
- This address is used by the host as a **source address.** However it is important to note that the unspecified address cannot be used as the **destination address.**
- This one-address subblock can be represented as ::/128 in the CIDR notation, and its format has been shown in Fig. 7.51.4.



(G-2137) **Fig. 7.51.4 : Format of the unspecified address**

7.51.6 Loopback Address :

- Like the previous one, this subblock also contains only one address which a host uses for testing itself without going into the network.
- Here the application layer creates an address, sends it to the transport layer and then passes it to the network layer.
- However it does not go to the physical layer. Instead, it returns to the transport layer and finally passed on to the application layer.
- This feature is very useful because using it we can test the functions of software package in these layers even before the computer is connected to the network.
- Fig. 7.51.5 shows the format of the loopback address which has the prefix of 00000000 and a suffix containing 119 zeros and one 1.
- We can represent this address in the CIDR notation as ::1/128.



(G-2138) Fig. 7.51.5 : **Format of the loopback address**

7.51.7 Difference between Loopback Address of IPv4 and IPv6 :

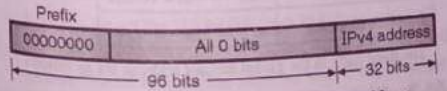
- In IPv4 classful addressing, the loop back addresses get a whole block allotted to them but in IPv6 loopback addresse is only one single address.
- In IPv4 the loop back addresses are accommodated as a part of class A address but in IPv6 it is only one single address in the reserved block.

7.51.8 Embedded IPv4 Addresses :

- As discussed in the migration from IPv4 to IPv6 in this transition period, the hosts can continue to use their IPv4 address which are embedded in IPv6 addresses.
- In order to achieve this, IPv6 has designed two formats namely **compatible format** and **mapped** format.

7.51.9 Compatible Address :

- The compatible address is an IPv6 address with 96 bits of zeros followed by 32 bits of IPv4 address.
- Fig. 7.51.6 shows the format of IPv6 compatible address.

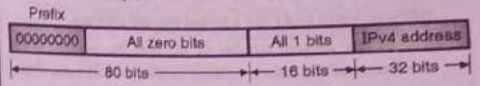


(G-2139) **Fig. 7.51.6 : Format of compatible address**

- The situation in which the compatible address is required to be used is as follows : If an IPv6 host wants to communicate with another IPv6 host but the packet is going to pass through a region in which still the IPv4 is being used by the networks.
- In order to ensure a successful passage of this packet the sender will have to use the **compatible address.**
- This is a reserved subblock which contains 2^{32} addresses and has a CIDR notation of ::/96.

7.51.10 A Mapped Address :

- The format of a mapped address is shown in Fig. 7.51.7. It shows that this address consists of 80 bits of zeros, followed by 16 bits of 1s, followed by 32 bits of IPv4 address.
- It is used when an IPv6 computer wants to communicate with an IPv4 computer.



(G-2140) **Fig. 7.51.7 : Mapped address**

- This packet can travel for an IPv6 guest, through a mostly IPv6 network and finally delivered to an IPv4 destination host.

7.51.11 Calculation of Checksum :

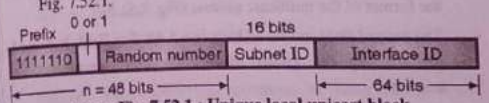
- The compatible and mapped addresses have been designed in such a way that the checksum can be calculated by either using the embedded address or the complete address because the extra zeros and ones are in multiples of 16. Hence they do not affect the checksum calculation in any way.
- So the value of checksum remains same even if the packet address is changed from IPv6 to IPv4.

7.52 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.**

7.52.1 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. 7.52.1.



(G-2141) **Fig. 7.52.1 : Unique local unicast block**

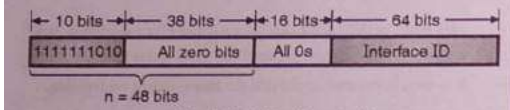
- We will discuss the first type i.e. the one which is reserved at the site in this section and the other one in the next section.

Scanned by CamScanner

- Refer Fig. 7.52.1 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. 7.52.1. 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.

7.52.2 Link Local Block :

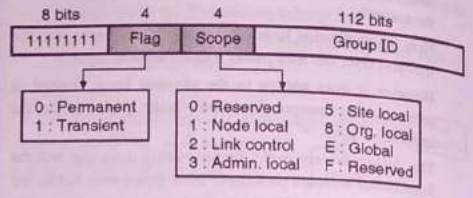
- Link local block is the second block designed for private addresses. It is possible to use a subblock in this block as a private address in a network.
- The format of the link local address is as shown in Fig. 7.52.2. The first 8 bit block consists of the block identifier which is 1111111010 for this type of address.
- 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. 7.52.2 : Link local address**

7.52.3 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. 7.52.3).
- 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. 7.52.3.



(G-2143) **Fig. 7.52.3 : Format of multicast address**

7.53 Global Unicast Address :

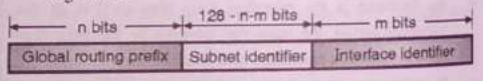
- This block is present in the address space. It is used by two hosts in the Internet for the unicast (one to one) communication between them. This block of addresses in IPv6 is called as **global unicast address block.**
- The CIDR notation used for this block is 2000::/3 which indicates that the 3 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.

7.53.1 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. 7.53.1.



(G-2144) **Fig. 7.53.1 : Global unicast address**

- The recommended values for the lengths of the three blocks shown in Fig. 7.53.1 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 :

7.53.2 Global Routing Prefix :

- As shown in Fig. 7.53.1, 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. 7.53.1, 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. 7.53.1).
- 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.

7.53.3 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.

7.54 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.

7.54.1 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.

Scanned by CamScanner

7.54.2 Comparison between IPv4 and IPv6 :

MU : May 10, Dec. 11

University Questions

Q. 1 Explain IPv4 protocol and differentiate with IPv6 protocol. **(May 10, 10 Marks)**

Q. 2 Explain difference between IPv4 and IPv6. **(Dec. 11, 5 Marks)**

IPv4	IPv6
In IPv4 there are only 2^{32} possible ways to represent the address (about 4 billion possible addresses)	In IPv6 there are 2^{128} possible way (about 3.4×10^{38} possible addresses)
The IPv4 address is written by dotted-decimal notation, e.g. 121.2.8.12	IPv6 is written in hexadecimal and consists of 8 groups, containing 4 hexadecimal digits or 8 groups of 16 bits each, e.g. FABC: AC77: 7834:2222:FACB: AB98: 5432:4567.
The basic length of the IPv4 header comprises a minimum of 20 bytes (without option fields). The maximum total length of the IPv4 header is 60 bytes (with option fields), and it uses 13 fields to identify various control settings.	The IPv6 header is a fixed header of 40 bytes in length, and has only 8 fields. Option information is carried by the extension header, which is placed after the IPv6 header.
IPv4 header has a checksum, which must be computed by each router	IPv6 has no header checksum because checksums are, for example, above the TCP/IP protocol suite, and above the Token Ring, Ethernet, etc.
IPv4 contains an 8-bit field called Service Type. The Service Type field is composed of a TOS (Type of Service) field and a precedence 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.

7.54.3 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. 7.54.1).
- There are a small number of such extension headers, each identified by a distinct Next Header value. An IPv6 packet may carry zero, one, or more extension headers, each identified by the Next Header field of the preceding header. There are seven kinds of extension header :

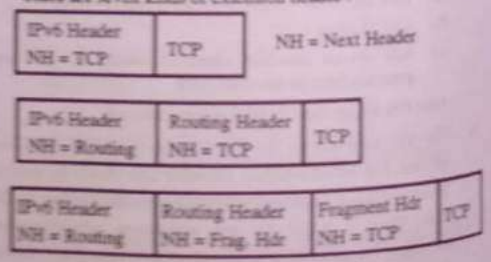


Fig. 7.54.1 : Examples of headers chain

- 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 :

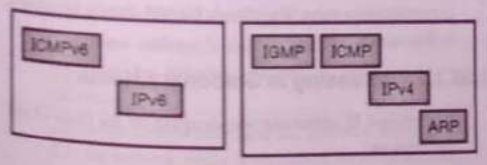
- The fragmentation in IPv6 is conceptually same as that discussed for IPv4, but the fragmentation in IPv6 takes place at a different place than that in IPv4.
- In IPv4 the fragmentation is done by the source or router, but in IPv6 the fragmentation may be carried out only by the original source.

2. Authentication and Privacy :

- IPv6 provides authentication and privacy using options in the extension header.

7.55 ICMPv6 (Internet Control Message Protocol) :

- As compared to ICMPv4, ICMPv6 is more complicated. In ICMPv6 some protocols are part of it which were independent in version 4 and some useful messages have been added in ICMPv6.
- Fig. 7.55.1 gives the comparison of network layer in version 4 and version 6.



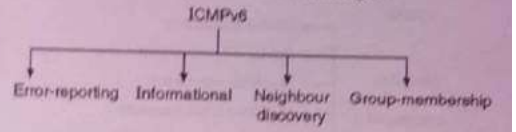
(a) Network layer in version 6 (b) Network layer in version 4

(G-2247) **Fig. 7.55.1 : Comparison**

- ICMPv6 is combination of three protocols (ICMP, ARP, IGMP) in version 4.

7.55.1 ICMPv6 Messages :

- Fig. 7.55.2 shows types of ICMPv6 messages.

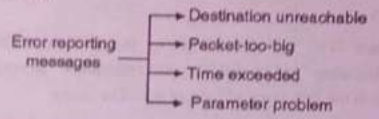


(G-2248) **Fig. 7.55.2 : ICMPv6 messages**

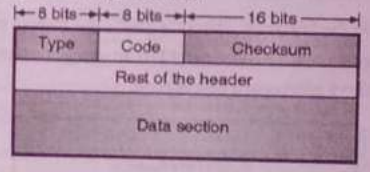
1. Error reporting messages :

- This type of messages follow the same policy as in version 4.

(G-2249)



- In version 6, fragmentation is not allowed for a router, hence packet-too-big is added.
- In case of too big message, a router will drop this message and to the source a router will send **packet-too-big** error message (Refer Fig. 7.55.3(a)).

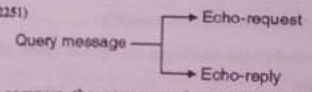


(G-2250) **Fig. 7.55.3(a) : Error reporting messages**

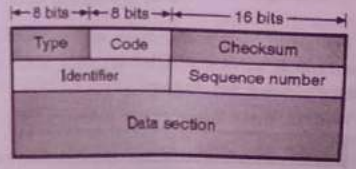
2. Informational messages :

- The query messages in version 4 and informational messages in version 6 plays the same role.

(G-2251)



- If we compare the messages in version 4, two messages timestamp request and timestamp reply have been dropped as they were used rarely.



(G-2252) **Fig. 7.55.3(b) : Informational messages**

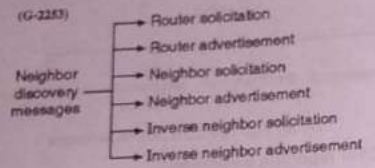
3. Neighbour discovery messages :

- This is new group of message added in version 6.
- The messages in this group can be used :
  1. To find routers in the neighborhood.
  2. To find link layer addresses of other hosts in the neighborhood.

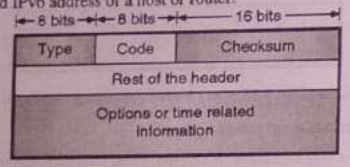
Scanned by CamScanner

3. To find IPv6 addresses of the hosts in the neighborhood.
4. Redirect messages.

(G-2253)



- The **router solicitation** and **router advertisement** messages are useful for host to search a default router to forward its packet.
- When IPv6 address is given, two messages **neighbor solicitation** and **neighbor advertisement** messages can search the link layer address of a host or router.
- In version 4, this task is done by ARP (address resolution protocols) which we have discussed earlier.
- The function of **redirection message** is same as we have discussed in version 4.
- When the link layer address is given, **the inverse neighbor solicitation** and **inverse neighbor advertisement** are used to find IPv6 address of a host or router.

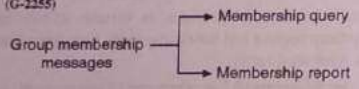


(G-2254) **Fig. 7.55.3(c) : Neighbor discovery messages**

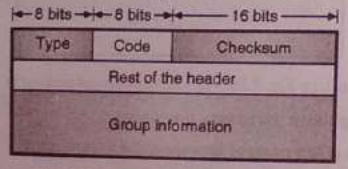
4. Group-membership messages :

- Group-membership messages are used in multicasting.

(G-2255)



- The function of membership query and membership report messages in ICMPv6 and IGMP are same which we have discussed earlier in this chapter.



(G-2256) **Fig. 7.55.3(d) : Group membership messages**

- Table 7.55.1 (a) to (d) shows type of messages and code values.

Table 7.55.1(a) : Error reporting messages

Sr. No.	Code	Type of message
1.	01	Destination unreachable (Code 0 to 6)
2.	02	Packet too big (Code 0)
3.	03	Time exceeded (Code 0 and 1)
4.	04	Parameter problem (Code 0 and 2)

Table 7.55.1(b) : Informational messages

Sr. No.	Code	Type of message
1.	128	Echo-request (0)
2.	129	Echo-reply (0)

Table 7.55.1(c) : Neighbor discovery messages

Sr. No.	Code	Type of message
1.	133, 134	Router solicitation and advertisement (0)
2.	135, 136	Neighbor solicitation and advertisement (0)
3.	137	Redirection (0 to 3)
4.	141, 142	Inverse neighbour solicitation and advertisement (0)

Table 7.55.1(d) : Group membership messages

Sr. No.	Code	Type of message
1.	130	Membership query (0)
2.	131	Membership report

7.56 Mobile IP :

- Mobile IP is the extension of IP protocol. It has been developed for the mobile and personal computers such as notebook.
- Mobile IP allows the mobile computers to get connected to the Internet at any location.

7.56.1 Addressing :

- Addressing is a very important problem in providing mobile communication using IP protocol. We will discuss its solution in this section.

7.56.1.1 Addressing in Stationary Hosts :

- The original IP addressing was designed on the basis of two assumptions :
  1. The host is stationary.
  2. The host is connected to only one network.
- An IP datagram is routed by the routers on the basis of the IP address.

- As discussed earlier in this chapter, an IP address is made of two parts : a prefix and a suffix.
- A host gets associated with a network due to the prefix part of its IP address. That means a host cannot carry its IP address with itself from one place to the other.
- That means with change in place, the network changes and so does the IP address of the host.
- Routers use the fixed association between a host and its network for routing the packets to the network to which the host is attached.

7.56.1.2 Mobile Hosts :

- The IP addressing structure needs to be changed when a host moves from one network to the other. To achieve this, various solutions have been suggested.
- Two of them are as follows :

1. Changing the address :

- One of the solutions is to allow the mobile host to change its IP address as it changes the network.
- This can be achieved by using DHCP. The mobile host can obtain a new IP address using DHCP and get associated with the new network.
- But this technique has many drawbacks. Some of them are as follows :

Drawbacks :

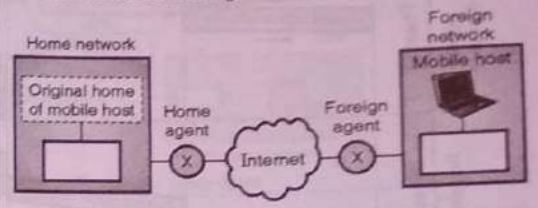
1. We need to change all the configuration files.
2. The mobile host would need rebooting, everytime it moves from one network to the other.
3. It would be necessary to revise the DNS table everytime so that all the other hosts on the Internet are aware of this address change.
4. If the mobile host moves from one network to the other when transmission is taking place, then the exchange of data will be interrupted because during the transmission, the client and server cannot change their port and IP addresses.

2. Two addresses :

- Due to all the drawbacks of the first approach, the second approach of using **two IP addresses** for a mobile host is tried out and it is found to be a more feasible approach.
- The two IP addresses assigned to a mobile host are :
  1. Home address and 2. Temporary address.
- The **home address** is the original IP address of the mobile host, and the temporary address is called as the **care of address.**
- The home address associated the host with its home network (i.e. the network which is permanent home of the host and it is its **permanent** IP address.
- When the host moves to the other network, its temporary (care-of) address changes. This care-of address associates the host with the **foreign network.**

7.56.2 Agents :

- A **home agent** and a **foreign agent** are required for making the change of address transparent to the rest of Internet.
- The position of home agent with respect to the home network and that of the foreign agent with respect to the foreign network are shown in Fig. 7.56.1.



(G-2257) **Fig. 7.56.1 : Home agent and foreign agent**

- In Fig. 7.56.1 the home and foreign agents have been shown as routers. However actually they act as a router as well as a host.

1. Home Agent :

- A home router is basically a router attached to the home network of a mobile host.
- When a remote host sends a packet to the mobile host, the home agent acts on behalf of the mobile host, receives the packet and sends it to the foreign agent.

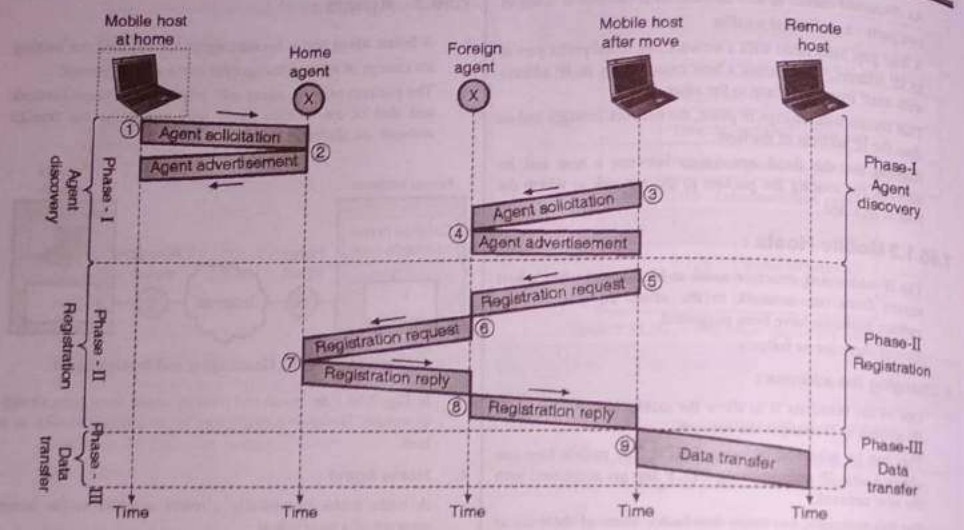
2. Foreign Agent :

- A foreign agent is a router connected to the foreign network.
- The packets sent by the home agent are received by the foreign agent and delivers them to the mobile host.
- Sometimes, a mobile host itself can act as foreign agent. Then there is no need of using a separate foreign agent.
- For this, the mobile host should have the ability to receive a care-of address on its own. This can be done using DHCP.
- In addition to this a special software needs to be installed at the mobile host to enable it to communicate with the home agent and to have the two addresses (home and temporary).
- It is necessary to keep the dual addressing transparent to the application programs.
- The care-of-address is called as **collocated care-of address** if a mobile host itself is acting as the foreign agent.
- The use of collocated care-of address has an advantage that the mobile host can move to any foreign network without even thinking about the availability of the foreign agent.
- However its disadvantage is that an extra software needs to be installed with the mobile host.

7.56.3 Three Phases :

- The communication of a mobile host with a remote host goes through the following three phases :
  1. Agent discovery 2. Registration
  3. Data transfer.
- All these phases are shown in Fig. 7.56.2.

Scanned by CamScanner



(G-2258)Fig. 7.56.2 : Communication between mobile host and remote host

1. **Phase-I : Agent Discovery (Steps 1 to 4) :**

- This is the first phase in mobile communication. It consists of the following two subphases :
  1. Agent solicitation and
  2. Agent advertisement.
- A mobile host must learn the address of (discover) its home agent before moving to any foreign network (Steps 1 and 2). The mobile host must also learn the address of (discover) the foreign agent once it moves to a foreign network (Steps 3 and 4).
- This process of address learning includes learning of both the care-of address and the foreign agents address.
- The agent discovery phase involves the discovery of home and foreign agents. This process requires the use of two messages namely :
  1. Advertisement message and
  2. Solicitation method.

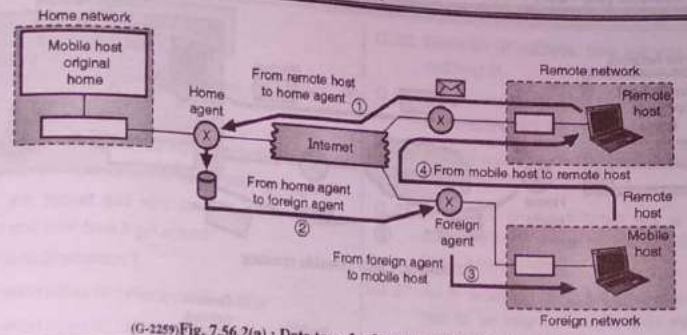
2. **Phase-II : Registration (Steps 5 to 8) :**

- This is the second phase of mobile communication. The mobile host first moves to the foreign network and discovers the foreign agent (Phase-I).
- After this it must undergo the registration phase, which corresponds to steps 5 to 8 in Fig. 7.56.2.
- The four aspects of registration are as follows :
  1. Registration of mobile host with the foreign agent (Step-5).
  2. Registration of mobile host with its home agent. This is normally done by the foreign agent on behalf of mobile host (Step 6).
  3. The mobile host must renew its registration if the registration has expired.
  4. The mobile host is supposed to cancel its registration when it returns back to its home network.
- The **registration request** and **registration reply** messages are used as shown in Fig. 7.56.2 for registration of mobile host with the home agent and foreign agent.

3. **Phase-III : Data Transfer :**

- This is the third phase in mobile communication after the agent discovery and registration. In this phase the mobile host can communicate with the remote host as shown in Fig. 7.56.2.

1. **From Remote Host to Home Agent :**
   - If a packet is to be transferred from the remote host to mobile host, then the remote host uses its address as the **source address** and home address of mobile host as **destination address.**
   - But practically the home agent is pretending as the mobile. So it will intercept the packet with the help of proxy ARP.
   - Thus the communication from remote host to mobile host actually takes place between the remote host and home agent as shown in Fig. 7.56.2.



(G-2259)Fig. 7.56.2(a) : Data transfer from remote host to home agent

   - The mobile communication between the Remote Host and Home agent has been marked by a thick path marked by "1" in Fig. 7.56.2(a).

2. **From Home to Foreign Agent :**
   - As the packet is received by the home agent it sends the packet to the foreign agent using the concept of tunneling.
   - The home agent encapsulates this received IP packet into a new IP packet by using its own address as the source address and foreign agents address as the destination address and sends this new IP packet to the foreign agent as shown by the thick path marked by "2" in Fig. 7.56.2(a).

3. **From Foreign Agent to Mobile Host :**
   - From the IP packet received the foreign agent will recover the original packet by decapsulation process.
   - However the recovered original packet has the home address of mobile host as its destination address.
   - The foreign agent will refer to a registry table and finds the **care-of-address** of the mobile host. The original packet is then sent to the care-of-address as shown by the thick path marked by "3" in Fig. 7.56.2(a).

4. **From Mobile Host to Remote Host :**
   - If a mobile host wants to send a packet to a remote host, it does it in a normal way.
   - To do this, the mobile host creates a packet with its home address (and not the care-of-address) as source address and remote host's address as the destination address.
   - It is very important to note that eventhough the packet originates from the foreign network, it has the home address of the mobile host.
   - This communication has been shown by the thick path "4" in Fig. 7.56.2(a).

7.56.4 Transparency :

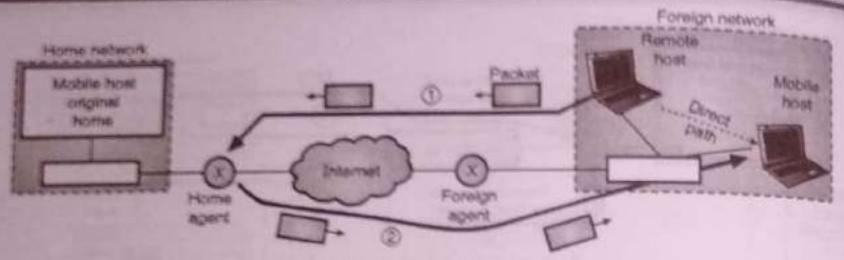
- In the entire data transfer process, the remote host absolutely does not know anything about the movement of the mobile host.
- Because, the remote host uses the home address as the destination address when sending a packet to the mobile host.
- Similarly the mobile host uses its home address as the source address while sending a packet to the remote host.
- In otherwords we say that movement of the mobile host is **totally transparent** because the rest of the Internet has absolutely no idea about the movement of the mobile host.

7.56.5 Inefficiency in Mobile IP :

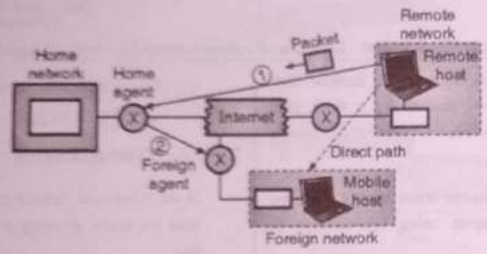
- The communication done with the help of mobile IP can be moderately to severely inefficient.
- The case of moderate inefficiency is also called as the **triangle routing, or dog leg routing** whereas the case of severe inefficiency is also referred to as **Double Crossing** or **2X.**
- We will discuss both these cases in this section.

1. **Double Crossing or 2X :**
   - Now consider a situation in which a remote host wants to communicate with a mobile host which has moved to the same network as that of the remote host as shown in Fig. 7.56.3.
   - This is called as a **double crossing or 2X** case i.e. the case of **severe inefficiency.**

Scanned by CamScanner



(G-2268) Fig. 7.56.3 : Double crossing



(G-2267) Fig. 7.56.4 : Triangle routing

- As discussed earlier, a mobile host can send a packet directly to the remote host. Therefore there is no loss of efficiency in this communication.
- However if the remote host wants to send a packet to the mobile host then it cannot do so directly (via the dotted direct path in Fig. 7.56.3).
- Instead the remote host has to send the packet first home agent (path-1 in Fig. 7.56.3) and the home agent will route the packet to the mobile host (path-2 in Fig. 7.56.3).
- In this the packet has to cross the Internet twice. Thus the resources are used twice unnecessarily in this communication which reduces the efficiency severely.
- Hence the double cross case is called as the case of severe inefficiency.

2. Triangle Routing or Dog Leg Routing :

- A triangle routing or dog leg routing is a case of moderate inefficiency. It occurs when a remote host wants to send a packet to the mobile host which is not attached to its own (remote) network.
- This situation is illustrated in Fig. 7.56.4.
- In this situation as well, if a mobile host wants to send a packet to a remote host it can do so directly without any loss of efficiency.
- But when a remote host wants to send a packet to a mobile host the packet has to first travel to the home agent and then to the mobile host as shown in Fig. 7.56.4.
- Thus the packet has to travel along two sides of a triangle instead of only one which is the direct path shown by a dotted line in Fig. 7.56.4.

7.56.6 Remedy :

- Binding the care-of-address to the home address of mobile could be one of the solutions to the problem of inefficiency.
- That means when the home agent receives the first packet from the remote host and sends it to the foreign agent it should also send an **update binding packet** to the remote host. By doing this it is ensured that all the future packets to this mobile host can be sent to the **care-of-address** rather than **home** address.
- The remote host can save this information in a cache.
- However this remedy also has an inherent flaw. The **cache entry** would become outdated as the mobile host moves to a new network.
- To avoid this the **home agent** must send a **warning packet** to the remote host to inform that the mobile host has moved to a new network.

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.

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 PING utility ? How many ways are there to implement PING ? Explain steps.

Q. 25 What is subnetting in IP network, explain with suitable examples.

Q. 26 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. 27 An IP datagram using the strict source routing option has to be fragmented. Do you think the option is copied into each fragment, or is it sufficient to just put it in the first fragment ? Explain your answer.

Q. 28 How is the addressing done in stationary hosts ?

Q. 29 How is the issue of addressing handled in mobile hosts ?

Q. 30 Explain the "changing the address" strategy in mobile host addressing and state its drawback.

Q. 31 Explain the two address strategy.

Q. 32 Define home agent and foreign agent in mobile IP and explain their roles.

Q. 33 Explain the three phased communication of a mobile host with a remote host in mobile IP.

Q. 34 With the help of a neat illustrative diagram explain the data transfer phase in mobile host to remote host communication.

Q. 35 What is transparency in mobile IP ?

Q. 36 Write a note on : Inefficiencies in mobile IP.

Q. 37 Write short note on : Network layer congestion.

Q. 38 State the difference between multiple unicasting and multicasting.

Q. 39 Explain the concept of multicast address.

Q. 40 Explain DVMRP.

Q. 41 Compare RPF and RPB.

Q. 42 Write short note on ICMPv6.

❑❑❑

Scanned by CamScanner

CHAPTER 8

Module V

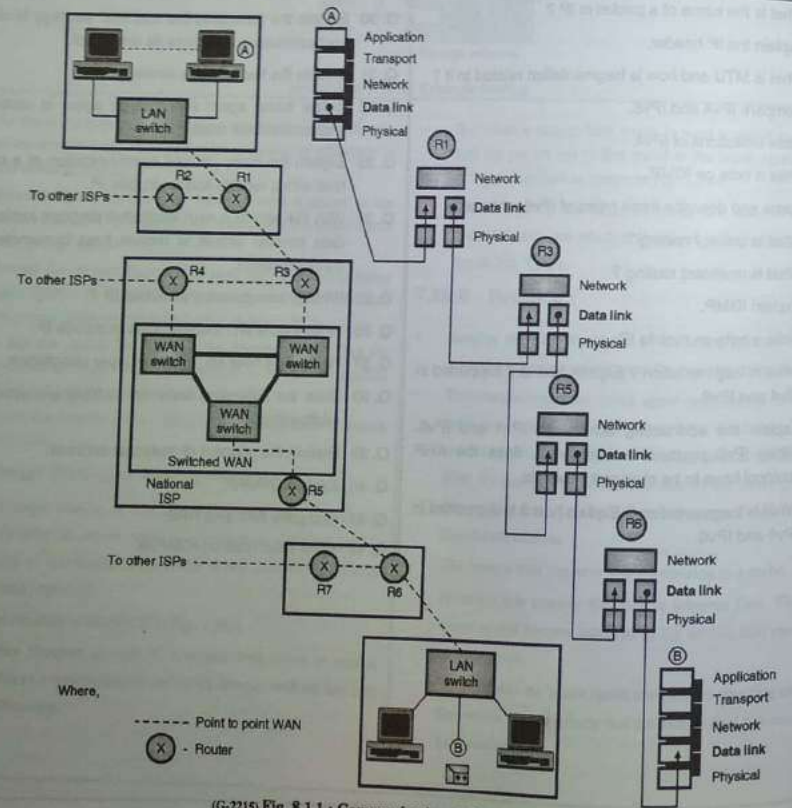
Data Link Layer

Syllabus :

Wired Networks : Introduction : Nodes and links, Two types of links, Two sublayers, Data link control : Framing, Flow and Error control, Error detection and correction, Two DLC protocols.

8.1 Wired Networks :

- In chapter 7, we have seen that communication at the network layer is host to host. It can be reassembled and fragmented.
- From the host, somewhere in the world, datagram (data unit) is sent to another host which is somewhere else in the world.
- A combination of networks attached together with the help of connecting devices such as routers or switches, is nothing but the **Internet.** A datagram needs to pass through these network if they want to travel from one host to another host.



(G-2215) **Fig. 8.1.1 : Communication at data link layer**

- Fig. 8.1.1 shows communication at the data link layer. Fig. 8.1.1 explains communication between two hosts A and B. Communication is provided using five separate logical connections between the data link layers.
- The data link layer at A's computer communicate with the data link layer at router R1. The data link layer at R1 communicate with the data link layer at R3, and so on.
- At last the data link layer at router R6 makes communication with the data link layer at B's computer.
- At the source and destination only one data link layer is involved whereas at each router two data link layers are involved. The reason is that A's and B's computers are connected to a single network however from one network, each router takes input and sends output to other network.

8.2 Analog and Digital Signals :

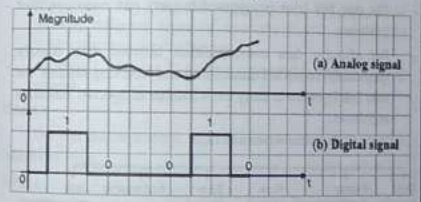
- Signals can be of two types :
  1. Analog signals. 2. Digital signals.

1. Analog signal :

It is the signal in which the signal magnitude varies in a smooth fashion without any break with respect to time, as shown in Fig. 8.2.1(a).

2. Digital signal :

It is the signal in which the signal magnitudes has a constant level for some period of time, then it changes suddenly to another constant level as shown in Fig. 8.2.1(b). The examples of digital signal are binary signal, hexadecimal signal etc.



(L-24) **Fig. 8.2.1 : Types of signals**

8.2.1 Analog and Digital Data :

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

1. Analog data :

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

2. Digital data :

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

8.2.2 Sources of Digital Signal :

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

8.2.3 Advantages of Digital Signals :

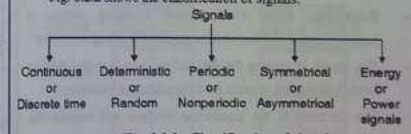
1. Digital signals can be processed and transmitted more efficiently and reliably than analog signals.
2. It is possible to store the digital data.
3. Play back or further processing of the digital data is possible.
4. The effect of "noise" (unwanted voltage fluctuations) is less. So digital data does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

8.2.4 Comparison of Digital and Analog Signals :

Sr. No.	Parameter	Analog signals	Digital signals
1.	Number of values	Infinite	Finite (2, 8, 16 etc.)
2.	Nature	Continuous	Discrete
3.	Sources	Signal generators, transducers etc.	Computers, A to D converters
4.	Examples	Sinewave, triangular wave	Binary signal

8.2.5 Classification of Signals :

- Fig. 8.2.2 shows the classification of signals.



(G-1250) **Fig. 8.2.2 : Classification of signals**

- Out of these we will concentrate only on periodic or non periodic signals.

8.2.6 Periodic and Non-periodic Signals :

Periodic signal :

- A signal which repeats itself after a fixed time period is called as a periodic signal. The periodicity of a signal can be defined mathematically as follows :

$$x(t) = x(t + T_0) \text{ : Condition of periodicity} \quad ...(8.2.1)$$

Where T_0 is called as the period of signal x (t), in other words, signal x (t) repeats itself after a period of T_0 sec.

- Examples of periodic signals are sine wave, cosine wave, square wave etc. Fig. 8.2.3(a) shows a sine wave which is periodic because it repeats itself after a period T_0.

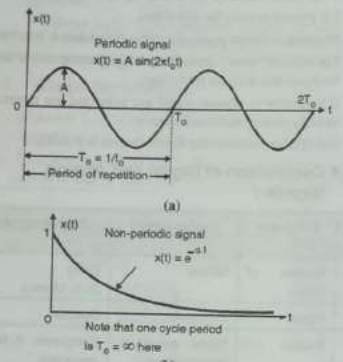
Scanned by CamScanner

Non-periodic signal :

- A signal which does not repeat itself after a fixed time period or does not repeat at all is called as a non-periodic or aperiodic signal.
- The non-periodic signals do not satisfy the condition of periodicity stated in Equation (8.2.1).

∴ For a non-periodic signal $x(t) \neq x(t + T_0)$ ...(8.2.2)

- Sometimes it is said that an aperiodic signal has a period $T_0 = \infty$. Fig. 8.2.3(b) shows a decaying exponential signal.

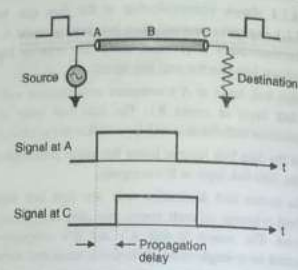


(G-1251) **Fig. 8.2.3 : Periodic and non-periodic signals**

- This exponential signal is non-periodic but it is deterministic because we can mathematically express it as $x(t) = e^{-at}$.

8.2.7 Signal Propagation :

- Refer Fig. 8.2.4 which shows a signal source, a communication channel and the destination or signal receiver.
- The signal containing the data information is in the electric form. It is applied at point A of the conducting medium.
- The electrons in the conducting medium will transfer the charge to the adjacent electrons and the signal at point A gets transferred to B and then to C which is the receiving point.
- The shape of the signal at the receiver (point C) is almost same as that at the source (point A), but the signal reaches point C after a finite delay called **propagation delay.**
- The signal producing source in Fig. 8.2.4 can be a person talking on the phone or a computer producing a data signal or a video camera producing a video signal etc.
- Thus if we apply a signal at one end of the conducting medium then eventually this signal gets propagated to the other end of the medium with some time delay.



(G-1252) **Fig. 8.2.4 : Signal propagation**

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

MU : Dec. 06, Dec. 07, Dec. 09, Dec. 11, May 14, Dec. 16

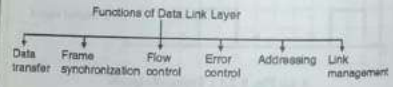
University Questions

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

Q. 2 Explain five functions of data-link layer. **(Dec. 07, Dec. 11, May 14, 10 Marks)**

Q. 3 Explain functions of data link layer. **(Dec. 09, Dec. 16, 10 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. 8.3.1 : Functions of data link layer**

1. **Services provided to the network layer :**

   The data link layer provides a well defined service interface to the network layer. The principle service is transferring data from the network layer on sending machine to the network layer on destination machine. This transfer always takes place via the DLL.

2. **Frame synchronisation :**

   The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frames can be recognized by the destination machine.

3. **Flow control :**

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

4. **Error control :**

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

5. **Addressing :**

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

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

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

7. **Link management :**

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

8.4 Nodes and Links :

- The type of communication taking place at the data link layer level is called as the **node to node communication.**
- A packet sent by a computer in the Internet will have to travel through different types of networks (LANs and WANs) before reaching the destination.
- All these LANs and WANs are connected to each other using routers.

Node :

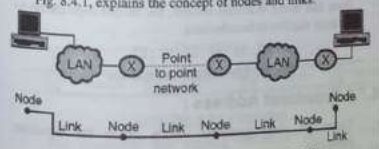
We can define a **node** as the two end hosts and the routers inbetween them.

Link :

The networks inbetween the two and hosts and the routers are called as **links.**

Source node and destination node :

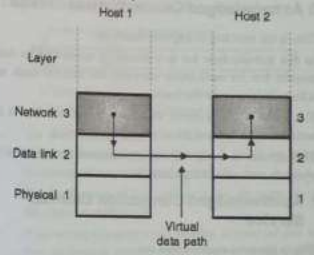
- The first node in the network is called as the source node while the last node is called as the destination node.
- Fig. 8.4.1, explains the concept of nodes and links.



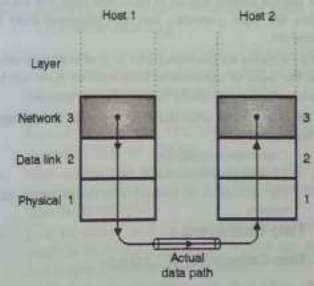
(G-2073) **Fig. 8.4.1 : Concept of nodes and links**

8.5 Services Provided to Network Layer :

- Network layer is the layer above the data link layer in the OSI model. So it is supposed to provide services to the network layer.
- The main service to be provided is to transfer data from the network layer on the sending machine to the network layer of the receiving machine.
- The virtual path followed for such a communication is shown in Fig. 8.5.1(a). It is not the actual path.
- The actual path followed by the data from sending machine to destination is shown in Fig. 8.5.1(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. 8.5.1(a)) using a data link layer protocol.



(a) Virtual communication



(b) Actual data path

(L-665) **Fig. 8.5.1**

8.5.1 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.

Scanned by CamScanner

8.5.2 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.

8.5.3 Acknowledged Connectionless Service :

- This is the next step to improve reliability.
- In this service, there are no connections established for data transfer but for each frame received, the receiver sends an acknowledgement to the sender.
- If a frame is not received within some specified time it is assumed to be lost and the sender will retransmit it.
- This service is suitable for communication over unreliable channels such as wireless channels.

8.5.4 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.

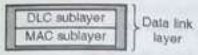
8.6 Two Sublayers :

8.6.1 Two Categories of Links :

- The medium which connects two nodes physically can be a cable or air. But the important point here is that the function of data link layer is to control how the medium is used.
- We can have a DLL which can utilize the capacity of the medium either fully or partially.
- A partially used medium is called as a **point to point link** whereas a fully used medium is called as the **broadcast link**.

8.6.2 Two Sublayers :

- We can divide the data link layer into two sublayers, in order to have a better understanding of its functionality and services provided by it.
- The two sublayers are as follows :
  1. Data link control sublayer. (DLC).
  2. Media access control sublayer (MAC).
- The two sublayers are as shown in Fig. 8.6.1. The DLC sublayer is supposed to handle all the issues common to the point to point as well as broadcast links.
- However the MAC sublayer is supposed to handle the issues related only to broadcast links.



(G-2074) **Fig. 8.6.1 : Two sublayers in data link layer**

8.7 Three Types of Addresses :

- There are some data link layer protocols which define the following three types of addresses :
  1. Unicast address.
  2. Multicast address
  3. Broadcast address.

8.7.1 Unicast Address :

- The meaning of the word **unicast** is **one-to-one** communication. A unicast address is assigned to each host or each interface of a router.
- Therefore if a frame is having a unicast destination address, then it is destined to go to only one entity in the link.
- The example of a unicast address is the LAN address. Ethernet addresses are 48 bit in length (six bytes) which is written as 12 hexadecimal digits separated by colons.
- The example of a link layer unicast address of a computer is as shown in Fig. 8.7.1(a).

A.4 : 36 : 43 : 12 : 94 : E1

Fig. 8.7.1(a) : A unicast address

8.7.2 Multicast Address :

- There are some protocols, which define multicast addresses.
- The meaning of the word **multicasting** is**one-to-many**, communication. However the communication is local i.e. inside the link.
- The multicast link layer addresses are very commonly used in LANs, Ethernet. They are 48 bit(6 bytes) long and are written as 12 hexadecimal digits separated by colons as shown in Fig. 8.7.1(b).
- Note that in the multicast address, the second digit should be an even number in hexadecimal.

A2 : 36 : 47 : 15 : 92 : E1

Fig. 8.7.1(b) : Multicast address

8.7.3 Broadcast Address :

- There are some protocols, which define the broadcast addresses.
- The meaning of the word **broadcasting** is **one-to-all** communication.
- If a frame has a destination broadcast address, then it will be sent to all the entities connected in the link.

- The broadcast address are very commonly used in LANs, Ethernets. They are 48 bit (6 bytes) long with all the bits equal to 1.
- They are written as 12 hexadecimal digits separated by colons as shown in Fig. 8.7.1(c).

FF : FF : FF : FF : FF : FF

Fig. 8.7.1(c) : Broadcast address

8.8 Data Link Control (DLC) :

- The data link control deals with the process of communication between two neighbouring nodes i.e. Node to node communication. It does not matter that whether the link is broadcast or dedicated.
- Following are the functions of data link control (DLC) :
  1. Framing
  2. Flow and error control
  3. Error detection and correction
- In the following sections we will discuss these functions of data link control.

8.9 Framing :

MU : May 09, Dec. 14, Dec. 15, Dec. 16

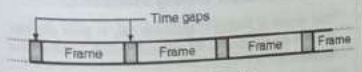
University Questions

Q. 1 With an example explain different methods of framing. **(May 09, 10 Marks)**

Q. 2 Write short note on : Framing at data link layer **(Dec. 14, 5 Marks)**

Q. 3 Explain framing in data link layer. **(Dec. 15, Dec. 16, 5 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. 8.9.1.



(G-178) **Fig. 8.9.1 : 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.

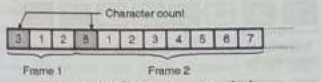
8.9.1 Framing Methods :

Following methods are used for carrying out framing :

1. Character count method.
2. Starting and ending characters, with character stuffing.
3. Starting and ending flags with bit stuffing.
4. Physical layer coding violations.

8.9.2 Character Count :

- In this method, a field in the header is used to specify the number of characters in the frame.
- This number helps the receiver to know the exact number of characters present in the frame following this count.
- The character count method is illustrated in Fig. 8.9.2.

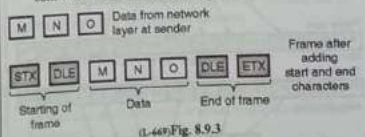


(L-668) **Fig. 8.9.2 : Character count method**

- The two frames shown in Fig. 8.9.2 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.

8.9.3 Starting and Ending Character with Character Stuffing :

- The problem of character count method is solved here by using a starting character before the starting of each frame and an ending character at the end of each frame.
- Each frame is preceded by the transmission of ASCII character sequence DLE STX. (DLE stands for data link escape and STX is start of TeXt).
- After each frame the ASCII character sequence DLE ETX is transmitted. Here DLE stands for Data Link Escape and ETX stands for End of TeXt.
- So if the receiver loses the synchronization, it just has to search for the DLE STX or DLE ETX characters to return back on track. This is shown in Fig. 8.9.3.



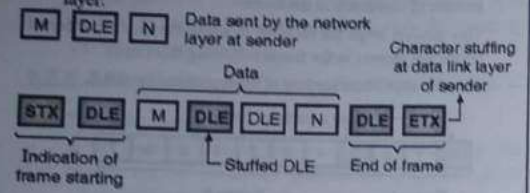
(L-669) **Fig. 8.9.3**

8.9.4 Character Stuffing :

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

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. 8.9.4 : Character stuffing**

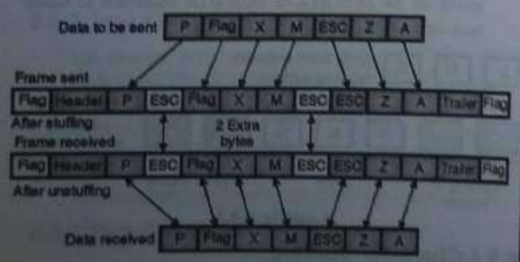
- Thus the DLE STX or DLE ETX used for framing purpose can be distinguished from the one in data because DLEs in the data always appear more than once.
- This is called character stuffing and it is shown in Fig. 8.9.4. Note that at the receiving end the destuffing is essential. Destuffing process is 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. 8.9.5 demonstrates the concept of byte stuffing.



(G-182) **Fig. 8.9.5 : Byte-stuffing**

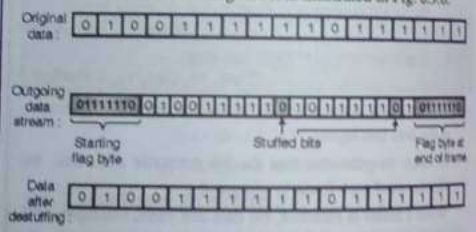
- Byte stuffing by the escape character will allow the presence of the flag is the data section of the frame. But it has a problem, if the text contains one or more escape characters followed by a flag.
- Because then the receiver will remove the escape character but will keep the flag.
- This problem is solved by marking the escape characters that are a part of the text by another escape (ESC) character as shown in Fig. 8.9.5.

8.9.5 Starting and Ending Flags, with Bit Stuffing :

- In this framing techniques at the beginning and end of each frame, a specific bit pattern 0111 1110 called **flag byte** is transmitted by the sending station.
- Since there are six consecutive 1s in the flag byte a technique called **bit stuffing** which is similar to character stuffing is used. It is as explained below.

Bit stuffing :

- Whenever the sender data link layer detects the presence of five consecutive ones in the data stream, it automatically stuffs a 0 bit into the outgoing bit stream. Thus the six consecutive 1s will never appear in the data stream. Hence there is no chance of misinterpretation.
- This is called bit stuffing and it is illustrated in Fig. 8.9.6.



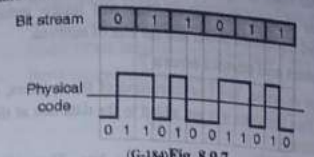
(G-183) **Fig. 8.9.6 : Bit stuffing and destuffing**

- 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. 8.9.6.
- Due to bit stuffing, the possible problem if the data contains the flag byte pattern (0111 1110) is eliminated.

8.9.6 Physical Layer Coding Violations :

- This method of framing is applicable only to those networks in which the encoding on the physical medium contains some redundancy.
- Some LANs encode each bit of data using two physical bits for example the use of the Manchester coding refer Fig. 8.9.7. 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. 8.9.7. 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. 8.9.7**

Which method of framing is used practically ?

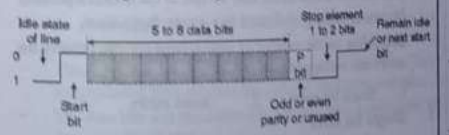
- Many data link protocols use the combination of the character count technique with one of the other techniques so as to have an extra safety.

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. 8.9.8. 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.

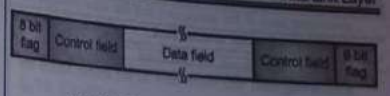


(G-185) **Fig. 8.9.8 : Asynchronous frame format**

- 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. 8.9.9.



(G-186) **Fig. 8.9.9 : Synchronous frame format**

- To prevent any possible timing problems between the transmitter and receiver, their clocks must be synchronised perfectly.
- One of the ways to synchronize is to provide a separate clock line between transmitter and receiver. The other way to provide synchronisation is to include the clocking information in the data signal itself.
- As shown in the Fig. 8.9.9, 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.

8.10 Flow and Error Control :

- Flow and error control at the data link layer is one of the function of the data link sublayer. In the following section we will discuss flow and error control in detail.

8.11 Error Control :

- The next problem to be dealt with is to make sure that all frames are eventually delivered to the network layer at the destination, in proper order.
- Generally the receiver sends back some feedback (positive or negative) to convey the information about whether it has received a frame or not.
- A positive acknowledgement (feedback) ACK indicates a successful and error free delivery of a frame. Whereas a negative acknowledgement (NAK) means that something has gone wrong and that particular frame needs to be retransmitted.
- Due to the presence of noise burst a frame may vanish completely. So the receiver does not receive anything and it does not react at all (no acknowledgement).
- This problem is overcome by introducing a timer in the data link layer. Its function of this timer is as follows.

8.11.1 Function of a Timer :

- As soon as a sender transmits a frame, it also starts the data link timer.
- The timer timing is set by taking into account the factors such as the time required for the frame to reach the destination,

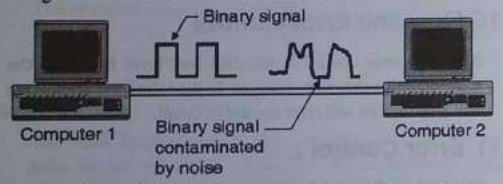
Scanned by CamScanner

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.

8.12 Introduction to Error Control Coding :

- When transmission of digital signals takes place between two systems such as computers as shown in Fig. 8.12.1, the signal get contaminated due to the addition of "Noise" to it.



(L-302)**Fig. 8.12.1 : Noise contaminates the binary signal**

- The noise can introduce an error in the binary bits travelling from one system to the other. That means a 0 may change to 1 or a 1 may change to 0.
- These error can become a serious threat to the accuracy of the digital system. Therefore it is necessary to detect and correct the errors.

8.12.1 Need of Error Control Coding :

- In data communication, errors are introduced during the transmission of data from the transmitter to receiver due to noise or some other reasons.
- The reliability of data transmission will be severely affected due to these errors.
- In order to improve the reliability of data transmission, the designer will have to increase the signal power or reduce the noise spectral density N_o so as to maximize the ratio E_b / N_o.
- But practically there is a limitation on the maximum value of the ratio E_b / N_o. We can not increase the ratio beyond this limit. **Hence for a fixed value of E_b / N_o, we have to use some kind of "coding" in order to improve the quality of the transmitted signal.**
- Another advantage of using coding is that we can reduce the required value of E_b / N_o if the error rate is predecided and remains fixed at that value. This will inturn reduce the required transmitted power and the size of antenna.

How to detect and correct errors ?

- For the detection, and / or correction of these errors, one or more than one extra bits are added to the data bits at the time transmitting.
- These extra bits are called as parity bits. They allow the detection or sometimes correction of the errors.
- The data bits alongwith the parity bits form a code word.

Error control techniques :

- The error control techniques can be divided into two types :
  1. Error detection techniques
  2. Error correction techniques
- The error detecting techniques are capable of only detecting the errors. They cannot correct the errors.
- The error correcting techniques are capable of detecting as well as correcting the errors.

8.12.2 Types of Errors :

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

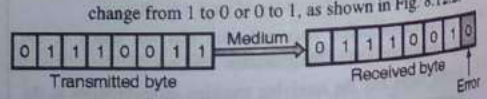
1. Content errors
2. Flow integrity errors.

- 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.

1. Single bit error :

- The term single bit error suggests that only one bit in the given data unit such as byte is in error.
- That means only one bit in a transmitted byte will change from 1 to 0 or 0 to 1, as shown in Fig. 8.12.2.

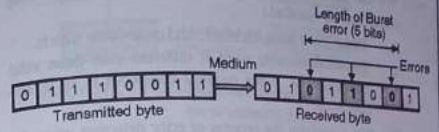


(G-188) **Fig. 8.12.2 : Single bit error**

2. Burst errors :

- If two or more bits from a data unit such as a byte change from 1 to 0 or from 0 to 1 then burst errors are said to have occurred.
- Refer Fig. 8.12.3 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. 8.12.3.



(G-189) **Fig. 8.12.3 : 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.

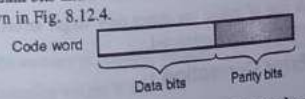
8.12.3 Disadvantages of Coding :

Some of the disadvantages of the coding technique are :

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

8.12.4 Redundancy :

- Redundancy involves transmission of extra bits alongwith the data bits. These extra bits actually do not contain any data or information but they ensure the detection and correction of errors introduced during the data travel from sender to receiver.
- As these extra bits do not contain any information, they are known as redundant bits.
- The redundant bits are also known as **parity check** bits. They are produced from the data bits using some predecided rules.
- The data bits and redundant bits together form a code word as shown in Fig. 8.12.4.



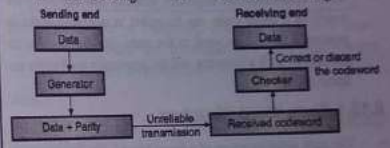
(L-303)**Fig. 8.12.4 : Structure of a transmitted code word**

8.13 Detection Versus Correction :

- Detection and correction of errors are the two most important aspects of error control in data communication.
- The correction of errors is more difficult as compared to their detection. The process of error detection is much easier because we have to simply find if error is present or absent in the received code word.
- In **error detection** we are not interested even in the number of errors. The only question to be answered is whether an error has occurred or not.
- In **error correction**, multiple processes are involved such as detecting the errors, knowing their number, the location of errors and then correcting the erroneous bits.

8.14 Coding :

- Redundancy can be implemented by using various coding schemes. The block diagram explaining the coding and decoding processes is shown in Fig. 8.14.1.
- At the sending end, redundant bits are added to data word using a well defined process. The receiver detects and corrects the errors and makes a decision on whether to accept or discard the received message.
- The two most important factors in any coding scheme are as follows :
  1. Ratio of parity bits to data bits.
  2. How robust the process is.
- The coding schemes can be divided into two types as follows :
  1. Block coding 2. Convolution coding.



(G-1448(a))**Fig. 8.14.1 : Structure of encoding and decoding process**

8.14.1 Modular Arithmetic :

- In modular arithmetic only a limited range of integers is used. The upper limit is defined as **modulus N.** Then the number of integers used are in the range 0 to (N – 1) inclusive of both.
- Addition and subtraction in modulo arithmetic are simple as there is no carry when you add or subtract two digits in a column.

8.14.2 Modulo – 2 Arithmetic :

- In modulo – 2 arithmetic N = 2 so we can use numbers 0 and 1 only. Arithmetic operations in modulo – 2 arithmetic are simple and as given below.

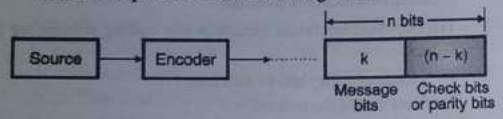
Addition	0 + 0 = 0	0 + 1 = 1	1 + 0 = 1	1 + 1 = 0
Subtraction	0 – 0 = 0	0 – 1 = 1	1 – 0 = 1	1 – 1 = 0

- Note that addition and subtraction gives the same result. In this arithmetic we use the XOR (exclusive OR) gate in order to implement both addition and subtraction.
- The XOR operation produces a 0 output if both the inputs are same (0 or 1) and it produces a 1 output if the inputs are different from each other.

Scanned by CamScanner

8.15 Linear Block Codes :

- The generation of block codes is illustrated in Fig. 8.15.1. 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. 8.15.1. As these bits do not contain any information, they are called as "redundant" bits.
- It is important to note that the (n – k) parity bits are related algebraically related to the "k" message bits. The n bit code word is thus produced as shown in Fig. 8.15.1.



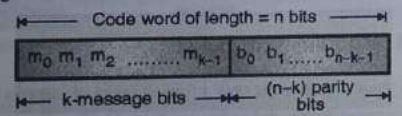
(L-316)**Fig. 8.15.1 : Generation of an n bit linear block code**

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.

8.15.1 Code Word Structure :

- The code word structure of a linear block code is as shown in Fig. 8.15.2.



(L-317)**Fig. 8.15.2 : Structure of the code word for a linear block code**

- Important points about the code word structure are as follows :
  1. A code word consists of "k" message bits which are denoted by $m_0, m_1, \ldots, m_{k-1}$ and (n – k) : parity bits denoted by $b_0, b_1, \ldots, b_{n-k-1}$.
  2. The sequence of message bits is applied to a linear block encoder to produce an "n" bit code word. The elements of this code word are $x_0, x_1, \ldots x_{n-1}$.
  3. As shown in Fig. 8.15.2, the first k bits of the code word are identical to the corresponding message bits ($m_0, m_1 \ldots$) and the next (n – k) bits are identical to the corresponding parity bits ($b_0, b_1 \ldots$). We can express this mathematically as :

$$\begin{cases} x_i = m_i & i = 0, 1, \ldots, k-1 \\ b_{i-k} & i = k, k+1, \ldots, n-1 \end{cases} \quad \ldots(8.15.1)$$

  4. The (n – k) parity bits are "linear sums" of the k message bits as will be discussed later on.
  5. The code word represented by Equation (8.15.1) can be mathematically represented as :

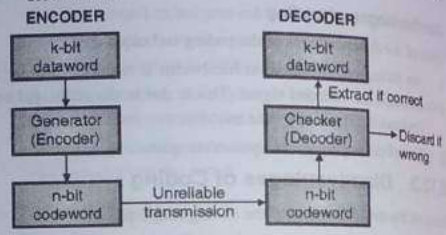
$$X = [M : B] \quad \ldots(8.15.2)$$

where M = k - message bits

and B = (n – k), parity bits

8.16 Error Detection in Block Coding :

- We can detect errors using **Block coding** if the following conditions are satisfied :
  1. The receiver has a list of all valid codewords with it.
  2. The received code word is different than these valid codewords i.e. if the received codeword is an invalid codeword.
- Fig. 8.16.1 explains the process of error detection using the block codes.

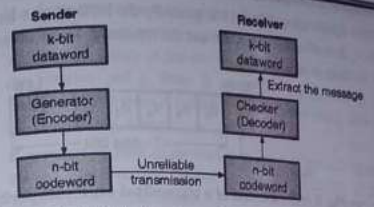


(G-1449)**Fig. 8.16.1 : Process of error detection in block coding**

- The k-bit datawords are applied to a generator or encoder. It applies the rules and procedures to encode these bits and generates an n-bit codeword.
- These codewords are transmitted using an unreliable transmission to the receiver. Each transmitted code word may change due to noise while travelling from transmitter to receiver.
- If the received codeword is same as one of the valid codewords then the receiver extracts the data word and uses it without any change.
- But if the received codeword is not valid, it is discarded. However if a corrupted received codeword matches with a valid codeword then the errors go unnoticed as the receiver treats this codeword as a valid codeword.
- This type of coding can detect only single errors. Multiple errors may remain undetected.

8.17 Error Correction :

- The process of error correction is much more difficult as compared to the error detection.
- In error correction the receiver has to detect the presence of error in the received codeword and correct it too.
- Therefore more redundant bits are required to be sent for error correction than those required for error detection. Fig. 8.17.1 explains how block coding can be used for error correction.
- Note that the block schematic of the sender and receiver for error correction is same as that for the error detection but the role of **checker** block is much more complex in error correction process.



(G-1554) **Fig. 8.17.1 : Structure of encoder and decoder in error correction**

8.17.1 Hamming Weight of a Code Word [w(x)] :

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

8.17.2 Hamming Distance :

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

(G-190(a))

Code word No.1 : 1 1 1 1 0 1 0 0

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

- Note that the bits 2, 4, 7 and 8 are different from each other. Hence Hamming distance is 4.

Ex. 8.17.1 : Find the Hamming weight of the following code vector :

x = 1 1 0 1 0 1 0 0

Soln. :

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

8.17.3 Minimum Hamming 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 code word is less than the minimum distance d_{min} because then the erroneous word is not a valid code word.
- But when the number of errors equals or exceeds d_{min} the erroneous code word may correspond to another valid code word and errors cannot be detected.
- The error detection and correction capabilities of a coding technique depend on the minimum distance d_{min} as shown in the Table 8.17.1.

Table 8.17.1 : Role of d_{min} for detection and correction of errors

Detect upto "s" errors per word.	$d_{min} \geq (s+1)$
Correct upto "t" errors per word.	$d_{min} \geq (2t+1)$
Correct upto "t" errors and detect s > t errors per word.	$d_{min} \geq (t+s+1)$

Ex. 8.17.2 : For a Hamming distance of 5 how many errors can be detected ? How many errors can be corrected ?

Soln. :

Refer to Table 8.17.1. Assuming minimum Hamming distance i.e. $d_{min} = 5$.

1. Number of errors that can be detected (s) can be obtained from

$$(s+1) \leq d_{min}$$
$$\therefore\ s \leq 5-1$$
$$\therefore\ s \leq 4 \quad \text{...Ans.}$$

Thus at the most 4 errors can be detected.

2. Number of errors that can be corrected (t) can be obtained from

$$(2t+1) \leq d_{min}$$
$$\therefore\ t \leq 2 \quad \text{...Ans.}$$

Thus at the most 2 errors can be corrected.

Ex. 8.17.3 : For a hamming distance of 6 how many errors can be detected ? How many can be corrected ?

Soln. :

1. Number of errors that can be detected is

$$s \leq d_{min} - 1$$
$$\therefore\ s \leq 6-1 = 5 \quad \text{...Ans.}$$

2. Number of errors that can be corrected $= t \leq \frac{d_{min}-1}{2}$.

$$\therefore\ t \leq 2.5.$$

So at the most 2 errors can be corrected.

Scanned by CamScanner

8.18 Linear Block Codes :

- Block codes can be of two types : Linear block codes and nonlinear block codes.
- Almost all the block codes used today are **linear block codes.** The non linear block codes are not used widely as their analysis and implementation is difficult.

Definition :

- A linear block code is defined as that code in which the exclusive OR (Modulo – 2 addition) of two valid codewords would produce an another valid codeword.

Minimum distance for linear block codes :

- For a linear block code, the minimum hamming distance is equal to the number of 1s present in that nonzero valid codeword which has the smallest number of 1s.

8.18.1 Some Linear Block Codes :

- Some of the important linear block codes are as follows :
  1. Simple parity check codes.
  2. Hamming codes.
- Out of these the parity checking codes are designed for error detection purpose whereas hamming codes are designed for error correction.

8.18.2 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. 8.18.1.

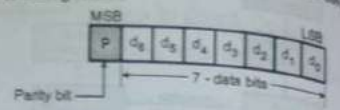
Transmitted codeword	10101100	11101011	00100101
Received codeword	1 1 1 0 1 1 0 0 (1 error)	0 1 1 1 1 0 1 1 (4 errors)	1 0 1 1 0 0 0 1 (4 errors)
Number of errors	1	2	3
Distance	1	2	3

(L-305) **Fig. 8.18.1**

- 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.

8.18.3 Parity Checking :

- 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. 8.18.2, generally the MSB of an 8-bit word is used as the parity bit and the remaining 7 bits are used as data or message bits.

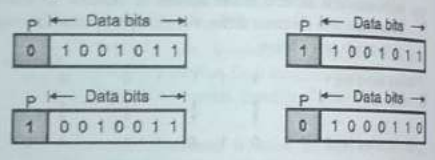


(L-309) **Fig. 8.18.2 : Format of a transmitted word with parity bit**

- The parity of the 8-bit transmitted word can be either even parity or odd parity.
- Even parity means the number of 1's in the given word including the parity bit should be even (2, 4, 6...).
- Odd parity means the number of 1's in the given word including the parity bit should be odd (1, 3, 5...).

8.18.4 Use of Parity Bit to Decide Parity :

- The parity bit can be set to 0 or 1 depending on the type of parity required.
- For odd parity this bit is set to 1 or 0 at the transmitter such that the number of "1 bits" in the entire word is odd.
- For even parity this bit is set to 1 or 0 such that the number of "1 bits" in the entire word is even. This is illustrated in Fig. 8.18.3.

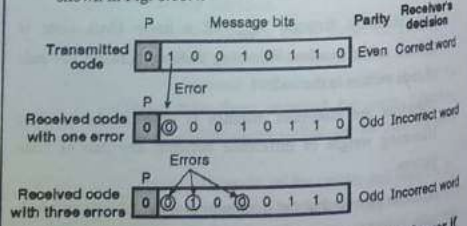


(a) Inclusion of a parity bit to obtain an even parity **(b) Inclusion of a parity bit to obtain the odd parity**

(L-310) **Fig. 8.18.3**

How does error detection take place ?

- The parity checking at the receiver can detect the presence of an error if the parity of the received signal is different from the expected parity. That means if it is known that the parity of the transmitted signal is always going to be "even" and if the received signal has an odd parity then the receiver can conclude that the received signal is not correct. This is as shown in Fig. 8.18.4.

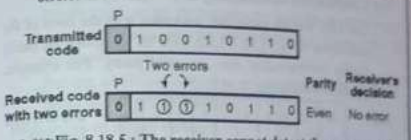


(L-311) **Fig. 8.18.4 : The receiver detects the presence of error if the number of errors is odd i.e. 1, 3, 5 ....**

- If a single error or an odd number of bits change due to errors introduced during transmission the parity of the code word will change. Parity of the received code word is checked at the receiver and if there is change in parity then it is understood that error is present in the received word. This is as shown in Fig. 8.18.4.
- If presence of error is detected then the receiver will ignore the received byte and request for the retransmission of the same byte to the transmitter.

When does parity checking fail to detect errors ?

- If the number of errors introduced in the transmitted code is two or any even number, then the parity of the received code word will not change. It will still remain even as shown in Fig. 8.18.5 and the receiver will fail to detect the presence of errors.



(L-312) **Fig. 8.18.5 : 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.

8.18.5 Simple Parity Check Block Code :

- In the simple parity check code, we have a k-bit data word which is changed to an n-bit codeword with n = k + 1. That means we add one extra bit to each k bit data word.
- The extra bit added is known as the **parity bit.** It is selected in such a way that it makes the total number of 1s in the codeword, an even number.
- The minimum hamming distance for this code is $d_{min} = 2$ which shows that it is a single bit error detecting code. It cannot correct any errors.
- Table 8.18.1 shows the codewords for a parity check linear block code, with k = 2 and n = 2 + 1 = 3 with an even parity.

Table 8.18.1 : Codewords for a parity check code with k = 2 and n = 3

Dataword	Codeword
00	000
01	011
10	101
11	110

Note : Parity bit has been underlined

(G-1400)

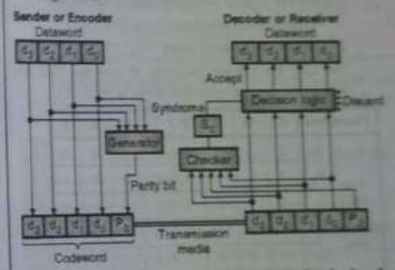
- Similarly it is possible to write codewords with k = 3 and n = 4 as shown in Table 8.18.2.

(G-1401) **Table 8.18.2 : Codewords for a parity check code with k = 3 and n = 4**

Dataword	Codeword	Dataword	Codeword
000	0000	100	1001
001	0011	101	1010
010	0101	110	1100
011	0110	111	1111

Encoder (Sender) :

- The encoder or sender for a parity check code is as shown in Fig. 8.18.6.



(G-1402) **Fig. 8.18.6 : Encoder and decoder of a parity check code**

- The generator uses the dataword as its input to generate a parity bit P_0. The codeword contains the original data word alongwith the parity bit as shown.
- The parity bit P_0 is generated by adding all the bits in the data word using themodulo – 2 addition.

$$\therefore \quad P_0 = d_0 \oplus d_1 \oplus d_2 \oplus d_3 \quad \text{... Modulo – 2.}$$

- The codeword is then sent over the transmission medium over which it may get corrupted due to noise.

Decoder or receiver :

- The 5 bit codeword corrupted by noise is received by the decoder or receiver as shown in Fig. 8.18.6.
- The function of the checker is same as that of the generator with one change. It adds all the5-bits (mod – 2 addition) in the received codeword and not four bits as in case of generator.

Scanned by CamScanner

- The result of this addition is known as syndrome. It is a single bit produced at the output of the checker as shown.
- The syndrome $S_0 = 0$ if the received codeword has an even parity and $S_0 = 1$ if it has an odd parity.

$$S_0 = d_0 \oplus d_1 \oplus d_2 \oplus d_3 \oplus P_0 \quad \text{... MOD 2 addition}$$

- This syndrome is then applied to the decision logic analyzer. If $S_0 = 0$ it indicates an even parity so there is no error in the received codeword. Hence the data bits of the received codeword would be accepted.
- But if $S_0 = 1$, it indicates an odd parity therefore an error is present in the received codeword. Hence, the data bits of this codeword are discarded.

8.18.6 Two Dimensional Parity Check (Block Parity) :

- 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. 8.18.7.
- 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. 8.18.7.

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
VRC bits (even parity)	b_6	0	0	0	0	0	0	0	0	0
	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. 8.18.7 : Vertical and longitudinal parity check bits**

The Vertical Redundancy Check (VRC) Bits :

- As shown in Fig. 8.18.7 the VRC bits are parity bits associated with the ASCII code of each character. Each VRC bit will make the parity of its corresponding column "an even parity". For example consider column 1 corresponding to character "C". The ASCII code for the character C is,

Character	C
b_1	1
b_2	1
b_3	0
b_4	0
b_5	0
b_6	0
b_7	1
VRC bit →	1

← Column - 1 of the data block

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

- 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. 8.18.7.

The Longitudinal Redundancy Check (LRC) Bits :

- The LRC bits are parity bits associated with the rows of the data block of Fig. 8.18.7. Each LRC bit will make the parity of the corresponding row, an even parity. For example, consider row 1 of Fig. 8.18.7.

Row 1 :	b_1	1	1	1	0	1	0	1	0	1

← LRC bit to make parity even

How to locate the bit in error ?

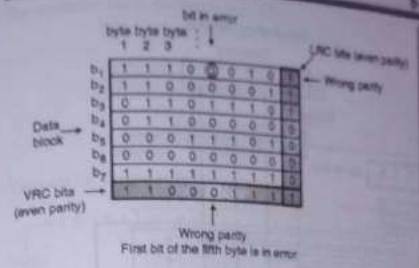
- Even a single error in any bit will result in a noncorrect "LRC" in one of the rows and an incorrect VRC in one of the columns. The bit which is common to the row and column is the bit in error.
- However there is still a limitation on the Block parity code, which is that, multiple errors in rows and 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. 8.18.1 : 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. 8.18.1 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.



(L-315(a))**Fig. P. 8.18.1**

8.19 Cyclic Codes :

- Binary cyclic codes are basically the linear block codes which actually satisfies all the restrictions that block code is supposed to satisfy.
- But the additional constraint on the binary cyclic codes is called as the **cyclic property.**

Properties of cyclic codes :

A binary code is said to be a cyclic code if it exhibits the following properties :

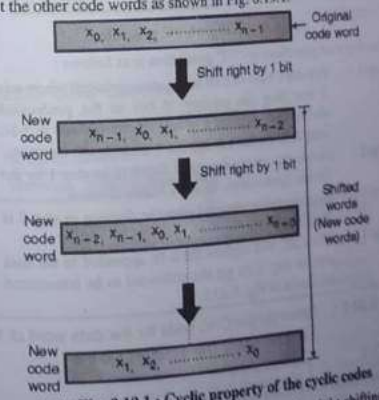
1. Linearity property 2. Cyclic property

Linearity property :

A code is said to be linear if sum of any two code words produces another valid code word. This property states that cyclic codes are linear block codes.

Cyclic property :

A code is said to be cyclic if any cyclic shift of any code word results in the formation of another code word. This is as shown in Fig. 8.19.1. Let ($x_0, x_1, ..., x_{n-1}$) be an n-bit (n, k) linear block codes. This code is shifted right 1 bit everytime in order to get the other code words as shown in Fig. 8.19.1.



(L-346)**Fig. 8.19.1 : Cyclic property of the cyclic codes**

All the n bit words obtained by the circular right shifting are new code words. This is called as the cyclic property of the cyclic codes.

8.20 Cyclic Redundancy Check (CRC) :

University Questions

Q. 1 What is CRC ? Write the algorithm for computing checksum. **(May 04, 10 Marks)**

Q. 2 What is CRC ? Write the algorithm for computing checksum and explain with suitable example. **(Dec. 06, Dec. 10, 10 Marks)**

Q. 3 Explain CRC and checksum. **(May 08, Dec. 11, 10 Marks)**

Q. 4 Explain CRC with an example. **(May 11, 10 Marks)**

Q. 5 Write short notes on : CRC and checksum. **(May 15, 5 Marks)**

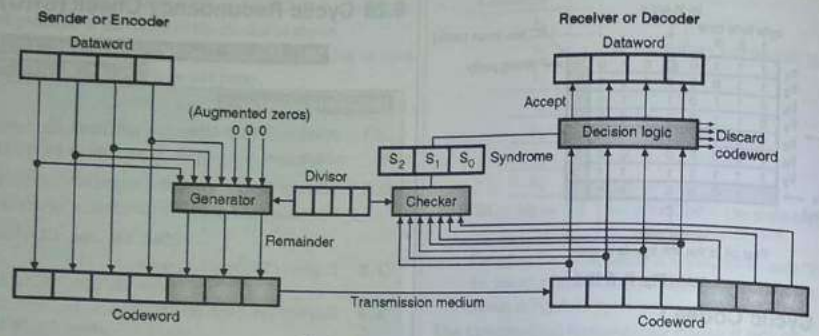
Q. 6 Write short note on : Explain CRC with example. **(May 18, 5 Marks)**

- 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.

8.20.1 CRC Encoder and Decoder :

- Fig. 8.20.1 shows the block diagrams of CRC encoder and decoder.

Scanned by CamScanner



(G-1454)**Fig. 8.20.1 : CRC generator and checker**

Encoder :

- The encoder shown in Fig. 8.20.1 has a 4 bit data word (k = 4) and 7 bit codeword (n = 7) with three parity check bits.
- The data bits are augmented by adding 3 zeros (n – k) to the R.H.S. of the word. This 7 bit resultant word is applied to the generator. This word acts as the dividend.
- The generator uses a 4 bit (n – k + 1) divisor which is predefined and used by the encoder as well as decoder to divide the augmented data word. This is a modulo – 2 division.
- The quotient of this division is discarded and the 3 bit remainder is appended to the data word to create a 7 bit codeword as shown in Fig. 8.20.1.

Decoder :

- A corrupted codeword is received by the decoder.
- All the 7 bits of the received codeword are applied to the checker alongwith the 4 bit divisor which is common to encoder and decoder. Checker is the replica of generator.
- A three bit syndrome is produced at the output of the checker which is actually a three bit remainder. The syndrome is applied to the decision logic block.
- If all the three syndrome bits are zero then the four leftmost bits of the received codeword are accepted ($S_2\ S_1\ S_0$ = 000 represents the no error situation).
- But if any of the syndrome bits are nonzero, then discard the 4 data bits because a non zero syndrome indicates presence of error in the received codeword.

8.20.2 Procedure to obtain CRC :

The redundancy bits used by CRC are derived by following the procedure given below :

1. Divide the data unit by a predetermined divisor.
2. Obtain the remainder. It is the CRC.

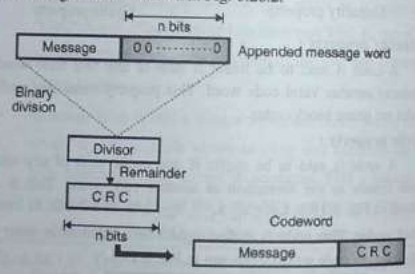
8.20.3 Requirements of CRC :

A CRC will be valid if and only if it satisfies the following requirements :

1. The number of bits in CRC should be one less than the number of bits in the divisor.
2. After we append the CRC at the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.

8.20.4 CRC Generator :

The CRC generator is shown in Fig. 8.20.2.



(L-819) **Fig. 8.20.2 : CRC generator**

The stepwise procedure in CRC generation is as follows :

Step 1 : Append a train of n 0s to the message word where n is 1 less than the number of bits in the predecided divisor (i.e. generator word). If the divisor is 5-bit long then we have to append 4-zeros to the message.

Step 2 : Divide the newly generated data unit in step 1 by the divisor (generator). This is a binary division.

Step 3 : The remainder obtained after the division in step 2 is the n bit CRC.

Step 4 : This CRC will replace the n 0s appended to the data unit in step 1, to get the codeword to be transmitted as shown in Fig. 8.20.2.

Ex. 8.20.1 : Generate the CRC code for the data word of 1 1 0 0 1 0 1 0 1. The divisor is 1 0 1 0 1.

Soln. :

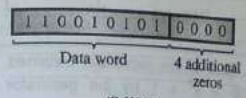
Given : Data word : 1 1 0 0 1 0 1 0 1

Divisor : 1 0 1 0 1.

The number of data bits = m = 9

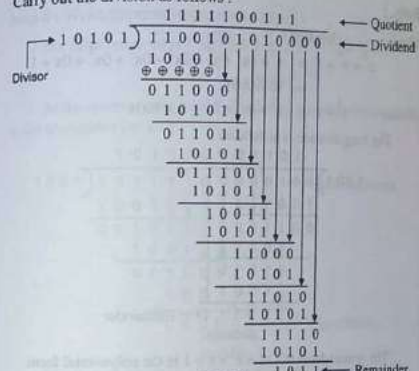
The number of bits in the divisor = n = 5

Dividend = Data word + (n – 1) zeros.



(G-801(a))

Carry out the division as follows :



(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

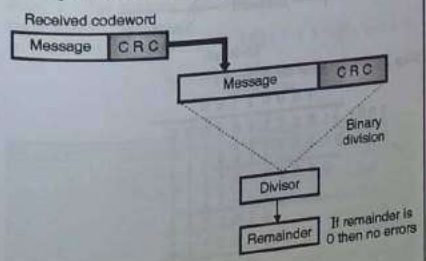
∴ Codeword = 1 1 0 0 1 0 1 0 1 | 1 0 1 1

Data word | Remainder

(G-1761)

8.20.5 CRC Checker :

Fig. 8.20.3 shows the CRC checker.



(L-820) **Fig. 8.20.3 : CRC checker**

- The codeword received at the receiver consists of message and CRC. (Fig. 8.20.3)
- The receiver treats it as one unit and divides it by the same (n + 1) bit divisor (generator word) which was used at the transmitter.
- 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.

Generation of CRC code :

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

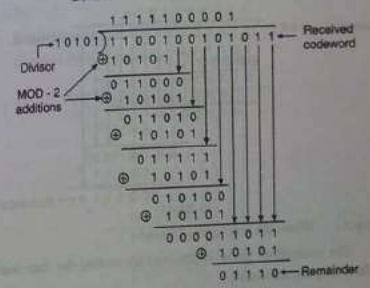
Ex. 8.20.2 : The codeword is received as 1100 1001 01011. Check whether there are errors in the received codeword, if the divisor is 10101. (The divisor corresponds to the generator polynomial).

Soln. :

- As we know the codeword is formed by adding the dividend and the remainder.
- This codeword will have an important property that it will be completely divisible by the divisor.
- Thus at the receiver we have to divide the received codeword by, the same divisor and check for the remainder.
- If there is no remainder then there are no errors. But if there is remainder after division, then there are errors in the received codeword.
- Let us use this technique and find if there are errors.

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.

Scanned by CamScanner

8.20.6 Advantages of Cyclic Codes :

The advantages of cyclic codes over most of the other codes are as follows :

1. They are easy to encode.
2. They possess a well defined mathematical structure therefore a very efficient decoding schemes can be deviced for them.
3. The methods that are to be used for error detection and correction are simpler and easy to implement.
4. These methods do not need look up table for decoding at the receiver.
5. It is possible to detect the error bursts using the cyclic codes.

8.20.7 Disadvantage of Cyclic Codes :

Even though the error detection is simpler, the error correction is slightly more complicated. This is due to the complexity of the combinational logic circuit used for error correction.

8.20.8 Solved Examples :

Ex. 8.20.3 : If the frame is 1101011011 and generator is $x^4 + x + 1$ what would be the transmitted frame. **May 13, 10 Marks**

Soln. :

Given : Data word : 1101011011

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 :

```
                1 1 0 0 0 0 1 0 1 0
Generator → 10011) 1 1 0 1 0 1 1 0 1 1 0 0 0 0 ← Dividend
                   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.

∴ 1101011011 0000 ← Dividend

\+ 1110 ← Remainder

Transmitted frame → 1101011011 1110

∴ 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. 8.20.4 : 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.

Ex. 8.20.5 : 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) : 10011101

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 :

| 1 0 0 1 1 1 0 1 | 0 0 0 |

← Dataword → ← 3 additional zeros

(G-216(g))

Step 2 : Carry out the division :

```
          1 0 0 0 0 1 1 0 0
1001) 1 0 0 1 1 1 0 1 0 0 0
      ⊖ 1 0 0 1
        0 0 0 0 1 1 0 1
            1 0 0 1
            0 1 0 0 0
              1 0 0 1
              0 0 0 1 0 0 ← Remainder
```

(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 :

Transmitted word = | 1 0 0 1 1 1 0 1 | 0 1 0 0 |

← Data word → ← Remainder

(G-216(i))

Error detection :

Step 4 : Write the erroneous received word :

The received word = 1 0 (1) 1 1 1 0 1 0 0 0 1

↑ Error

At the receiver, this word is divided by the same divider used at the transmitter i.e. 1001.

```
          1 0 1 0 1 0 0 0 0
1001) 1 0 1 1 1 1 0 1 0 0 0 1 ← Received word
      1 0 0 1
      0 0 1 0 1 1
        1 0 0 1
        0 0 1 0 0 1
          1 0 0 1
          0 0 0 0 0 0 0 1 ← Remainder
```

(G-216(j))

A non zero remainder indicates that there is an error in the received codeword.

Ex. 8.20.6 : A bit string 0111101111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing ?

Soln. : The original bit stream and the stream after bit stuffing are shown in Fig. P. 8.20.6.

Original data : 0 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 1 0

Outgoing data : | 0 1 1 1 1 1 1 0 | 0 1 1 1 1 0 1 1 1 1 1 | 0 | 0 1 1 1 1 1 | 0 | 1 0 |

Starting flag byte — Stuffed bits

(G-217) Fig. P. 8.20.6

Ex. 8.20.7 : Apply bit stuffing

0110111111111111111110010

Soln. : The outgoing data after bit stuffing is shown in Fig. P. 8.20.7.

0 1 1 0 1 1 1 1 1 1 (0) 1 1 1 1 1 (0) 1 1 1 1 1 (0) 1 0 0 1 0

Stuffed bits

(G-218) Fig. P. 8.20.7

Ex. 8.20.8 : 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

| 0 1 1 0 1 1 0 1 | 0 0 0 0 |

← Data bit sequence → ← 4 Zeros

(G-216(k))

Step 2 : Carry out division :

```
                1 1 1 1 1 0 1 1 1
10101) 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-216(l))

Step 3 : Codeword :

Codeword = Dividend + Remainder

= | 0 1 1 0 1 1 0 1 | 1 0 1 1 |

Part II :

Received word : 110011001100

Carryout the division as follows :

```
                1 1 1 1 1 1 1 0 0
10101) 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 ← Remainder
```

(G-216(m))

Scanned by CamScanner

Since the remainder is 0, the received codeword is acceptable and does not contain errors. So it is acceptable.

Received codeword = | 1 1 0 0 1 1 0 0 | 1 1 0 0 |

(G-801(r))

Ex. 8.20.9 : 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 : 1 1 0 1 1 0 1

Generator : 1 0 1 0 1

Step 1 : Obtain the dividend :

Dividend = Data word followed by 4 zeros.

= 1 1 0 1 1 0 1 0 0 0 0

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 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 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, (G-801(w))

| 1 1 0 0 1 1 0 0 | 1 1 0 0 |

← Bit sequence → ← Remainder →

∴ Received bit sequence = 1 1 0 0 1 1 0 0

Ex. 8.20.10 : Consider a message 11010011101100, divisor 1011. Compute n bit binary CRC.

Dec. 14, 5 Marks

Soln. :

Given : Dataword : 11010011101100

Divisor : 1011

Step 1 : Obtain the dividend :

Dividend = dataword + 3 zeros = 11010011101100000

Step 2 : Carry out division :

```
                1 1 1 1 0 0 0 1 1 1 1 1 0 0
1 0 1 1 ) 1 1 0 1 0 0 1 1 1 0 1 1 0 0 0 0 0
          1 0 1 1
          0 1 1 0 0
            1 0 1 1
            0 1 1 1 0
              1 0 1 1
              0 1 0 1 1
                1 0 1 1
                0 0 0 0 1
                  0 0 0 0
                  0 0 0 1 1
                    0 0 0 0
                    0 0 1 1 0
                      0 0 0 0
                      0 1 1 0 1
                        1 0 1 1
                        0 1 1 0 1
                          1 0 1 1
                          0 1 1 0 0
                            1 0 1 1
                            0 1 1 1 0
                              1 0 1 1
                              0 1 0 1 0
                                1 0 1 1
                                0 0 0 1 0 0
```

(G-1779) Fig. P. 8.20.10

Transmitted word = 11010011101100100 ...Ans.

8.21 Checksum :

MU : Dec. 11

University Questions

Q. 1 Explain CRC and checksum. **(Dec. 11, 10 Marks)**

- Checksum is the last error detection method. It is used in the Internet by many protocols. The concept of checksum is based on the principle of redundancy. This is very similar to linear block codes and cyclic codes.
- Some protocols still use checksum for error detection but now a days CRC is more preferred. Hence CRC is fast replacing the checksum.
- Checksum is used at the data link layer level and CRC is used in some layers other than the data link layer.
- Simple parity cannot detect two or even number of errors within the same word.
- One way to overcome this problem is to use a sort of two dimensional parity.
- 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. 8.21.1.

```
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
```

Fig. 8.21.1 : 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 sent.
- The errors normally occur in burst. The parity check method is not useful in detecting the errors under such conditions. The checksum error detection method can be used successfully in detecting such errors.
- In this method a "checksum" is transmitted along with every block of data bytes. In this method an eight bit accumulator is used to add 8 bit bytes of a block of data to find the "checksum byte". The carries of the MSB are ignored while finding out the checksum byte.
- The generation of checksum will be clear if you refer to the following example.

Ex. 8.21.1 : Find the checksum of the following message.

10110001,10101011,00110101,10100001

Soln. :

Ignored

Carries	(10)	1	0	1	1	1	1	0	
Data bytes		1	0	1	1	0	0	0	1
	+	1	0	1	0	1	0	1	1
	+	0	0	1	1	0	1	0	1
	+	1	0	1	0	0	0	0	1
Checksum byte		0	0	1	1	0	0	1	0

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

How to detect error using the checksum byte ?

1. 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.
2. 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.
3. Sometimes the 2's complement of the checksum is transmitted instead of the checksum itself. The receiver will accumulate all the bytes including the 2's complement of the checksum. If there is no error, the contents of the accumulator should be zero after accumulation of the 2's complement of the checksum byte.

8.21.1 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.

Scanned by CamScanner

Ex. 8.21.2 : What is the checksum of the following characters ?

01011010, 11000101, 1101 1001.

Soln. :

```
      0 1 0 1 1 0 1 0  ← Byte 1
+     1 1 0 0 0 1 0 1  ← Byte 2
+     1 1 0 1 1 0 0 1  ← Byte 3
  (2) 1   1 1 1 1 1    ← Carry
      1 1 1 1 1 0 0 0  ← Checksum
```

Discard final carry

8.21.2 One's Complement Checksum :

- In one's complement arithmetic, we can represent the unsigned numbers between 0 and $2^n - 1$ using n bits.
- If the number to be represented has more than n bits then the extra leftmost bits in this number need to be added to n rightmost bits. This is called as **wrapping.**
- In 1's complement arithmetic a negative number is represented by inverting all its bits. This would have the same effect as subtracting that number from $(2^n - 1)$.

Ex. 8.21.3 : Represent number 23 in one's complement arithmetic using only four bits.

Soln. :

Given number N = 23

Binary equivalent = $(1\,0\,1\,1\,1)_2$

But the binary equivalent has 5 bits. So we use the wrapping technique.

∴ 1's Complement equivalent = (1) 0 1 1 1

```
+ 1
  (1 0 0 0)2 = 8
```

(G-1460) ... Ans.

Ex. 8.21.4 : Represent the number – 7 using one's complement arithmetic.

Soln. :

Given number N = –7

Binary equivalent of 7 = 0 1 1 1

Invert all bits = 1 0 0 0

So 1's complement of – 7 = 1 0 0 0 = 8

Alternative method :

- Another method to find 1's complement is to subtract the given negative number from $(2^n - 1) = 2^4 - 1 = 15$.
- So in this example we subtract 7 from 15 to get 8.

Ex. 8.21.5 : The data items 7, 11, 12, 0 and 6 are to be sent with the help of 1's complement checksum technique. Calculate the value of checksum generated at the sending end. Demonstrate how error detection takes place at the receiver.

Soln. :

Step 1 : Generation of checksum :

- To generate the checksum, we add all the data items

$7 + 11 + 12 + 0 + 6 = 36$

- Represent 36 in the binary form.

36 = 1 0 0 1 0 0

- Perform the wrapping in order to have a 4-bit checksum.

```
36 : 1 0 0 1 0 0
+ 1
Wrapping :  1 0
            0 1 1 0 = 6
```

(G-1461)

- Now complement this number by subtracting it from $2^n - 1$ i.e. from 15.

∴ Checksum = 15 – 6 = 9

Step 2 : Write the packet sent by the sender :

The packet sent by the sender is as shown in Fig. P. 8.21.5(a).

7	11	12	0	6	9

Checksum

(G-1462) **Fig. 8.21.5(a) : Packet sent by the sender**

Step 3 : At the receiver :

At the receiver first all the received bits are added together.

7 + 11 + 12 + 0 + 6 + 9 = 45

Binary equivalent of 45 = 1 0 1 1 0 1

- The wrapping is carried out in the following manner.

```
45 : 1 0 1 1 0 1
+ 1
Wrapping :  1 0
            1 1 1 1 = 15 Wrapped sum
```

(G-1463)

- Subtract from 15 to get complemented wrapped sum.

15 – 15 = 0 complemented wrapped sum

- Since the value of complemented wrapped sum or checksum is 0 at the receiver the received data is **NOT CORRUPTED.** So the receiver drops the checksum and keeps the other data items.
- But if the checksum at the receiver is not zero then the entire packet is dropped.

8.21.3 Internet Checksum :

- The error detection in several Internet protocols such as IP, TCP, UDP etc. is done by using the check bits.

- For IP, a checksum is calculated for the contents of header and it is included in a special field.
- This checksum is recalculated at every router. Hence the algorithm for the checksum was selected for its ease of implementation in software.
- This algorithm assumes that the header consists of a certain number say L of 16 bits represented by

$b_0, b_1, b_2, \ldots, b_{L-1}$ and a checksum b_L

- These L words correspond to the information.
- The 16 bit checksum b_L corresponding to this information is calculated as follows.

Steps to calculate the checksum b_L :

Step 1 :	Treat each 16 bit word as an integer and add the L words modulo $2^{16} - 1$. $\therefore\ x = b_0 + b_1 + b_2 + \ldots + b_{L-1}$ modulo $2^{16} - 1$.
Step 2 :	The checksum b_L then consists of the negative value of x as follows, $b_L = -x$
Step 3 :	The checksum b_L is then inserted in the dedicated field in the header.

- The contents of all headers, including the checksum field, must satisfy the following pattern.

$0 = b_0 + b_1 + b_2 + \ldots + b_{L-1} + b_L$ modulo $2^{16} - 1$.

- Each router can check for the errors present in the header.
- Table 8.21.1 shows the 16 possible codewords that result when the checksum calculating algorithm is applied to two bit words with L = 2.

Table 8.21.1 : Codewords resulting with L = 2

b_0	b_1	b_2	Codeword		
0	0	3	00	00	11
0	1	2	00	01	10
0	2	1	00	10	01
0	3	0	00	11	00
1	0	2	01	00	10
1	1	1	01	01	01
1	2	0	01	10	00
1	3	2	01	11	10
2	0	1	10	00	01
2	1	0	10	01	00
2	2	2	10	10	10
2	3	1	10	11	01
3	0	0	11	00	00
3	1	2	11	01	10
3	2	1	11	10	01
3	3	0	11	11	00

Error detecting capability :

- From Table 8.21.1 it is evident that the minimum distance $d_{min} = 2$. That means at least two bits are required to change one codeword to the other.
- The error patterns which cause the words $b_0 + b_1 + b_2 + \ldots + b_{L-1} + b_L$ to change by a total of a multiple of $2^{16} - 1$ will not be detected.

8.21.4 Performance :

- The traditional checksum uses a small number of bits normally 16 for detecting errors in a message of any size.
- But the error checking capability of checksum method is not as good as that of the CRC method.
- So new protocols are designed in which the checksum is replaced by CRC.

8.22 Flow Control :

- This is another important design issue related to the data link layer.
- In flow control the problem to be handled is what to do with the sender computer wants to send data at a faster rate than the capacity of the receiver to receive them.
- This happens when the sender is using a faster computer than the receiver. The data sent at a very fast rate will completely overwhelm the receiver.
- The receiver will keep losing some of the frames simply because they are arriving too quickly.
- The solution to this problem is to introduce the **flow control.**
- The flow control will control the rate of frame transmission to a value which can be handled by the receiver.
- It requires some kind of a feedback mechanism from the receiver to the sender, so as to adjust the sending rate automatically.
- We are going to discuss some flow control techniques based on this principle.
- It is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver; otherwise there will be overflow of data.
- The data flow should not be so fast that the receiver is overwhelmed.
- 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.

Scanned by CamScanner

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.

8.23 Elementary Data Link Protocols :

MU : May 11

University Questions

Q. 1 What are different Data Link Layer protocols ? Explain in detail one bit sliding window protocol. **(May 11, 10 Marks)**

- In this section we are going to discuss some elementary data link layer protocols.

8.23.1 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.

8.23.2 A Simplex Stop and Wait Protocol :

MU : Dec. 03, May 07

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 example. **(May 07, 10 Marks)**

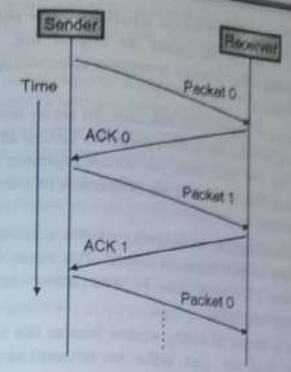
- The most unrealistic restriction in the previous protocol is the assumption that the receiving network layer can process the data with zero processing time.
- In the simplex stop and wait protocol it is assumed that a finite processing time is essential.
- However like the first protocol, the communication 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.

8.23.3 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. 8.23.1 : 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. 8.23.2.
   - To support this feature, the sender keeps timer for each frame.
   - We have already discussed that a timer is introduced in the data link layer

8.23.4 Piggybacking :

MU : Dec. 07

University Questions

Q. 1 Write a pseudo code for the following :
1. Encrypt given INPUT.TXT file to ENCRYPT.TXT
2. Decrypt ENCRYPT.TXT file to ORIGINAL.TXT **(Dec. 07, 10 Marks)**

Q. 2 Describe the following in brief : Piggybacking. **(Dec. 07, 4 Marks)**

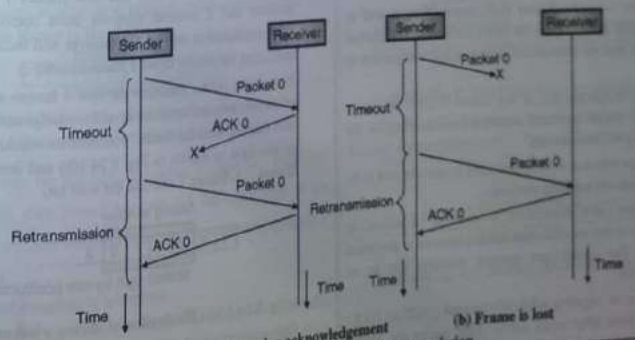
- In all the practical situations, the transmission of data needs to be bi-directional. This is called as full-duplex transmission.
- One way of achieving full duplex transmission is to have two separate channels one for forward data transmission and the other for reverse data transfer (for acknowledgements).
- 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.



(a) Sender does not receive acknowledgement (b) Frame is lost

(G-221)**Fig. 8.23.2 : Timeout and retransmission**

Scanned by CamScanner

Ex. 8.21.2 : What is the checksum of the following characters ?

01011010, 11000101, 11011001.

Soln. :

```
      0 1 0 1 1 0 1 0  ← Byte 1
+     1 1 0 0 0 1 0 1  ← Byte 2
+     1 1 0 1 1 0 0 1  ← Byte 3
  → (2) 1   1 1 1 1 1  ← Carry
      1 1 1 1 1 1 0 0  ← Checksum
```

Discard final carry

8.21.2 One's Complement Checksum :

- In one's complement arithmetic, we can represent the unsigned numbers between 0 and $2^n - 1$ using n bits.
- If the number to be represented has more than n bits then the extra leftmost bits in this number need to be added to n rightmost bits. This is called as **wrapping**.
- In 1's complement arithmetic a negative number is represented by inverting all its bits. This would have the same effect as subtracting that number from $(2^n - 1)$.

Ex. 8.21.3 : Represent number 23 in one's complement arithmetic using only four bits.

Soln. :

Given number N = 23

Binary equivalent = $(10111)_2$

But the binary equivalent has 5 bits. So we use the wrapping technique.

∴ 1's Complement equivalent = (1) 0 1 1 1

+ → 1

$(1\ 0\ 0\ 0)_2 = 8$

(G-1460) ... Ans.

Ex. 8.21.4 : Represent the number – 7 using one's complement arithmetic.

Soln. :

Given number N = –7

Binary equivalent of 7 = 0 1 1 1

Invert all bits = 1 0 0 0

So 1's complement of –7 = 1 0 0 0 = 8

Alternative method :

- Another method to find 1's complement is to subtract the given negative number from $(2^n - 1) = 2^4 - 1 = 15$.
- So in this example we subtract 7 from 15 to get 8.

Ex. 8.21.5 : The data items 7, 11, 12, 0 and 6 are to be sent with the help of 1's complement checksum technique. Calculate the value of checksum generated at the sending end. Demonstrate how error detection takes place at the receiver.

Soln. :

Step 1 : Generation of checksum :

- To generate the checksum, we add all the data items

$7 + 11 + 12 + 0 + 6 = 36$

- Represent 36 in the binary form.

36 = 1 0 0 1 0 0

- Perform the wrapping in order to have a 4-bit checksum.

```
36 :  1 0 0 1 0 0
Wrapping :  +  → 1 0
            0 1 1 0 = 6
```

(G-1461)

- Now complement this number by subtracting it from $2^n - 1$ i.e. from 15.

∴ Checksum = 15 – 6 = 9

Step 2 : Write the packet sent by the sender :

The packet sent by the sender is as shown in Fig. P. 8.21.5(a).

7	11	12	0	6	9

Checksum

(G-1462) **Fig. 8.21.5(a) : Packet sent by the sender**

Step 3 : At the receiver :

At the receiver first all the received bits are added together.

$7 + 11 + 12 + 0 + 6 + 9 = 45$

Binary equivalent of 45 = 1 0 1 1 0 1

- The wrapping is carried out in the following manner.

```
45 :  1 0 1 1 0 1
Wrapping :  +  → 1 0
            1 1 1 1 = 15 Wrapped sum
```

(G-1463)

- Subtract from 15 to get complemented wrapped sum.

15 – 15 = 0 complemented wrapped sum

- Since the value of complemented wrapped sum or checksum is 0 at the receiver the received data is **NOT CORRUPTED**. So the receiver drops the checksum and keeps the other data items.
- But if the checksum at the receiver is not zero then the entire packet is dropped.

8.21.3 Internet Checksum :

- The error detection in several Internet protocols such as IP, TCP, UDP etc. is done by using the check bits.

- For IP, a checksum is calculated for the contents of header and it is included in a special field.
- This checksum is recalculated at every router. Hence the algorithm for the checksum was selected for its ease of implementation in software.
- This algorithm assumes that the header consists of a certain number say L of 16 bits represented by

$b_0, b_1, b_2, \ldots, b_{L-1}$ and a checksum b_L

- These L words correspond to the information.
- The 16 bit checksum b_L corresponding to this information is calculated as follows.

Steps to calculate the checksum b_L :

Step 1 : Treat each 16 bit word as an integer and add the L words modulo $2^{16} - 1$.

$\therefore\ x = b_0 + b_1 + b_2 + \ldots + b_{L-1}$ modulo $2^{16} - 1$.

Step 2 : The checksum b_L then consists of the negative value of x as follows,

$b_L = -x$

Step 3 : The checksum b_L is then inserted in the dedicated field in the header.

- The contents of all headers, including the checksum field, must satisfy the following pattern.

$0 = b_0 + b_1 + b_2 + \ldots + b_{L-1} + b_L$ modulo $2^{16} - 1$.

- Each router can check for the errors present in the header.
- Table 8.21.1 shows the 16 possible codewords that result when the checksum calculating algorithm is applied to two bit words with L = 2.

Table 8.21.1 : Codewords resulting with L = 2

b_0	b_1	b_2	Codeword		
0	0	3	00	00	11
0	1	2	00	01	10
0	2	1	00	10	01
0	3	0	00	11	00
1	0	2	01	00	10
1	1	1	01	01	01
1	2	0	01	10	00
1	3	2	01	11	10
2	0	1	10	00	01
2	1	0	10	01	00
2	2	2	10	10	10
2	3	1	10	11	01
3	0	0	11	00	00
3	1	2	11	01	10
3	2	1	11	10	01
3	3	0	11	11	00

Error detecting capability :

- From Table 8.21.1 it is evident that the minimum distance $d_{min} = 2$. That means at least two bits are required to change one codeword to the other.
- The error patterns which cause the words $b_0 + b_1 + b_2 + \ldots + b_{L-1} + b_L$ to change by a total of a multiple of $2^{16} - 1$ will not be detected.

8.21.4 Performance :

- The traditional checksum uses a small number of bits normally 16 for detecting errors in a message of any size.
- But the error checking capability of checksum method is not as good as that of the CRC method.
- So new protocols are designed in which the checksum is replaced by CRC.

8.22 Flow Control :

- This is another important design issue related to the data link layer.
- In flow control the problem to be handled is what to do with the sender computer wants to send data at a faster rate than the capacity of the receiver to receive them.
- This happens when the sender is using a faster computer than the receiver. The data sent at a very fast rate will completely overwhelm the receiver.
- The receiver will keep losing some of the frames simply because they are arriving too quickly.
- The solution to this problem is to introduce the **flow control**.
- The flow control will control the rate of frame transmission to a value which can be handled by the receiver.
- It requires some kind of a feedback mechanism from the receiver to the sender, so as to adjust the sending rate automatically.
- We are going to discuss some flow control techniques based on this principle.
- It is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver; otherwise there will be overflow of data.
- The data flow should not be so fast that the receiver is overwhelmed.
- 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.

Scanned by CamScanner

Ex. 8.24.2 : 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.

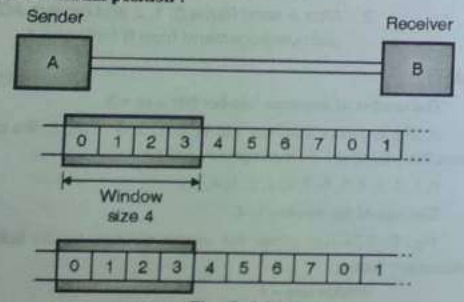
Soln. :

- 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

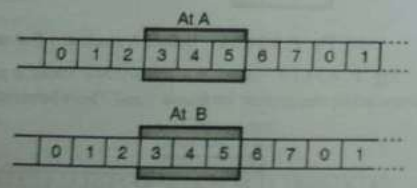
  0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, ...
- The size of the window is 4.
- The positions and frame flow at A and B for different situations are as shown in Fig. P. 8.24.2.

Case 1 : Initial position :



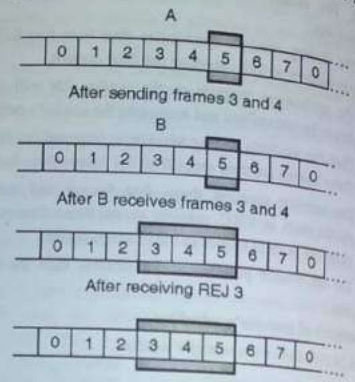
(G-231) **Fig. P. 8.24.2(a)**

Case 2 : After A sends frames 0, 1, 2 and B acknowledge 0, 1 :



(G-232) **Fig. P. 8.24.2(b)**

Case 3 : A sends frames 3 and 4 and then receives REJ 3 from B :



(G-233) **Fig. P. 8.24.2(c)**

8.24.1 A One Bit Sliding Window Protocol (Stop and Wait ARQ) :

MU : May 04, May 05, Dec. 05, Dec. 09, Dec. 10, May 11

University Questions

Q. 1 Explain a one – bit sliding window protocol in detail. **(May 04, 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)**

Q. 4 What is stop and wait protocol ? Where is it applicable ? **(Dec. 09, 5 Marks)**

Q. 5 Explain Stop and Wait Protocol and Sliding Window Protocol. **(Dec. 10, 10 Marks)**

Q. 6 What are different Data Link Layer protocols. Explain in detail one bit sliding window protocol. **(May 11, 10 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.

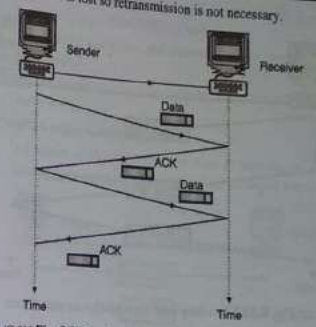
1. The transmitter stores the copy of last frame transmitted until an acknowledgement for that frame is received from the destination.
2. For distinctly identifying different types of frames both data and ACK frames are numbered alternately 0 and 1. The first data frame sent is numbered as 0. This frame is acknowledged by an ACK 1 frame. After receiving ACK 1 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 :

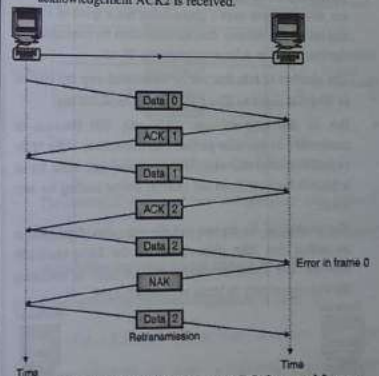
- Fig. 8.24.2 illustrates the protocol operation when everything is normal.
- No frame is lost so retransmission is not necessary.



(G-235) **Fig. 8.24.2 : Stop and wait under normal condition**

Stop and wait ARQ for damaged frame :

- As seen in Fig. 8.24.3(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.



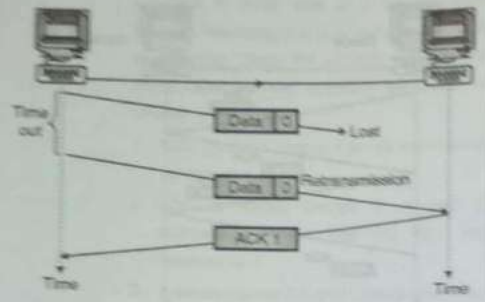
(G-236) **Fig. 8.24.3(a) : Stop and wait ARQ damaged frame**

- The process goes on in this way, but if an error occurs the receiver sends a NAK requesting retransmission of the corrupted data frame (data 2). So the transmitter retransmits the data frame 2.

Stop and wait ARQ for lost data frame :

- Fig. 8.24.3(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.

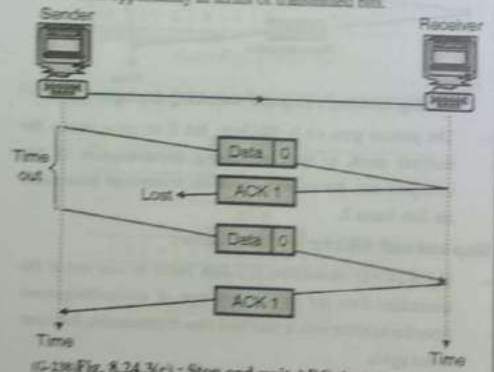
Scanned by CamScanner



(G-237)Fig. 8.24.3(b) : Stop and wait ARQ, lost data frame

Stop and wait ARQ for lost acknowledgement :

- Fig. 8.24.3(c) shows that if the acknowledgement sent by the receiver is lost, the transmitter retransmits the same data frame after its timer goes off.
- Stop and wait ARQ protocol becomes inefficient when the propagation delay is much greater than the time to transmit a frame. e.g. let us assume that we are transmitting frames that are 800 bits long over a channel that has a speed of 1 Mbps and let us also assume that the time taken for transmission of the frame and its acknowledgement is 30 mS.
- The number of bits that can be transmitted over this channel in 30 mS is equal to $30 \times 10^{-3} \times 1 \times 10^{6} = 30{,}000$ bits.
- But in the stop-and-wait ARQ only 800 bits can be transmitted in this time period. This inefficiency is due to the fact that in stop and wait ARQ the transmitter waits, for an acknowledgement from the receiver before sending the next frame.
- The product of the bit rate and the delay that elapses before an action can take place is called the Delay-bandwidth product. The Delay-bandwidth product helps in measuring the lost opportunity in terms of transmitted bits.



(G-238)Fig. 8.24.3(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.

8.24.2 A Protocol using GO Back n :

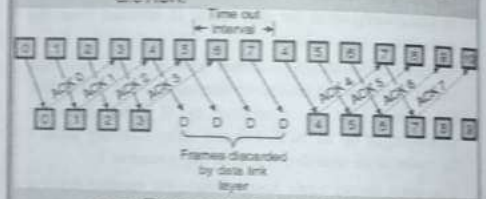
MU : Dec. 03, Dec. 04, May 11

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 **(Dec. 04, 10 Marks)**

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.



(G-883) Fig. Q. 2 : Go-Back-N sliding window

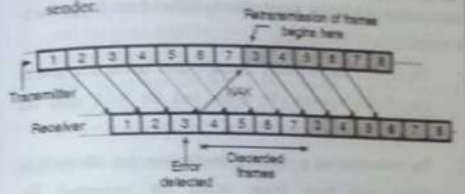
Q. 3 Differentiate between Go Back and Selective Repeat. **(May 11, 10 Marks)**

- 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 acknowledgment 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. 8.24.4 to understand the principle of GO-Back-n ARQ.
- The major difference between this and the previous system is that the sender does not wait for ACK signal for the transmission of next frame.
- It transmits the frames continuously as long as it does not receive the "NAK" signal. NAK is the negative acknowledgement signal sent by the receiver to the transmitter.
- When the receiver detects an error in the third frame as shown in Fig. 8.24.4, the receiver sends a NAK signal back to sender.



(G-239)Fig. 8.24.4 : Go back n ARQ system

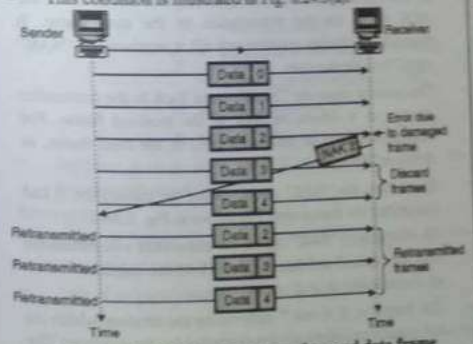
- But this signal takes some time to reach the transmitter. By that time the transmitter has transmitted frames upto frame 7.
- On reception of the NAK signal, the transmitter will retransmit all the frames from 3 onwards. The receiver discards all the frames it has received after 3 i.e. 3 to 7. It will 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. 8.24.5(a).

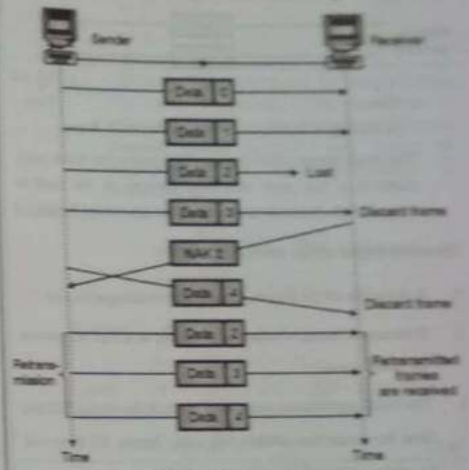


(G-240)Fig. 8.24.5(a) : Go-back-n, damaged data frame

- 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. 8.24.5(b) the case of lost frame is also treated in the same manner as that of the damaged frame.



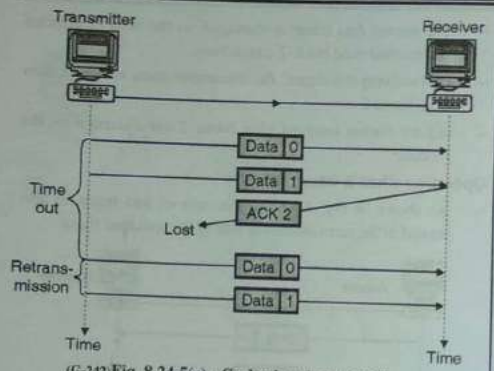
(G-241)Fig. 8.24.5(b) : Go-back-n, lost data frame

- 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 :

- The Fig. 8.24.5(c) shows the condition for lost acknowledgement. In case of go-back-n method the transmitter does not expect an acknowledgment after every data frame.
- It cannot use the absence of sequential ACK numbers to identify lost ACK or NAK frames, instead it uses a timer.
- The transmitter can send as many frames as the window allows before waiting for an acknowledgment.
- 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



(G-242)Fig. 8.24.5(c) : Go-back-n, lost ACK frame

- 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.

8.24.3 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.

8.24.4 Selective Repeat ARQ :

MU - Dec. 03, May 11, May 15, May 16

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 Differentiate between Go Back and Selective Repeat. **(May 11, 10 Marks)**

Q. 3 Suppose you have to develop an error recovery protocol for a link that is unreliable and delay sensitive, which of the following protocol would you like to choose ? Justify your answer.

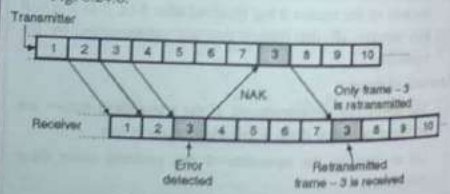
1. Stop and wait 2. Selective repeat
3. Go back **(May 15, 5 Marks)**

Q. 4 Explain selective repeat protocol. **(May 16, 5 Marks)**

In this method only the specified damaged or lost frame is retransmitted. A selective repeat systems differs from the go-back-n method in the following ways :

1. The receiver can do sorting of data frames and is also able to store frames received after it has sent the NAK until the damaged frame has been replaced.
2. The transmitter has a searching mechanism that allows it to choose only those frame which are requested for retransmission.
3. The window size in this method is less than or equal to (n + 1)/2, whereas in case of go-back-n it is n – 1.

- The principle of operation of this protocol is illustrated in Fig. 8.24.6.



(G-243)Fig. 8.24.6 : 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. 8.24.6.
- By the time this "NAK" signal reaches the transmitter, it had transmitted the frames upto 7 as shown in Fig. 8.24.6.
- 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. 8.24.6.
- 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.

8.24.5 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 :

$$\eta = \frac{t_f}{t_f + 2t_p} \quad \text{...(8.24.1)}$$

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 $A = t_p/t_f$

$\therefore \eta = 1/(1+2A)$

Prorogation time is equal to distance (d) of the link divided by velocity of propagation (v).

$\therefore t_p = d/v$

Transmission time is equal to the length of the frame (bits), divided by rate R.

$\therefore t_f = L/R$

$$\therefore A = \frac{d/v}{L/R} = \frac{Rd}{Lv}$$

Ex. 8.24.3 : 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, $\eta = 1/(1+2A) = 1/(1+2\times0.02)$

$= 0.96$

$\therefore \% \eta = 96\%$ **...Ans.**

Ex. 8.24.4 : 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, $0.5 = \dfrac{t_f}{t_f + (2\times20\times10^{-3})}$

$\therefore 0.5\,t_f + 20\times10^{-3} = t_f$

$\therefore t_f = 40\times10^{-3}$ sec.

Note that t_f = Transmission time for 1 frame

Step 2 : Calculate the frame size :

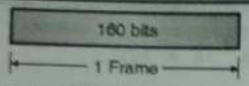
R = Data rate = 4 kbps = 4000 bps

$\therefore N = R\times t_f$

where N = Frame size

$\therefore N = 40\times10^{-3}\times4\times10^{3} = 160$ bits **...Ans.**

Scanned by CamScanner



(G-244 Fig. P. 8.24.4 : 1 frame size

Ex. 8.24.5 : 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) = ?

$$\text{Efficiency} = \frac{L}{(L+BT)}$$

$$0.5 = \frac{L}{(L+4.8\times10^{3}\times20\times10^{-3})}$$

$$= \frac{L}{(L+96)}$$

$$0.5(L+96) = L$$

$$0.5L+48 = L$$

$$\therefore L = \frac{48}{0.5} = 96 \text{ bits.}$$ ...Ans.

How to improve the throughput efficiency ?

- If the data signalling rate (R) is increased, then the time taken to transmit each block (B/R) will be reduced.
- However as delay remains unchanged, the throughput efficiency will decrease.
- To compensate for this it will be necessary to use longer blocks for higher data rates (R).
- Longer blocks however will have a greater probability of error, therefore an optimum block length 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.

8.25 Two Data Link Control Protocols :

- After discussing all issues related to the DLC sublayer, now we will discuss two DLC protocols i.e. HDLC and point-to-point protocols.
- HDLC protocol is the base of many protocols that have been used for the design of LANs. For point to point links, a protocol derived from HDLC i.e. point to point protocol is used.

8.26 High Level Data Link Control (HDLC) Protocol :

MU : Dec. 07, May 08, Dec. 14, May 15, Dec. 15, May 16, Dec. 16, May 17

University Questions

Q. 1 What is HDLC ? Explain the frame formats of I-frame, U-frame and S-frame. **(Dec. 07, May 16, 10 Marks)**

Q. 2 Explain HDLC. **(May 08, 10 Marks)**

Q. 3 Explain HDLC protocol with sutiable diagram. **(Dec. 14, Dec. 16, 10 Marks)**

Q. 4 Write short notes on : HDLC **(May 15, 5 Marks)**

Q. 5 Explain HDLC protocol alongwith its different frame structure. **(Dec. 15, May 17, 10 Marks)**

- The high level data link control (HDLC) protocol was developed by ISO.
- It is the most widely accepted data link layer protocol. It has the advantages of flexibility, adaptability, reliability and efficiency of operation.
- HDLC is a bit oriented data link control protocol, and it is designed to satisfy many of data control requirements.
- For the HDLC protocol the following three types of stations have been defined :
  1. Primary station
  2. Secondary station
  3. Combined station

1. Primary station :

A primary station takes care of the data link management. When communication between the primary and secondary stations takes place, the primary station would connect and disconnect the data link. The frames sent by a primary station are called commands.

2. Secondary station :

A secondary station operates under the control of a primary station. When communication between primary and secondary stations takes place, the frames sent by the secondary station takes place are called responses.

3. Combined station :

A combined station can act as primary as well as secondary stations. Therefore it can send both commands and responses.

Operating modes for data transfer :

- In HDLC both synchronous and asynchronous modes of communication are permitted.
- The meaning of the words synchronous and asynchronous is different from that of a physical layer.
- Following modes of operation are possible for data transfer :
  1. Normal response mode (NRM)
  2. Asynchronous response mode (ARM)
  3. Asynchronous balanced mode (ABM)
- The first two modes of operation are suitable for an unbalanced type of data transfer between one primary and the other secondary stations whereas the third one is suitable for a balanced type of data transfer.

Normal Response Mode (NRM) :

This mode is suitable for point-to-point as well as point-to-multipoint configurations. Here the primary station will control the overall data link management. It is a synchronous mode of communication.

Asynchronous Response Mode (ARM) :

- This mode is used for communication between primary and secondary stations. As the name indicates it is an asynchronous mode of communication.
- In ARM the secondary station can transmit response (frame) without taking permission from the primary station.
- This is not allowed in NRM. Therefore NRM is a more disciplined mode than ARM. The responsibility of link management function still lies with the primary station.

Asynchronous Balanced Mode (ABM) :

- This mode is applicable to the point to point communication between two combined station.
- As both these stations are combined stations, they are capable of link management functions.
- As the communication is asynchronous, one station can transmit a frame without permission from the other station. In this mode information frames can be transmitted in full duplex manner.

8.26.1 Frame Structure in HDLC :

MU : Dec. 07, Dec. 14, Dec. 15, May 16, Dec. 16

University Questions

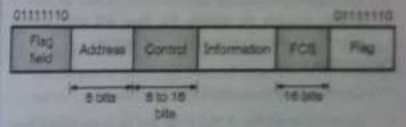
Q. 1 What is HDLC ? Explain the frame formats of I-frame, U-frame and S-frame. **(Dec. 07, May 16, 10 Marks)**

Q. 2 Explain HDLC protocol with sutiable diagram. **(Dec. 14, Dec. 16, 10 Marks)**

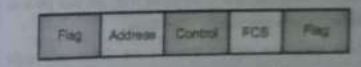
Q. 3 Explain HDLC protocol alongwith its different frame structure. **(Dec. 15, 10 Marks)**

- In the discussion of ARQ, we saw that the functionality of a protocol depends on the control fields that are used in the header.
- The format of the HDLC frame is defined in such a way that it can accommodate various data transfer modes.
- The HDLC uses two different frame formats as shown in Fig. 8.26.1(a) and Fig. 8.26.1(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. 8.26.1(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. 8.26.1

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.

8.26.2 Frame Types in HDLC :

MU : Dec. 15, May 16

University Questions

Q. 1 Explain HDLC protocol alongwith its different frame structure. **(Dec. 15, 10 Marks)**

Scanned by CamScanner

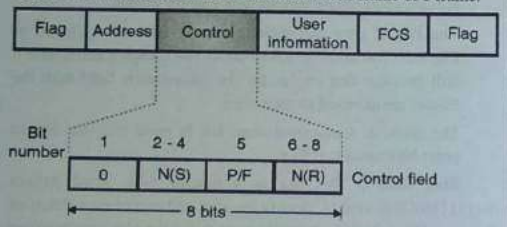
Q. 2 What is HDLC ? Explain the frame formats of I-frame U-frame and S-frame. **(May 16, 10 Marks)**

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. 8.26.2 shows the format of the information frame or I-frame.



(G-251)**Fig. 8.26.2 : I-frame format**

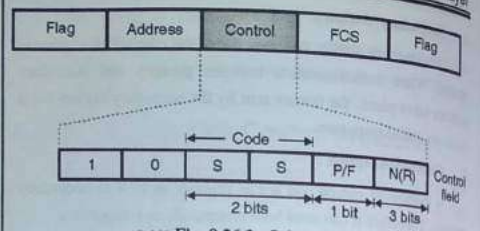
- It is supposed to carry the user data from the network layer. It is also possible to include the flow and error control information which is also called piggybacking.

Explanation :

- Concentrate on the control field of the I-frame.
- As shown in the Fig. 8.26.2 if the first bit in the control field is 0 it is identified as an information frame (I-frame).
- The next three bits (2 to 4) are called N (S) and their job is to define the sequence number of the frame.
- Since there are only 3 bits, we can define only eight combinations (2^3 = 8). Therefore a sequence number is between 0 and 7 only.
- The value of N(S) field corresponds to the value of control variable S as discussed for the three ARQ mechanisms.
- The next bit (5th) is the poll/final (P/F) bit. It can have two possible values 0 or 1 out of which only the logical 1 is meaningful. Logic 0 in this position has no meaning.
- When P/F = 1, it means poll when a frame is sent by a primary station to secondary. .
- When P/F = 1, it means final when a frame is sent by a secondary station to primary.
- The last three bits (6 to 8) define the N(R) field. It is used for piggybacking. The 3 bits in the N(R) field will represent the value of ACK when piggybacking is used.

The S-Frames :

- Fig. 8.26.3 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.

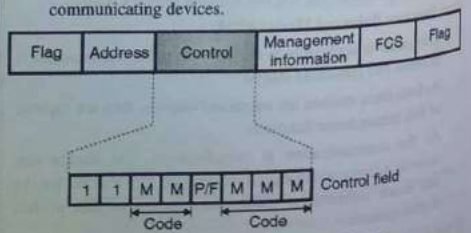


(G-252)**Fig. 8.26.3 : S-frame format**

- 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. 8.26.3.
- 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. 8.26.4.
- These frames are used for exchanging the session management and control information between the communicating devices.



(G-253)**Fig. 8.26.4 : Format of U-frame**

- A 11 in the first two bits of the control field identifies an unnumbered (U) frame as shown in Fig. 8.26.4.
- 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. 8.26.4) 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.

8.26.3 Transparency in HDLC :

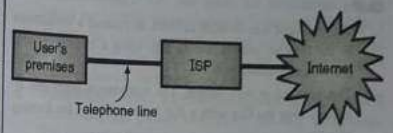
- The data field of HDLC frame is capable of carrying text and non-text information. The examples of non-text information is audio, video, graphics etc.
- But a problem is introduced for some message types during the transmission.
- If the data field of an HDLC frame contains the pattern 01111110 which 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.

8.26.4 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.
- 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.

8.27 The Data Link Layer in the Internet :

- Now we can access the Internet in a number of different ways. Earlier the only way to access the Internet was to obtain a telephone connection and then open an account with an ISP (Internet Service Provider). This type of Internet access is known as the basic access method and it is as shown in Fig. 8.27.1. So in this system the ISP will allow the user to access the Internet.



(G-1435) **Fig. 8.27.1 : Basic Internet access method**

- In modern era, the basic framework of Internet access has not changed considerably. But the ways of getting connected to the ISP from user's premises have changed to a great extent.
- The different possible ways are as follows :
  1. Dial up access
  2. ADCL
  3. ISDN
  4. Cable modems
  5. Leased lines
- One important thing to be noted is that all such methods still use the services of an ISP. They only provide different ways for the user to get connected to the ISP and Internet.

Dial up access for an individual user :

- A user can access the Internet backbone and the computers connected in a number of different ways. The simplest way is to use Internet protocol called TELNET. This protocol is an integral part of the TCP/IP suite. Here the ISP is not required but the user should have the knowledge of using the TELNET program.
- But home users generally do not know how to use TELNET. So they prefer a direct connection to the Internet, that means they want to connect to Internet through an ISP. This is a simpler way of getting connected.
- For this type of connection, the serial communication is used. The communication between client (home user) and ISP takes place using two data link layer protocols.
  1. Point to Point Protocol (PPP) and
  2. Serial Line Internet Protocol (SLIP)
- Using these two protocols the home user can dial into an ISP over the pre-existing telephone line.
- If one uses PPP and SLIP then connection is called as dial up connection because the client first dials up into server computer of ISP and makes the Internet access.
- Due to the use of PPP and SLIP protocols the communication between the client and the Internet takes place in such a way as if there is a direct connection between the home user and Internet.

8.28 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)

Scanned by CamScanner

SLIP :

- This protocol was devised in 1984, to connect a workstation to the internet over a dial-up line using a modem. It is a connection oriented protocol.
- This protocol is very simple. The workstation sends raw IP packets over the line with a flag byte at the end for framing purpose.
- If the flag format appears in the data, then a two byte sequence (0XDB, 0XDC) is sent in its place.
- If 0XDB occurs in the flag byte, then it is also stuffed.
- In some SLIP implementations, a flag byte is attached at the front and back of each IP packet sent.

Problems with SLIP protocol :

- SLIP is a simple and widely used protocol. But it has some serious problems. They are as follows :
  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.

8.29 Point-to-Point Protocol (PPP) :

- One of the most common protocols used for point to point access is PPP. The long form of PPP is point to point protocol.
- This protocol is used by a lot of Internet users to connect their home computers to the server of an Internet service provider (ISP).
- Most of these users have a traditional modem and they are connected to the Internet through a telephone line or a TV cable.
- The PPP is used for controlling and managing the data transfer.

8.29.1 Services Provided by PPP :

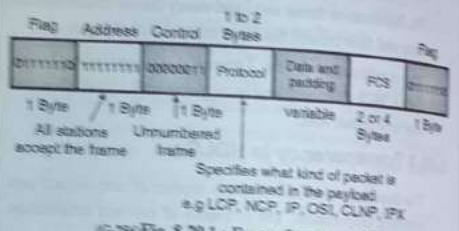
Following are some of the services provided by PPP :

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).

8.29.2 Frame Format of PPP :

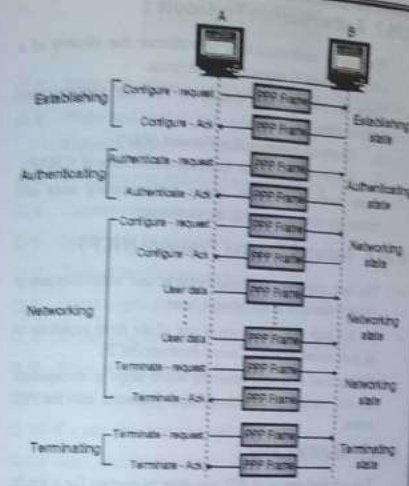
- The PPP protocol uses an HDLC like frame format as shown in Fig. 8.29.1.



(G-256) **Fig. 8.29.1 : Frame format of PPP**

The descriptions of various fields is as follows :

1. **Flag :** The PPP frame always begins and ends with the standard HDLC flag i.e. 01111110.
2. **Address :** Since PPP is used for a point-to-point connection, it uses the broadcast address of HDLC i.e. 11111111, to avoid a data link address in the protocol. All 1's in the address field indicates that all stations are to accept the frame.
3. **Control :** This field has the same format as that of the U-frame in HDLC. The value is 00000011 in this field indicates that the frame does not contain any sequence numbers and that there is no flow or error control.
4. **Protocol :** It defines the nature of contents of the data field, i.e. user data or other information.
5. **Data field :** It carries either the user data or other information.
6. **FCS (Frame Check Field) :** This field is a 2 or 4 byte CRC. It can use the CCITT 16 or CCITT 32 generator polynomial.
   - The PPP protocol provides many useful capabilities if used alongwith two protocols namely a Link Control Protocol (LCP) and the Network Control Protocol (NCP).
   - The Link Control Protocol (LCP) is used to carry out various tasks such as to set-up, configure, test, maintain and terminate a link connection.
   - After authentication has been completed a Network Control Protocol (NCP) is used.
   - The NCP consists of multiple control protocols. It help in the encapsulation of data coming from network layer protocols such as IP, IPX, Decent, Apple Talk in the PPP frame.

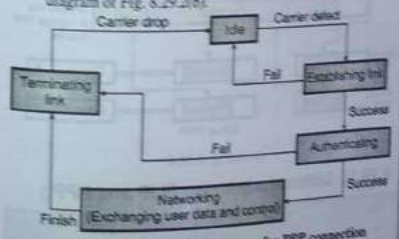


(G-257) **Fig. 8.29.2(a) : States of PPP connection**

- The PPP connection will have to go through different states, such as establishing authenticating, networking and terminating state as shown in Fig. 8.29.2(a).

8.29.3 Transition Phases :

- The PPP connection goes through different phases. These states and their interrelation is shown in the transition state diagram of Fig. 8.29.2(b).



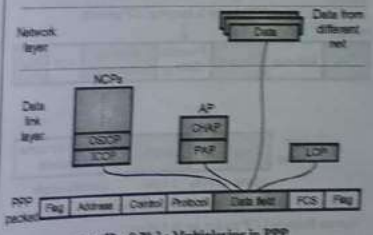
(G-258) **Fig. 8.29.2(b) : Flow diagram for PPP connection**

- Figs. 8.29.2(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 is terminated.

8.29.4 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. 8.29.3, 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.

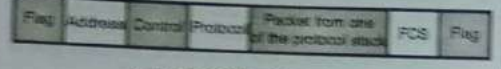


(G-259) **Fig. 8.29.3 : Multiplexing in PPP**

8.29.5 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. 8.29.4 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.

Scanned by CamScanner



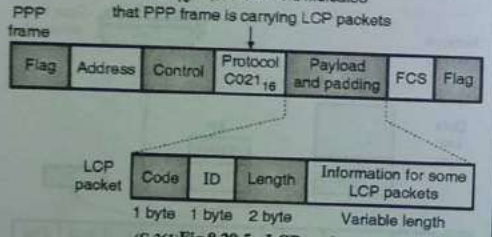
(G-260)Fig. 8.29.4 : Protocol stack

8.29.6 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. 8.29.5.



(G-261)Fig.8.29.5 : 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.

8.29.7 Authentication Protocols :

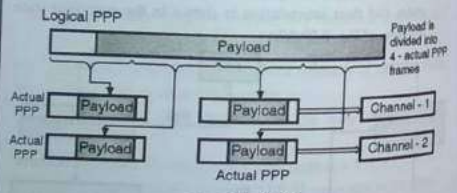
- Meaning of authentication is to validitate the identity of a user who wants an access to the resources.
- There are two protocols created by PPP for authentication purpose namely :
  1. Password Authentication Protocol (PAP)
  2. Challenge Handshake Authentication Protocol (CHAP).
- These protocols are used during authenticating state and during this state no user data are exchanged.

8.29.8 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.

8.29.9 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. 8.29.6.



(G-262)Fig. 8.29.6

8.29.10 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 ?

8.30 University Questions and Answers :

Q. 1 Which protocol Go-Back-N or selective-Repeat makes more efficient use of network bandwidth ? Why ? **(Dec. 2003, 10 Marks)**

Ans. : Selective repeat makes more efficient use of network bandwidth. Refer sections 8.24.2 and 8.24.4 for more details.

□□□

Scanned by CamScanner

CHAPTER 9

Module V

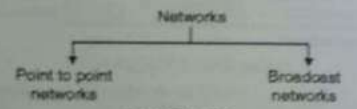
Medium Access Control

Syllabus :

Medium access control protocols : Random access, Controlled access, Channelization, Link layer addressing, Wired LANs : Ethernet protocol, IEEE project 802, Standard Ethernet, Fast Ethernet (100 Mbps), Gigabit Ethernet, 10 Gigabit Ethernet, Virtual LANs.

9.1 Introduction :

- We can classify the networks into two categories as shown in Fig. 9.1.1.
- 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.

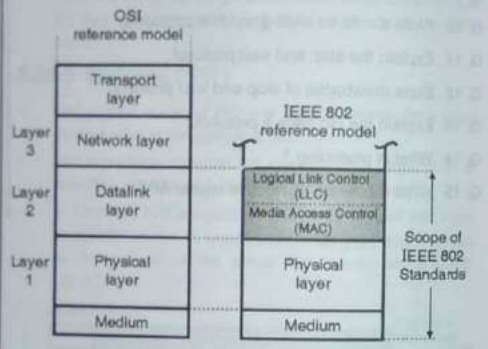


(G-264)Fig. 9.1.1

- The MAC sublayer is very important in LANs because it is a broadcast network.

9.1.1 MAC and LLC Sublayers :

- Fig. 9.1.2 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. 9.1.2.
- Fig. 9.1.2 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. 9.1.2 : IEEE 802 protocol layers compared to OSI model

Functions of Media Access Control (MAC) sublayer :

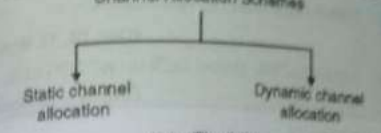
- To perform the control of access to media.
- It performs the unique addressing to stations directly connected to LAN.
- Detection of errors.

Functions of Logical Link Control (LLC) sublayer :

- Error Recovery
- It performs the flow control operation
- User addressing.

9.2 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. 9.2.1.



(G-266)Fig. 9.2.1

9.2.1 Static Channel Allocation in LANs and MANs : MU : Dec. 14

University Questions

Q. 1 Write short note on : Static channel allocation of LAN and MAN. **(Dec. 14, 5 Marks)**

- 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.

9.2.2 Dynamic Channel Allocation in LAN and MAN :

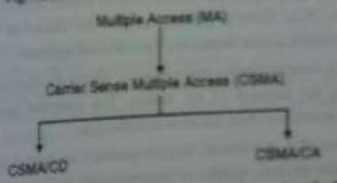
- In this method either a fixed frequency or fixed time slot is not allotted to the user. The user can use the single channel as per his requirement. Following assumptions are made for the implementation of this method :
  1. Station model – This model consists of N independent stations such as a PC, computer etc. which can generates 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.

9.3 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.

9.3.1 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. 9.3.1.



(G-267)Fig. 9.3.1 : Evolution of random access methods

9.3.2 Evolution of Random Access Methods :

- The first method in the evolution ladder of Fig. 9.3.1, known as ALOHA used a simple procedure called multiple access (MA).
- It was improved to develop the carrier sense multiple access (CSMA).
- The CSMA further evolved into two methods namely CSMA/CD (CSMA with collision detection) and CSMA/CA (CSMA with collision avoidance) which avoids the collisions.

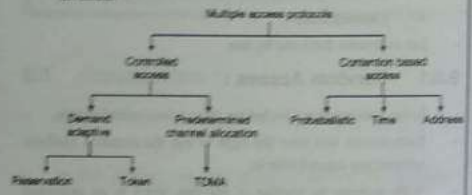
Scanned by CamScanner

9.3.3 Taxonomy (Classification) of Multiple Access Protocols : MU : May 11

University Questions

Q. 1 Explain the Taxonomy of multiple access protocols. (May 14, 10 Marks)

- Multiple access protocols, determine the allocation of channel among the stations. These protocols can be broadly divided into two classes :
  1. Controlled access
  2. Contention based access.
- Fig. 9.3.2 explains these two classes and their further sub-division.



(G-1544) Fig. 9.3.2

- The controlled access protocols are characterized by a collision free access to the channel. That means the stations are co-ordinated in such a way that two or more stations never attempt to transmit simultaneously.
- The controlled access protocols are further classified into two types :
  1. Demand adaptive 2. Predetermined channel allocation.
- The PCA (TDMA) protocols allocate the channel to the stations in a static manner (on fixed time sharing basis).
- The demand adaptive protocols try to allocate the channel as per the demands of the stations. The controlled access protocols have been discussed in section 9.6.
- Both PCA and demand adaptive protocols are inefficient if there are large number of stations having bursty message transmissions.
- The second broad class of multiple access protocols is known as contention-based protocols. These are further classified into three types, probabilistic, them based and address based protocols.
- The ALOHA and CSMA protocols (Sections 9.4 and 9.5) belong to the contention based protocols.

9.4 Multiple Access (ALOHA System) :

MU : Dec. 06, May 09, Dec. 09, Dec. 10, May 11, Dec. 11

University Questions

Q. 1 Write short note on : ALOHA. (Dec. 06, 3 Marks, May 09, Dec. 10, May 11, 5 Marks)

Q. 2 Explain ALOHA and Slotted ALOHA. (Dec. 09, 10 Marks)

Q. 3 Explain ALOHA, slotted ALOHA and CSMA/CD. (Dec. 11, 15 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.

9.4.1 Pure ALOHA :

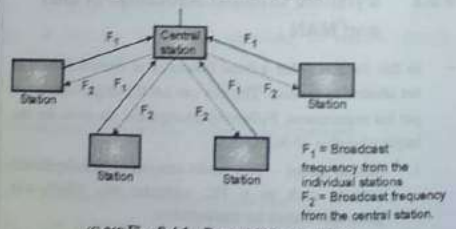
MU : Dec. 11, May 13, May 15

University Questions

Q. 1 Explain ALOHA, slotted ALOHA and CSMA/CD. (Dec. 11, 15 Marks, May 13, 5 Marks)

Q. 2 What is pure ALOHA and slotted ALOHA ? What is the efficiency ? Justify your answer. (May 15, 10 Marks)

- 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. 9.4.1, when the central station receives a frame it sends an acknowledgement on a different frequency.

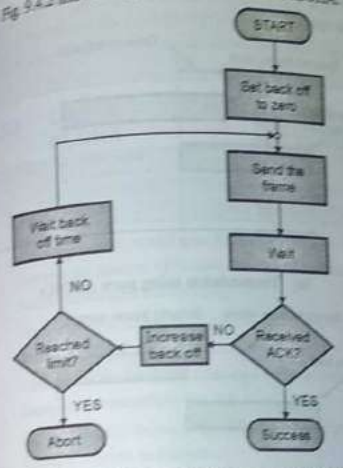


(G-268) Fig. 9.4.1 : Pure ALOHA system

- 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.

9.4.2 Protocol Flow Chart for ALOHA :

- Fig. 9.4.2 shows the protocol flow chart for ALOHA.



(G-269) Fig. 9.4.2 : 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.

9.4.3 Efficiency of an ALOHA Channel :

MU : Dec. 04, May 15

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 What is pure ALOHA and slotted ALOHA ? What is the efficiency ? Justify your answer. (May 15, 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

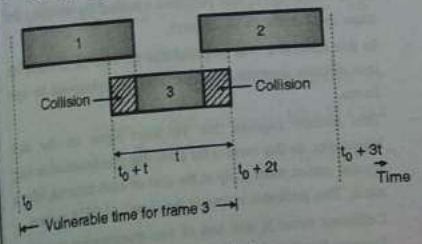
$$\text{Frame time} = \frac{\text{Frame length}}{\text{Bit rate}}$$

- 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. 9.4.3.



(G-270) Fig. 9.4.3

Scanned by CamScanner

- What is the condition for frame 3 in Fig. 9.4.3 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. 9.4.5 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.

9.4.4 Slotted ALOHA :

MU : Dec. 07, Dec. 09, Dec. 11, May 13, May 15

University Questions

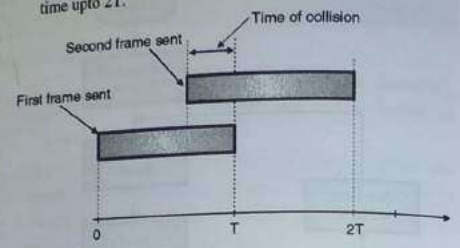
Q. 1 Describe the following in brief : Slotted ALOHA **(Dec. 07, 5 Marks)**

Q. 2 Explain ALOHA and Slotted ALOHA. **(Dec. 09, 10 Marks)**

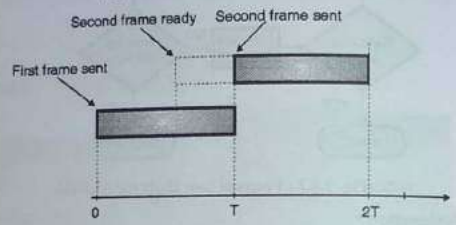
Q. 3 Explain ALOHA, slotted ALOHA and CSMA/CD. **(Dec. 11, 15 Marks, May 13, 5 Marks)**

Q. 4 What is pure ALOHA and slotted ALOHA ? What is the efficiency ?Justify your answer. **(May 15, 10 Marks)**

- To overcome the disadvantage of the pure ALOHA system (of low capacity) Robert published a method for doubling the capacity of traffic on the channel.
- In this method it was proposed that the time be divided up into discrete intervals and each interval correspond to one frame.
- This method requires that the users agree on the slot boundaries. In this method for achieving synchronisation one special station emits a pip at the start of each interval, like a clock. This method is known as the slotted ALOHA system.
- Collisions occur if any part of two transmission overlaps. Suppose that T is time required for one transmission and that two stations must transmit.
- The total time required for both stations to do so successfully is 2T as shown in Fig. 9.4.4. 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. 9.4.4

- 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. 9.4.4(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. 9.4.5. 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.

9.4.5 Comparison of Pure and Slotted ALOHA :

MU : May 16, May 17

University Questions

Q. 1 Compare slotted ALOHA and pure ALOHA. **(May 16, May 17, 5 Marks)**

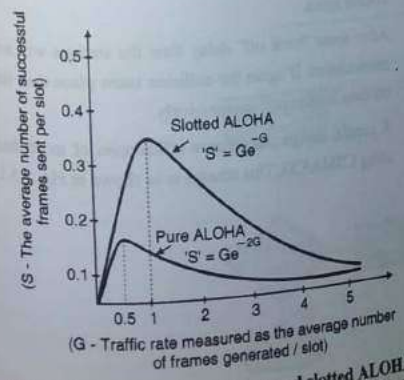
- A mathematical model can be created for the relationship between the number of frames transmitted and the number of frames transmitted successfully.
- Let G represent the traffic measured as the average number of frames generated per slot.
- Let S be the success rate measured as the average number 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. 9.4.5.
- As seen in the Fig. 9.4.5 both graphs have the same shape. If G is small so is S, which means that if few frames are generated few frames will be transmitted successfully.
- As G increases so does S but upto a certain point. As G continues to increase S approaches to 0 which means that if more frames are generated there will be more collisions and the success rate will fall to 0.
- Similarly for pure ALOHA the maximum occurs at G = 0.5 for which S = 1/2e = 0.184 which means the rate of successful transmissions is approximately 18.4%.



(G-272)Fig. 9.4.5 : Comparison of pure and slotted ALOHA

- As seen from the graph the maximum for slotted ALOHA occurs at G = 1 for which S = 1/e = 0.368. In other words the rate of successful transmissions is approximately 0.368 frames per slot time or 37% of the time will be spent on successful transmissions.
- Hence the slotted ALOHA has a double throughput efficiency than the pure ALOHA system.
- The maximum utilization achievable using CSMA can be increased much beyond that obtainable using ALOHA or slotted ALOHA.
- The maximum utilization is dependent on length of the frame and on the propagation time.
- With increase in the length of the frame or reduction in the propagation time the utilization gets improved.

Ex. 9.4.1 : 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.

Dec. 12, 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

$\therefore$ Throughput = 1000×0.184

= 184 frames /sec

2. Number of frames / sec = 500

$\therefore$ Throughput = 500×0.184 = 92 frames / sec

3. Number of frames / sec = 250

$\therefore$ Throughput = 200×0.184 = 36.8 frames / sec

Throughput of all stations = 184 + 92 + 36.8

= 312.8 frames / sec

Scanned by CamScanner

9.5 Carrier Sense Multiple Access (CSMA) : 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)

- 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.

9.5.1 Carrier Sense Multiple Access/Collision Detection (CSMA/CD) :

MU : Dec. 07, May 09, Dec. 09, Dec. 10, Dec. 11, Dec. 12, May 13, Dec. 14, Dec. 15, May 17

University Questions

Q. 1 Describe the following in brief : CSMA/CD **(Dec. 07, 5 Marks)**

Q. 2 Explain CSMA/CD. **(May 09, Dec. 10, 10 Marks)**

Q. 3 Write short note on : CSMA/CD. **(Dec. 09, Dec. 12, 5 Marks)**

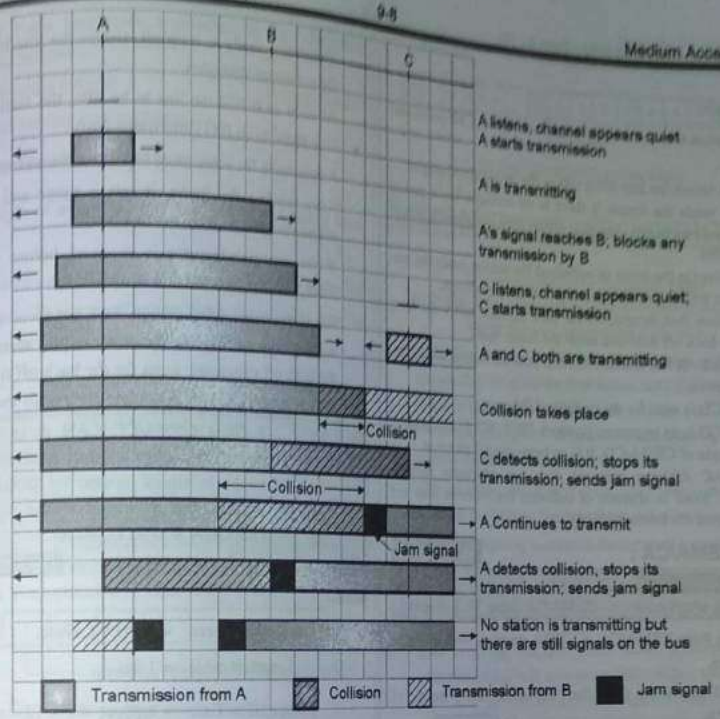
Q. 4 Explain ALOHA, slotted ALOHA and CSMA/CD. **(Dec. 11, 15 Marks, May 13, 5 Marks)**

Q. 5 Explain CSMA/CD protocol. **(Dec. 15, May 17, 10 Marks)**

The CSMA/CD specifications have been standardized by IEEE 802.3 standard. It is a very widely used MAC protocol.

Media access control :

- The problem in CSMA explained earlier is that a transmitting station continues to transmit its frame even though a collision occurs.
- The channel time is unnecessarily wasted due to this. In CSMA/CD, if a station receives other transmissions when it is transmitting, then a collision can be detected as soon as it occurs and the transmission time can be saved.
- As soon as a collision is detected, the transmitting stations release a jam signal.
- The jam signal will alert the other stations. The stations then are not supposed to transmit immediately after the collision has occurred.
- Otherwise there is a possibility that the same frames would collide again.
- After some "back off" delay time the stations will retry the transmission. If again the collision takes place then the back off time is increased progressively.
- A careful design can achieve efficiencies of more than 90% using CSMA/CD. This scheme is as shown in Fig. 9.5.1.



(G-273)**Fig. 9.5.1 : CSMA/CD scheme**

9.5.2 CSMA/CD Procedure : MU : May 09, Dec. 09, Dec. 14

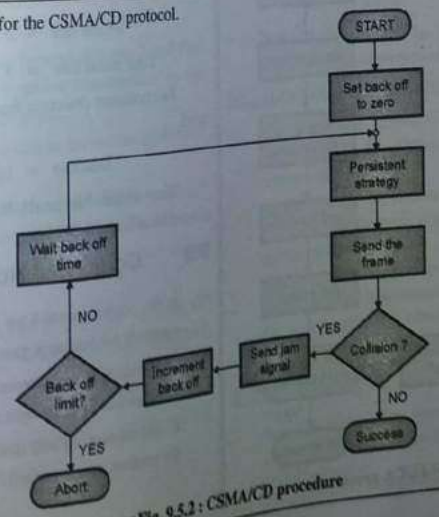
University Questions

Q. 1 Explain CSMA/CD. **(May 09, 10 Marks)**

Q. 2 Write short note on : CSMA/CD. **(Dec. 09, 5 Marks)**

Q. 3 Explain collision detection procedure in CSMA/CD. **(Dec. 14, 5 Marks)**

- Fig. 9.5.2 shows a flow chart for the CSMA/CD protocol.



(G-276)**Fig. 9.5.2 : CSMA/CD procedure**

Scanned by CamScanner

Explanation :

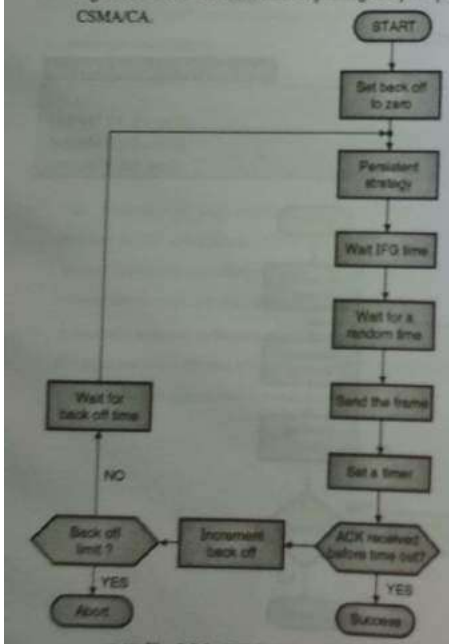
- The station that has a ready frame sets the back off parameter to zero.
- Then it senses the line using one of the persistent strategies.
- It then sends the frame, if there is no collision for a period corresponding to one complete frame, then the transmission is successful.
- Otherwise (in the event of collision) the station sends the jam signal to inform the other stations about the collision.
- The station then increments the back off time and waits for a random back off time and sends the frame again.
- If the back off has reached its limit then the station aborts the transmission.
- CSMA/CD is used for the traditional Ethernet.
- CSMA/CD is an important protocol. IEEE 802.3 (Ethernet) is an example of CSMA/CD. It is an international standard.
- The MAC sublayer protocol does not guarantee reliable delivery. Even in absence of collision the receiver may not have copied the frame correctly.

9.5.3 CSMA/CA : MU : May 16

University Questions

Q. 1 Write short note on : CDMA/CA. (May 16, 5 Marks)

- The long form CSMA/CA is CSMA protocol with collision avoidance.
- Fig. 9.5.3 shows the flow chart explaining the principle of CSMA/CA.



(G-27)Fig. 9.5.3 : 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.

Ex. 9.5.1 : 1 Gbps CSMA/CD LAN 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, 10 Marks

Soln. :

Propagation speed = 200000 km/sec.

Length of cable = 1 km

Propagation Time $= \frac{1}{200000} = 5 \times 10^{-6}$ s = 5 μ sec

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.

$$1 \times 10^9 \times \frac{1}{20000} = 0.5 \times 10^5 = 5 \times 10^4 \text{ bits.}$$

Frame size $= 5 \times 10^4 \times 2 = 10{,}000$ bits

Total round time $= 5 \times 2 = 10$ μ sec.

For collision detection frame should take at least 10 μ S to send.

Data rate = 1000 bit per μ S.

Thus 10,000 bits could be sent in 10 μS. Thus frame size should be at least 10,000 bits.

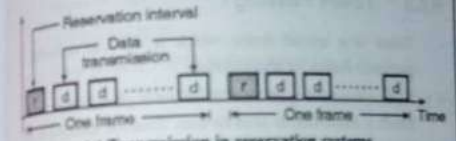
9.6 Controlled Access :

- 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.

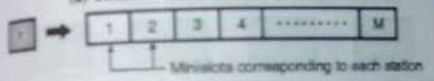
- There are three important approaches in the scheduling approach as follows :
  1. Reservation system
  2. Polling system
  3. Token passing ring networks.

9.6.1 Reservation Systems :

- The principle of reservation system can be understood from Fig. 9.6.1.
- 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. 9.6.1(a).



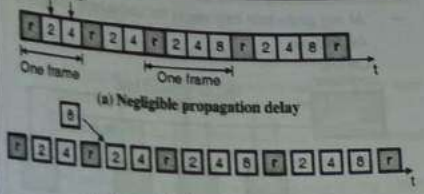
(a) Transmission in reservation systems



(b) Details of reservation interval

(L-733)Fig. 9.6.1 : Basic reservation system

- Fig. 9.6.1(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. 9.6.2.



(a) Negligible propagation delay

(b) Non negligible propagation delay

(L-734)Fig. 9.6.2 : Operation of reservation system with negligible and non-negligible delays

- Refer Fig. 9.6.2(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. 9.6.2(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) :

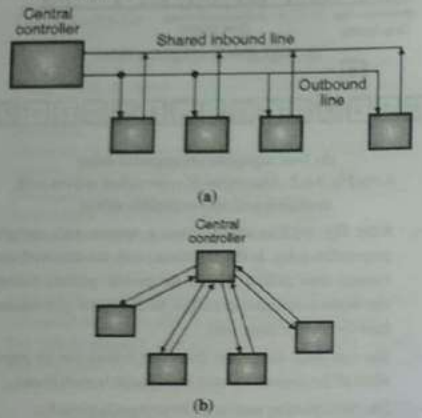
- The reservation intervals introduce overhead which is proportional to M. That means the reservation interval becomes $M \times v$.
- As the number of stations (M) become very large, this overhead will become significant. This then becomes a serious problem.
- This problem can be sorted out by not allocating 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.

9.6.2 Polling :

- Now consider polling system shown in Fig. 9.6.3. In this system the stations access the common medium one by one (by taking turns).

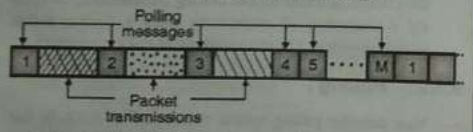
Scanned by CamScanner

- At any given time only one of the stations will transmit into the medium.



(L-735)**Fig. 9.6.3 : 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. 9.6.3(a) shows a scheme in which M stations communicate with a central controller. The outbound line is used for carrying the information from the central controller to the M users whereas the shared inbound line is required to carry the information from users to the central computer.
- Thus the inbound line acts as the shared medium that requires a medium access control (MAC).
- The host computer acts as a central controller. It sends control messages which co-ordinate the transmissions from the stations.
- The central controller sends a polling message to a particular station. That station sends its message on the shared inbound line. Once this process is over, the station gives a go-ahead message.
- It is possible that the central controller may poll the stations in a round robin (serial) fashion or it may do it according to some pre-determined rule.
- Fig. 9.6.3(b) shows another system where it is possible to use polling. The central controller of this system can make use of radio transmission.
- Fig. 9.6.4 shows the sequence of polling messages.

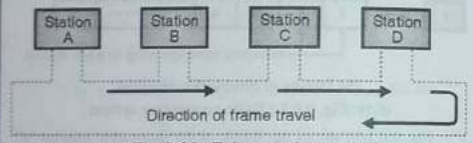


(L-736)**Fig. 9.6.4 : Polling messages and transmissions in a polling system**

- 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.

9.6.3 Token Passing :

- Token is a special frame which is used to authorize a particular station for transmission.
- In the token passing method, the token is given to that station, which is authorized to send its data. Thus the station that has the token with it can transmit others listen.



(L-737)**Fig. 9.6.5 : Token passing network**

- In a token passing network, each station has a predecessor and successor as shown in Fig. 9.6.5.
- The frames travel in one direction. They come from the predecessor and go to the successor as shown in Fig. 9.6.5.
- 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.

9.7 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.

9.7.1 FDMA :

- In the frequency division multiple access (FDMA), the available channel (medium) bandwidth is shared by all the stations. That means each station will have its own specific slot reserved in the entire channel bandwidth.
- So each station uses its allocated frequency band to send its data. Each band is thus reserved for a specific station. e.g. the frequency band f_0 to f_1 is for station-1, then f_2 to f_3 is for station-2 and so on.
- The concept of FDMA is illustrated is Fig. 9.7.1.
- FDMA is a data link layer protocol which uses FDM at the physical layer.

(L-739)**Fig. 9.7.1 : 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 :

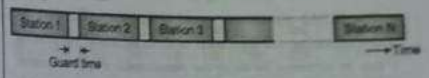
1. All the stations can operate continuously all 24 hours without having to wait for their turn to come.
2. The power required for transmission depends on the number of channels being transmitted.
3. The signal to noise ratio is improved due to the use of FM.
4. No synchronization is necessary.

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.

9.7.2 TDMA :

- TDMA stands for Time Division Multiple Access.
- In TDMA, the entire bandwidth can be used by every user (station) but not simultaneously.
- A station can use the entire bandwidth only for the allocated time slot.
- Thus each channel is allocated a time slot only during which it can send its data. Thus the time is shared, frequency band is not shared.
- Fig. 9.7.2 illustrates the concept of TDMA. Guard times are inserted between the adjacent time slots in order to prevent any cross talk. Not data transmission takes place during the guard times.



(L-740)**Fig. 9.7.2 : 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.

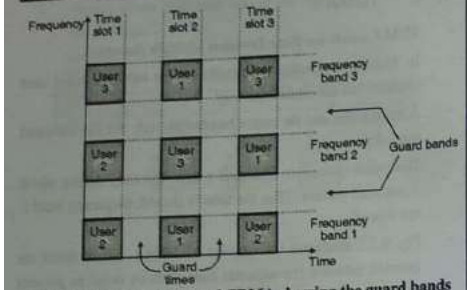
9.7.3 Code Division Multiple Access (CDMA) :

- 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.
- 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



(L-741)**Fig. 9.7.3 : Structure of CDMA showing the guard bands and the guard times**

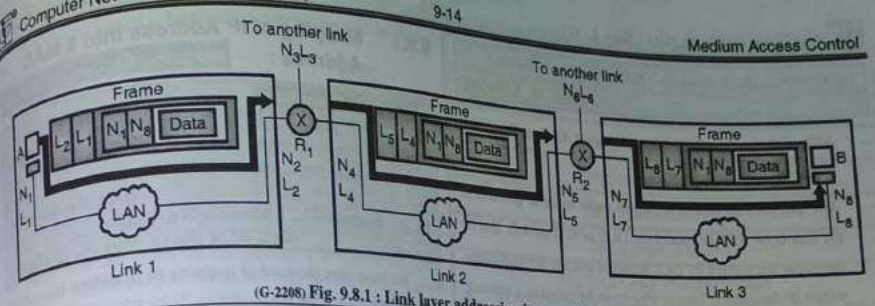
- The CDMA signals are spread in frequency. Therefore the demodulation and separation of these signals at the receiver can be achieved by using the pseudorandom code sequence. CDMA is sometimes also called as spread spectrum multiple access (SSMA).
- In CDMA as the bandwidth as well as time of the channel is being shared by the users, it is necessary to introduce the guard times and guard bands as shown in Fig. 9.7.3.
- CDMA does not need any synchronization, but the code sequences or signature waveforms are required to be used.

9.7.4 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.

9.8 Link Layer Addressing :

- In this section we will discuss an issue about data link layer i.e. link layer addresses.
- We have discussed in chapter 7 that the network layer IP addresses works as identifiers. IP addresses define the accurate point where source and destination host are connected in the internet.
- But in a connectionless internetwork (internet), using only IP addresses we can't make a datagram to reach its destination. The reason is that in the internet each datagram may take a different path from the same source host to same destination host.
- The source and destination IP addresses can define the two ends but not able to define links through which the datagram should pass.
- Remember that in a datagram there should not be any change in IP addresses.
- The packet will never reach it's destination if the destination IP address in a datagram will change. Where as if source IP address in a datagram changes, there will not be any communication between source and destination host.
- To overcome this problem we need another method of addressing in a connectionless internetwork. Link layer addresses of the two nodes is mechanism used to solve the above discussed problem.
- Link layer address is also called as MAC address, link address or physical address.
- The addresses required to belong to the data link layer because at the data link layer a link is controlled.
- The datagram will be encapsulated in a frame when it passes from the network layer to data link layer and into the frame header two data link addresses are added.
- When frame moves from one link to other then at every time there will be change in these two link addresses.
- Fig. 9.8.1 shows link-layer addressing in a small internet.



(G-2208) **Fig. 9.8.1 : Link layer addressing in a small internet**

Where N = IP addresses
L = Link layer addresses

Address order : IP address – source, destination
Link layer address – destination, source

Fig. 9.8.1 consists of :

1. Three links
2. Two routers (R1 and R2)
3. Two hosts, A (Source) and B (destination).

- We have two addresses for each host i.e. N (IP address) and L (Link layer address).
- As many number of links are connected to the router, router has that many pairs of addresses.
- Each link includes three frames as shown In Fig. 9.8.1. Each frame in each link holds the datagram which includes the same source and destination address i.e. N_1 and N_8 from link to link there is change in link layer addresses of frame.
- Link layer addresses in link 1 are L_1 and L_2.
- Link layer addresses in link 2 are L_4 and L_5.
- Link layer addresses in link 3 are L_7 and L_8.
- It is important to note that the order of IP address and link-layer address is not same. The source address comes before the destination address for IP addresses whereas the destination address comes before the source address for link layer address.
- In this way frames and datagrams are designed.
- While designing we may have several questions. These questions are discussed as follows :

Q. 1 In any datagram sent from a source to destination where the IP address of router does not appear anywhere then why we need to allocate IP addresses to routers ?

Ans. :

A router can act as a sender or receiver of a datagram in some protocols. In such a case communication takes place in between the routers. Because of this reason it is necessary assign IP address to routers.

Q. 2 In a packet how the source and destination IP addresses are determined ?

Ans. :

It is necessary that the host must know its own IP address that IP address becomes source address in the packet. To find the destination address, application layer uses DNS services and for insertion in the packet it passes it to the network layer.

Q. 3 In a router, why we require more than one IP address one for each interface ?

Ans. :

For a connection of a router to a link interface is used. A point in the internet at which a device is connected is defined by an IP address. In the internet at n points, a router with n interface are connected.

Q. 4 What is the size of link-layer addresses ?

Ans. :

The size of link-layer addresses depends on the protocol used by the link.

Q. 5 For each link, how the source and destination link-layer addresses are determined ?

Ans. :

Each host must know its own link layer address and using ARP (Address resolution protocol) the destination link layer address can be determined.

9.9 ARP (Address Resolution Protocol) :

MU : May 04, May 09, May 10, Dec. 10

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 notes on : ARP, RARP **(May 09, 10 Marks)**

Q. 3 Explain main features of following protocols. ARP **(May 10, 2 Marks)**

Scanned by CamScanner

Q. 4 Write short notes on : ARP, RARP (Dec. 10, 5 Marks)

- ARP as defined in RFC 826 is Ethernet Address Resolution Protocol.
- ARP provides service to IP, which make us think that it is in the link layer TCP/IP model (or DLL of OSI model). But its messages are carried by DLL protocol and are not capsulated within IP datagrams. That is why it can be called as a network layer protocol as well. Thus ARP occupies an unusual place in TCP/IP suite.
- But the most important point is that ARP provides an essential service when TCP/IP is running on a LAN.
- An internet consists of various types of networks and the connecting devices like routers.
- A packet starts from the source host, passes through many physical networks and finally reaches the destination host.
- At the network level, the hosts and routers are recognised by their IP addresses.

IP address :

- An IP address is an internetwork address. It is a universally unique address.
- Every protocol involved in internetworking requires IP addresses.

MAC address :

- The packets from source to destination hosts pass through physical networks. At the physical level the IP address is not useful but the hosts and routers are addressed by their MAC addresses.
- A MAC address is a local address. It is unique locally but it is not unique universally.
- The IP and MAC address are two different identifiers and both of them are needed, because a physical network can have two different protocols operating at the network layer at the same time.
- Similarly a packet may travel through different physical networks.
- So to deliver a packet to a host or a router, we require addressing to take place at two levels namely IP addressing and MAC addressing.
- Most importantly we should be able to map the IP address into a corresponding MAC address.

9.9.1 Mapping of IP Address into a MAC Address : MU : Dec. 04, Dec. 07, May 08

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 Explain MAC address with examples. **(Dec. 07, 2 Marks, May 08, 10 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.

9.9.2 ARP Operation :

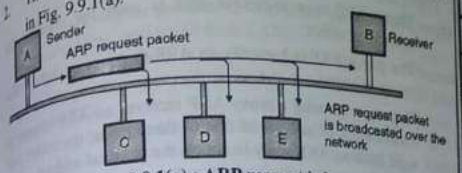
- ARP is used for mapping an IP address to its MAC address. For a LAN, each device has its own physical or station address as its identification. This address is stored on the NIC (Network Interface Card) of that machine.

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 :

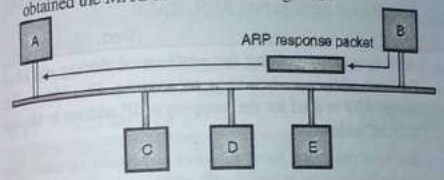
1. The router or host A who wants to find the MAC address of some other router, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender A and the IP address of the receiver (B).

2. This request packet is broadcasted over the network as shown in Fig. 9.9.1(a).



(G-575) **Fig. 9.9.1(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. 9.9.1(b). Thus host A has obtained the MAC address of B using ARP.



(G-576) **Fig. 9.9.1(b) : ARP response unicast**

9.9.3 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.

9.9.4 ARP Packet Format :

The ARP message format is as shown in Fig. 9.9.2. 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.

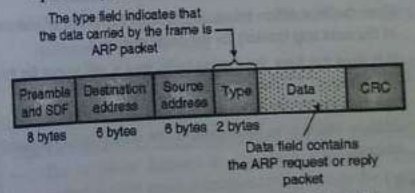
Hardware Type (16 bits)		Protocol type (16 bits)
Hardware length	Protocol length	Operation request 1, Reply 2
Sender hardware address		
Sender protocol address		
Target hardware address		
Target protocol address		

Fig. 9.9.2 : 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.

9.9.5 Encapsulation :

- An ARP packet (request or reply) is inserted directly into the data link frame. Such an insertion is known as encapsulation.
- Fig. 9.9.3 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. 9.9.3 : Encapsulation of ARP packet**

9.9.6 Operation of ARP on Internet :

- The services of ARP can be used under the following working conditions when it is being operated on internet :
  1. The sender is a host and wants to communicate with another host which is on the same network.
  2. The sender is a host and wants to communicate with a host on another network.
  3. The sender is a router. It has received a datagram with a destination address of a host on another network.
  4. The sender is a router. It has received a datagram which is meant for a host in the same network.

Scanned by CamScanner

- Now let us see how ARP works on the internet.

Operation :

1. The sender (host or router) knows the IP address of the target.
2. IP orders ARP to create an ARP request message. The request packet consists of senders physical and IP addresses plus the IP address of the target but the physical address of the target is not known.
3. This ARP request packet is sent to the data link layer. Here the ARP request packet is inserted in a frame.
4. Every router or host receives this frame because it is broadcast. All the machines except the target drop this packet as discussed earlier.
5. The target machine sends back a reply packet which contains the target's physical address. This reply is unicast and addressed only to the sender.
6. The sender receives the reply packet. Hence the physical address of the target has been obtained.
7. The IP datagram carrying data for the target machine is inserted in a frame and the frame is unicast to the target machine.

9.9.7 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.

9.9.8 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.

9.9.9 The Reverse Address Resolution (RARP) Protocol : MU : May 09, Dec. 10

University Questions

Q. 1 Write short notes on : ARP, RARP **(May 09, 10 Marks)**

Q. 2 Write short note on : ARP, RARP **(Dec. 10, 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.
- 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.

9.10 Wired LANs : Ethernet Protocol :

- We know that for physical layer and data-link layer, TCP/IP protocol suite does not define any protocol. i.e. at these two layers any protocol can be accepted by TCP/IP which can provide service to the network layer.
- We know that for a limited geographic area such as a campus or building, local area networks (LANs) are designed.
- In an organization to connect computers, LAN is used as an isolated network.

- Now a days LANs are linked to a internet or WANs. Many different types of LANs were used in the 1980's and 1990's. For resolving the problem of sharing the media, media access method was used by all these LANs.
- The approach used in the Ethernet is CSMA/CD. Whereas token-passing approach is used in the token bus, token ring and FDDI.
- During this period, in the market new LAN technology ATM LAN comes into existance which deployed the high speed WAN (wide area networks) technology.
- From the marketplace except Ethernet almost every LAN has disappeared. To meet the requirements of time, Ethernet was able to update itself.
- With the demand for high transmission rate, Ethernet could evolve for this reason the Ethernet protocol was designed.
- In the past, the organization that has used an ethernet LAN, now if they want higher data rate, instead of switching to another technology they would update to the new generation. It may cost more.
- In the following sections we will discuss wired LAN i.e. Ethernet.
- In the 1970s, the Ethernet LAN was developed by Robert Metcalfe and David Boggs..

9.11 Ethernet : MU : Dec. 09

University Questions

Q. 1 Write short note on : Ethernet. **(Dec. 09, 5 Marks)**

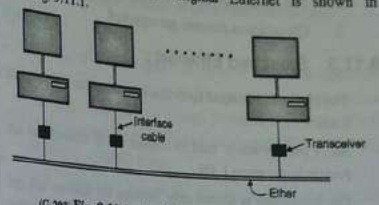
- Both Internet and ATM were designed for wide area networking. But in many applications, a large number of computers are to be connected to each other.
- For this the local area network (LAN) was introduced. The most popular LAN is called Ethernet.
- The IEEE 802.3 standard is popularly called as Ethernet. 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. 9.11.1.



(G-293) **Fig. 9.11.1 : Architecture of original Ethernet**

- The original Ethernet was standardized as IEEE 802.3 standard. The committee also standardized a token bus (802.4) and token ring (802.5) standards which were not as popular as Ethernet.

Computer connected to internet via LAN :

- When a computer is connected to Internet via LAN, it has to use all the five layers of the internet model.
- The three upper layers (network, transport and application) are common to all the LANs.
- The data link layer is divided into two sublayers namely the logical link control (LLC) and the medium access control sublayer (MAC).
- The LLC sublayer is designed to be the same for all the LANs so that all the LANs can be connected to each other and operate without any problem.
- This means that only the MAC sublayer and physical layer of various LANs will be different from each other.
- If we compare different types of Ethernets then it is observed that, the MAC sublayer is slightly different but the physical sublayer is almost the same.

9.11.1 Traditional Ethernet : MU : May 16

University Questions

Q. 1 Explain traditional Ethernet. **(May 16, 5 Marks)**

- The traditional Ethernet is the oldest version of Ethernet created in 1976 which is designed to operate at the maximum data rate of 10 Mbps.
- The access to the network by a device is through the CDMA/CD i.e. the MAC uses CSMA/CD and the media is shared between all the hosts connected in LAN.

Why Ethernet has been so successful ?

- First, an Ethernet is extremely easy to administer and maintain.
- There are no switches, which can fail, no routing or bath tables that have to be kept up-to-date. We can add new host easily to this network second, it is inexpensive, cable is cheap, only network adapter is little costly.

Scanned by CamScanner

9.11.2 Bridged Ethernet :

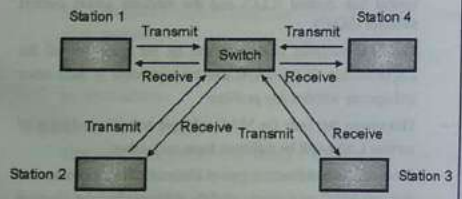
- We can divide a LAN into smaller segments by inserting bridges in between.
- Bridges affect the Ethernet LAN in the following two ways :
  1. The bandwidth requirement increases.
  2. The collision domains get separated.

9.11.3 Switched Ethernet :

- The concept of bridged LAN can be extended to the switched LAN.
- An N port switch is used to connect the N stations that are present in the given LAN.
- The bandwidth is shared only between the stations and the switch. The collision domain is divided into N domains. The packet handling becomes faster due to the use to layer-2 switches.

9.11.4 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. 9.11.2 : 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 fill duplex mode.
- Fig. 9.11.2 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.

9.11.5 Fast Ethernet :

- Fast Ethernet is the protocol designed to work at higher data rates than the traditional one. Typically it can support the data rates upto 100 Mbps.
- The traditional Ethernet can operate only upto 10 Mbps. Hence for higher data rates fast Ethernet has been developed.

Autonegotiation :

This is the new feature of the fast Ethernet. The autonegotiation will make it possible to negotiate on the mode or data rare of operation between the communicating devices.

9.11.6 Gigabit Ethernet :

- The gigabit Ethernet protocol has been designed in order to operate at data rates upto 1000 Mbps or 1 Gbps. This is the highest bit rate of all the types.
- The MAC layer was supposed to remain unchanged for all the versions of the Ethernet but it does not remain so when such a high data rate is to be supported.
- The Gigabit Ethernet is capable of operating in either half duplex or full duplex modes.

9.12 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 :

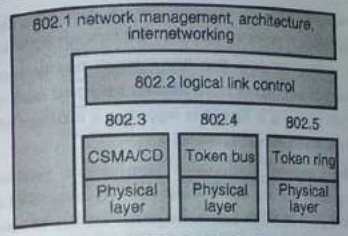
802.1	Architecture, Management and Internetworking
802.2	Logical Link Control (LLC)
802.3	Carrier Sense Multiple Access/Collision Detect (CSMA/CD)
802.4	Token Bus
802.5	Token Ring
802.6	Metropolitan Area Networks (MANs)
802.7	Bandpass Technical Advisory Group
802.8	Fibre Optic Technical Advisory Group
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. 9.12.1.

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. 9.12.1 : IEEE LAN and related standards**

9.13 Traditional Ethernet : MU : May 17

University Questions

Q. 1 Write short note on traditional Ethernet. **(May 17, 5 Marks)**

- 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.

9.13.1 Traditional Ethernet Frame :

Fig. 9.13.1 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

Fig. 9.13.1 : Traditional Ethernet frame

Frame format :

- The 64-bit (8 bytes) preamble allows the receiver to synchronize with the signal, it is a sequence of alternating 0's and 1's.

DA and SA :

- Both the source and destination hosts are identified with a 48-bit (6 bytes) address. These are indicated by the 6 byte number entered in the destination address (DA) and source address (SA) fields of the frame.
- The packet type field serves as the de-multiplexing key.

Data :

- Each frame contains upto 1500 bytes of data. The minimum size of a frame is 46 bytes of data, the reason for this is that the frame must be long enough to detect a collision. Each frame includes 32 bit (4 bytes) checksum. CRC is the last field in the Ethernet frame.
- The Ethernet is a bit-oriented framing protocol. An Ethernet frame has 14-byte header, two 6-bytes addresses and 2-byte type field.
- The sending adapter attaches the preamble, CRC and postamble before transmitting and the receiving adapter removes them.

Start Frame Delimiter (SFD) :

- This is the second field in the Ethernet frame and it is of 1 byte length. The byte stored at this field is 10101011.
- This field signals the beginning of the frame.
- The SDF is used to communicate to the station that this is the last chance for synchronization.
- The last two bits 11 alert the receiver that the next field in the frame contains the destination address.

9.13.2 Frame Length :

- There is a restriction imposed on the minimum and maximum length of the frame of the Ethernet.
- The minimum frame length is 512 bits or 64 bytes and the maximum frame length is 12,144 bits or 1518 bytes.
- The format of the minimum length frame is shown in Fig. 9.13.2(a) and that of the maximum length frame is shown in Fig. 9.13.2(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. 9.13.2 : 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.

Scanned by CamScanner

9.13.3 Addressing :

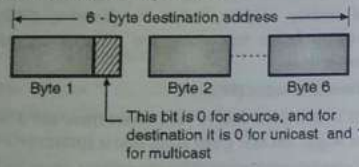
- There can be various types of stations connected on an Ethernet network such as PC on workstation or printer.
- Each station has its own network interface card (NIC) which fits inside the station to contain the 6 byte physical address of the station.
- Fig. 9.13.3 shows a 6-byte Ethernet address in the hexadecimal notation.

04 – 02 – 01 – 06 – 1C – 5B

(G-307) **Fig. 9.13.3 : Ethernet address**

9.13.4 Types of Addresses :

- A source address is only unicast address. This is because the frame comes from only one source.



(G-308) **Fig. 9.13.4 : Difference between unicast and multicast addresses**

- The destination address can be one of the following three types :
  1. Unicast 2. Multicast 3. Broadcast
- Fig. 9.13.4 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.

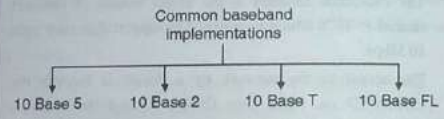
3. **Broadcast address :**
   - Broadcasting process is the process in which the sender transmit and all others receive or listen.
   - This type of destination address is a special case of multicast address in which all stations are destinations.

9.13.5 Physical Properties of Ethernet :

- Let us see some physical properties of Ethernet. An Ethernet segment is implemented on a coaxial cable of upto 500 m.
- A **transceiver**, which is a small device directly attached to the tap, detects when the line is idle and drives the signal when the host is transmitting. Tap must be at least 2.5 m apart.
- Transceiver also receives incoming signals. It is in turn, connected to an Ethernet adapter, which is plugged into the host. All the power of Ethernet is in adapter.
- Multiple Ethernet segments can be joined together by repeaters. A **repeater** is a device that forwards digital signals.
- Note that, no more than four repeaters may be positioned between any pair of hosts. Ethernet has a total reach of only 2500 m and it is limited to supporting a maximum of 1024 hosts with 100 base T, twisted pair.
- The common configuration have several point-to-point segments coming out of a multi-way repeater, called a hub, multiple 100-Mbps Ethernet segments can also be connected by a hub.

9.14 Physical Layer Implementation of Standard Ethernet :

The standard has defined four different implementations for the baseband (digital) 10 Mbps Ethernet as shown is Fig. 9.14.1.



(G-312) **Fig. 9.14.1 : 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.

9.15 Fast Ethernet :

- Fast Ethernet is the protocol designed to work upto 100 Mbps and it is compatible with the standard Ethernet.
- The traditional Ethernet can operate only upto 10 Mbps. Hence for higher data rates fast Ethernet has been developed.

9.15.1 MAC Sublayer and Topology :

- 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 topology 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.

9.15.2 Autonegotiation :

This is the new feature of the fast Ethernet. Due to this feature the two stations can make the negotiation on the mode or data rate of operation.

Features of the autonegotiation :

The important features of autonegotiation are :

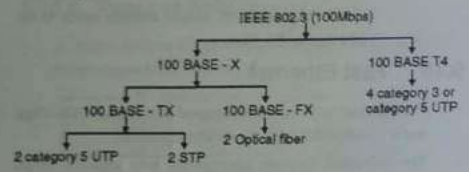
1. The non-compatible devices can be connected to each other.

Scanned by CamScanner

2. One device can be allowed to have multiple capabilities.
3. A station can check hub's capabilities.

9.15.3 Physical Layer Implementation :

- Fig. 9.15.1 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. 9.15.1 : IEEE 802.3 100 BASE – T options**

- All of the 100 BASE – T options shown in Fig. 9.15.1 use the IEEE 802.3 MAC protocol and frame format.
- 100 BASE – X indicates the options which use the medium specifications defined by FDDI.
- 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. 9.15.1. 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.

9.16 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.

9.16.1 MAC Sublayer :

- The MAC sublayer cannot 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

  Slot time = $512 \text{ bits} \times 1 \times 10^{-9}$ sec. = 0.512 µsec.
- Due to reduced slot time, the collision is detected 100 times earlier and therefore the maximum length of the network is restricted to only 25 m i.e. 100 times less than the maximum length of the traditional Ethernet (2.5 km).
- This length is very short and not suitable for connecting computers even in one single office.
- Due to these demerits the traditional approach is not suitable.

2. Carrier extension method :

- In order to increase the length of the network the minimum frame length is increased to 512 byte i.e. 4096 bits in the carrier extension approach.
- This is 8 times longer than the minimum frame size of 64 bytes in the traditional approach. Therefore the maximum length of the network also is increased 8 times and becomes $25 \times 8 = 200$ m.

3. Frame bursting :

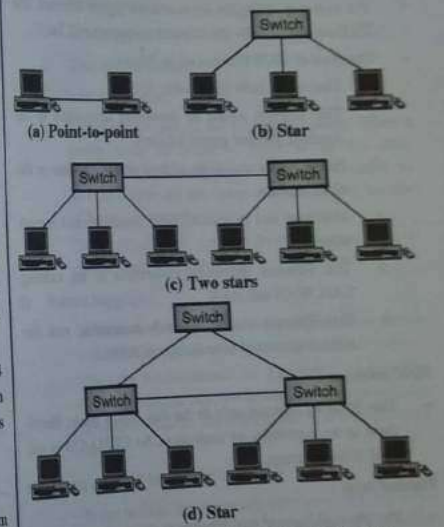
- The carrier extension technique increases the maximum length of the network. But it is very inefficient technique because for sending short frames we need to send a lot of redundant data so a make the frame length equal to 4096 bits.
- The efficiency can be increased with the help of the **frame bursting** 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.

9.16.2 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. 9.16.1(c) and (d).

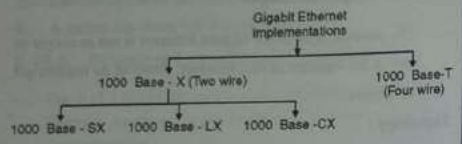


(L-799) **Fig. 9.16.1 : Topologies of Gigabit Ethernet**

9.16.3 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. 9.16.2 shows the physical layer implementations for the Gigabit Ethernet.

Scanned by CamScanner



(G-323) **Fig. 9.16.2 : 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.

9.16.4 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 :

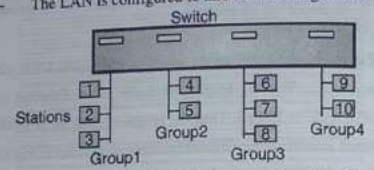
- This Ethernet operates only in the full duplex mode. Hence there is no possibility of contention. So CDMA/CD is not used in this Ethernet.

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-l
  3. 10 G Base-E

9.17 Virtual LANs :

- The virtual local area network (VLAN) is a LAN configured not by physical wiring like conventional LAN but it is configured by software.
- It is developed in order to establish a connection between two stations belonging to two different physical LANs.
- The concept of VLAN technology is based on dividing a LAN into logical instead of physical segments. A LAN can be divided into several logical LANs called VLANs.
- The concept of VLAN will be clear after referring to Fig. 9.17.1 which shows the conventional switched LAN.
- The total number of stations are grouped into 4 groups and the groups are connected by a switch.
- The LAN is configured to allow this arrangement.

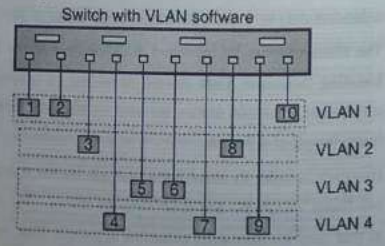


(L-744) **Fig. 9.17.1 : A conventional LAN**

- In a conventional LAN if we wish to transfer stations 1 and 2 from group 1 to any other group, then the LAN configuration needs to be changed. Rewiring would be required.
- This is the biggest problem in the conventional LAN. But the problem is solved by using a VLAN.

9.17.1 VLAN Configuration :

- Fig. 9.17.2 shows the configuration of VLAN connecting the same ten stations in four VLAN segments.
- The total stations are divided in four logical instead of physical segments. A LAN can be divided into several logic LANs called VLANs.
- It is possible to move one station from one group to any other group without changing the physical configuration because the membership of a group is defined by software and not by hardware.
- Any station can be moved logically to another VLAN.
- All the members corresponding to a VLAN can receive the broadcast message broadcast sent to that VLAN.
- Using the VLAN technology it is even possible to group stations connected to different switches.
- VLAN is very useful for a company having two separate buildings.



(L-745) **Fig. 9.17.2 : VLAN configuration**

- Thus VLANs group stations belonging to one or more physical LANs into broadcast domain. The stations in a VLAN communicate with each other as if they belong to the physical segment.

9.17.2 Membership :

- There are various characteristics used to group various stations in a VLAN.
- Some of such characteristics are port number, MAC addresses, IP addresses, IP multicast address. We can use them singly or a combination of two or more characteristics for grouping various stations in VLAN.

1. Port number :

- An administrator may define that the stations connected to ports 1, 3, 5, 7 of a switch correspond to VLAN-1, the stations connecting to ports 2, 4, 6, 8 correspond to VLAN-2 etc. So in this case the port number of the switch is being used as a membership characteristic.

2. MAC addresses :

- The 48 bit MAC address is used as a membership characteristics by some vendors. The stations having particular MAC addresses are grouped together to form VLAN-1. The stations having some other MAC addresses form VLAN-2 etc.

3. IP addresses :

- The 32-bit IP addresses are used as membership characteristics by some vendors. The principle is same as that for the MAC addresses.

4. Multicast IP addresses and combinations :

- Some vendors use the multicast IP addresses as a membership characteristics and some of them use the combination of all the characteristics mentioned earlier to form the VLANs.

9.17.3 Configurations :

The grouping of stations in a VLAN can be carried out by using one of the following configurations :

1. Manual configuration
2. Automatic configuration
3. Semiautomatic configuration.

1. Manual configuration :

- In the manual configuration, the network administrator assigns the stations to different VLANs using VLAN software but manually.
- If required, the migration of a station from one VLAN to the other also takes place manually.
- Since VLAN is a logical configuration, all the assignments and migrations take place via VLAN software.

2. Automatic configuration :

- In an automatic configuration, the stations are brought into or taken out of the VLANs automatically.
- The criteria for connection or otherwise is defined by the administrator.

3. Semi automatic configuration :

- This configuration is in between the manual and automatic configurations. The initialization process is done manually whereas the migration is an automatic process.

9.17.4 Communication between Switches :

- In the backbone using multiple switches each switch is supposed to know the stations and their VLANs and the membership of stations connected to each switch.
- Methods devised for the purpose of communication between switches are as follows :
  1. Table maintenance
  2. Frame tagging.
  3. Time division multiplexing.

1. Table maintenance :

- This method works in the following manner. When a station sends its broadcast frame to all the other members of its own group, the switch will create an entry in a table and note down the membership number of the broadcasting station.
- The modified tables are sent by the switches to each other periodically for updating.

2. Frame tagging :

- In this method, when a frame is moving from one switch to the other, an extra header is added to its MAC frame.
- This extra header defines the destination VLAN. The receiving switches then use this header to determine the destination VLANs. The extra header is known as frame tag.

3. Time division multiplexing (TDM) :

- In this method, the connection between switches is done on the basis of time sharing of channels which is the principle of TDM.
- If there are six VLANs connected in a backbone network, then each trunk (connection) is divided into six channels.
- Channel 1 is designated to VLAN-1 channel 2 to VLAN-2 and so on.

IEEE standard :

- In late 1990s the IEEE 802.1 committee passed a new standard called 802.1 Q to define the format for frame tagging.
- This standard defines the format used in multiswitched backbones as well.

Scanned by CamScanner

- 802.1 Q is the first step towards the future standardisation and most vendors have already accepted this standard.

9.17.5 Advantages of VLANs :

Some of the advantages are :

1. Reduction in cost.
2. Saving of time required for rewiring.
3. No need to change the physical configuration.
4. VLANs provide additional security. The message broadcast in one group cannot be listened by members of other groups.

Review Questions

Q. 1 Explain the layered architecture of LAN explaining the function of the LLC and MAC sublayer.

Q. 2 What is static and dynamic channel allocation ?

Q. 3 Compare and explain the pure and slotted ALOHA system.

Q. 4 Explain the different CSMA protocols.

Q. 5 What is CSMA with collision detection ?

Q. 6 Why there is no need of CSMA/CD for a full duplex Ethernet LAN ?

Q. 7 Explain CSMA/CD.

Q. 8 What is CSMA/CA ?

Q. 9 Write a note on : Physical layer implementation in traditional Ethernet.

Q. 10 Compare the data rates of traditional, fast and Gigabit Ethernets.

Q. 11 Explain the physical layer implementation in fast Ethernet.

Q. 12 What are the common fast Ethernet implementations ?

Q. 13 Compare the reconciliation sublayer in Fast Ethernet with the PLS sublayer in traditional Ethernet.

Q. 14 What is GMII in Gigabit Ethernet ?

Q. 15 What is Fast Ethernet ?

Q. 16 Explain the LLC and MAC in IEEE 802 standard and explain the operation of CSMA/CD as used in LAN.

❑❑❑

CHAPTER 10

Module V

Other Wired Networks

Syllabus :

Point to point networks, SONET, Switched network : ATM, Connecting devices : Repeaters or hubs, Link layer switches, Routers, Sliding window compression.

10.1 Other Wired Networks :

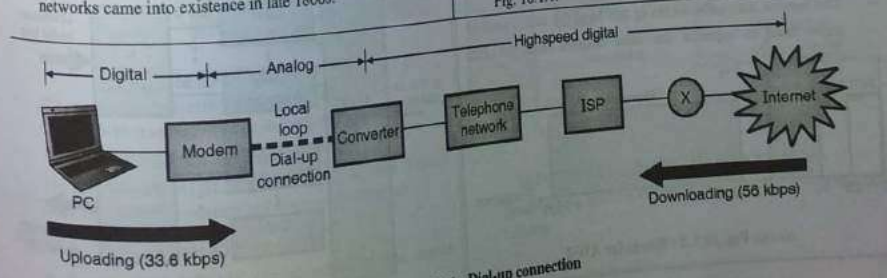
- Either LANs or WANs are the networks which come across the internet.
- But there is one dispute in the terminology i.e. some access networks e.g. dial-up connection or cable connection are known as wide area networks (WAN) by some people where as other people call it as MAN (metropolitan area networks).
- In this section we will discuss direct or indirect use of these networks-without calling them WAN or MAN. We will call them just as networks.

10.1.1 Point-to-point Networks :

- To provide internet access from internet user premises, point-to-point networks such as cable, dial-up and DSL are used.
- There is no use of media access control (MAC) because there is dedicated connection between the two devices. PPP (point to point protocol) is used in such a networks.

10.1.1.1 Dial-up Connection / Network :

- For transmission of data, dial-up network uses the services provided by the telephone networks.
- Telephone networks use circuit switching. The telephone networks came into existence in late 1800s.
- The POTS (Plain Old Telephone System) is the old telephone network which used analog system and analog signals to transmit voice.
- After the invention of computers, the telephone network in 1980s started carrying data in addition to the voice signals.
- During the recent years, the telephone network has changed a lot. The network is now digital.
- The line which connects the subscriber to the telephone network is analog.
- Dial-up modem is invented for digital data communication.
- The term 'MODEM' is derived from the words MOdulator and DEModulator. A MODEM contains a modulator as well as demodulator.
- The function of modulator is to generate an analog signal from digital data.
- The function of demodulator is to recover the digital data from the modulated signal.
- If only one party is using digital signaling then only these connections can be used. (e.g. through an Internet provider).
- There is asymmetry in the uploading and downloading rate.
- The data flow from ISP (Internet Service Provider) to the PC i.e. downloading rate is maximum of 56 kbps.
- The data flow from PC to ISP i.e. uploading rate is maximum of 33.6 kbps.
- Dial-up connection to provide Internet access is as shown in Fig. 10.1.1.



(G-2216) Fig. 10.1.1 : Dial-up connection

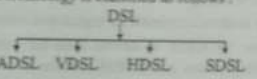
Scanned by CamScanner

- In **uploading**, it is necessary that the analog signal should be sampled before it enters into high speed digital telephone network.
- The uploading rate is reduced to 33.6 kbps because quantization noise is introduced into the signal.
- In **downloading**, there is no effect of quantization noise on the signal because there is no sampling.
- To access the Internet, user requires high speed for downloading as compared to uploading.
- Note that, if a telephone line is used then it is not possible to access the internet and voice communication at the same time. While accessing the Internet we cannot use it for voice communication.
- The question arises that how we reach at the speed of 56 kbps ? Telephone system use 8-bits per sample to make 8000 samples per second. In each sample one bit is used for control purpose. That means rate = 8000 × 7 = 56000 bps or 56 kbps.

10.1.1.2 DSL (Digital Subscriber Line) :

- DSL stands for digital subscriber line and it has been developed for providing a high-speed access to the Internet.
- It allows the user a high speed digital communication over the existing local loops.
- The DSL technology is classified as follows :

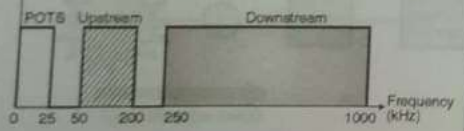
(G-162)



- Thus DSL technology is actually a set of technologies which is referred to as xDSL where x can be A, V, H or S.

ADSL :

- The long form of ADSL is asymmetrical DSL.
- Similar to 56 k modem, it provides higher bit rate in the downstream direction (from Internet to the user) as compared to the bit rate in the upstream direction (from user to Internet). This is why it is called as asymmetrical.
- ADSL divides the bandwidth of a twisted pair cable of 1 MHz into 3 bands as shown in Fig. 10.1.2.
- The first band is between 0 and 25 kHz. It is used for regular telephone (Plain Old Telephone Sets - POTS).
- This service uses only 4 kHz of this band the rest is used as guard band to separate the voice channel from the data channels.



(G-163) **Fig. 10.1.2 : Bands for ADSL**

- The second band is from 50 kHz to 200 kHz. It is used for upstream data communication.
- The third band is from 250 kHz to 1 MHz. It is used for downstream data communication.
- ADSL technology is designed for the home users. It is not suitable for business applications because such applications need larger bandwidth than the home users.

Use of Existing Local Loop :

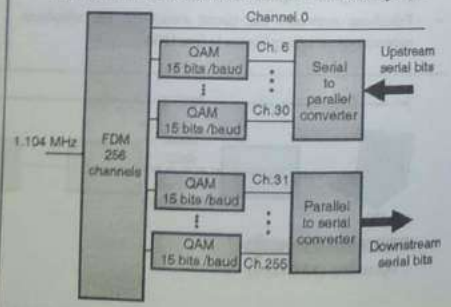
- The ADSL uses the existing local loop and still it can support very high data rates. Let us see how.
- Actually the twisted pair local telephone cable can support the bandwidth upto 1.1 MHz. The bandwidth reduces to 4 kHz due to the filters installed at the end of line.
- If this filter is removed then the bandwidth can again become 1.1 MHz.
- Hence the existing local loop with this modification can have a bandwidth of 1.1 MHz and ADSL can make use of the existing loop for voice as well as data communication.

Adaptive Technology :

- The bandwidth of 1.1 MHz is not always available practically. It will depend on various factors such as distance, cable size, type of signaling etc.
- So ADSL has been designed to operate as an adaptive technology. That means depending on the conditions and actually available bandwidth, the data rate of ADSL is adjusted.
- Thus ADSL is an adaptive technology. The data rate of the system is adjusted based on the conditions of the local loop.

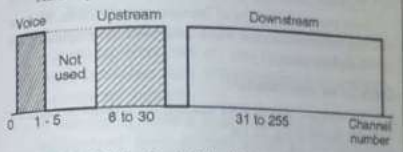
Discrete Multitone Technique (DMT) :

- DMT is the standard modulation technique for ADSL. It is a combination of QAM and FDM techniques.
- Typically the available bandwidth of 1.1 MHz is divided into 256 channels. However this is not a rule. The division may change system to system.
- Fig. 10.1.3 shows the block schematic of the DMT system.



(G-164) **Fig. 10.1.3 : Block diagram of DMT**

- Channel 0 is reserved for the voice communication.
- Channels 1 to 5 are called as **idle channels** since they are not used. These channels create a guard band between the voice and data channels.
- Channels 6 to 30 (25 channels) are used for the upstream data transfer and control. 24 channels are for data transfer and one channel for control.
- For 24 channels (4 kHz each) with QAM modulation the bandwidth is 24 × 4 kHz × 15 or 1.44 Mbps in the upstream.
- The channels 31 to 255 (225 channels) are alloted for downstream data transfer and control. Out of 225 channels, one is reserved for control and remaining 224 are reserved for data.
- The downstream bit rate is 224 × 4 kHz × 15 = 13.4 Mbps. Fig. 10.1.4 shows the bandwidth allocation for this (DMT) ADSL system.



(G-165) **Fig. 10.1.4 : Bandwidth division in ADSL with DMT**

Actual bit rate :

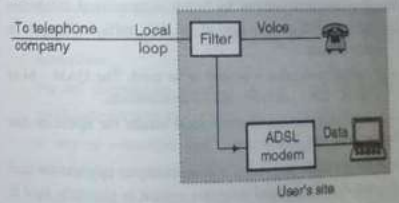
The actual bit rates are normally less than the theoretical values. The actual bit rates are as stated below :

Upstream : 64 kbps to 1 Mbps

Downstream : 500 kbps to 8 Mbps

ADSL Modem :

The ADSL modem installed at the users site is shown in Fig. 10.1.5.

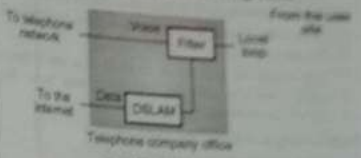


(G-1085) **Fig. 10.1.5 : ADSL modem**

- The local loop (pre-existing telephone wire) is connected to the filter which separates voice and data from each other.
- The voice goes to the telephone instrument.
- The data goes to ADSL modem which modulates it using DMT to create the upstream and down stream channels.

DSLAM :

- A device called DSLAM (digital subscriber line access multiplexer) is installed at the telephone company site.
- Its function is very similar to that of the 56k modem with an additional function of packetizing the data to be sent to the Internet ISP server.
- The DSLAM configuration is shown in Fig. 10.1.6.



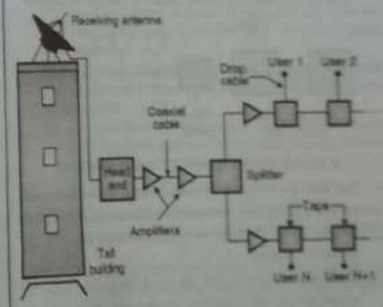
(G-167) **Fig. 10.1.6 : DSLAM**

10.1.1.3 Cable TV :

- Now-a-days, the cable companies have come forward to provide high-speed access to the Internet.
- Due to the DSL technology, it has become possible to provide the high data rate connection for the residential user on the local loop.
- But DSL technology, uses the existing unshielded twisted pair cable which does not perform well in the presence of external interference or noise.
- So the data rate on such cables cannot be increased beyond a certain limit.
- A solution to this problem is to use the cable TV network.

Traditional Cable TV Network :

- Fig. 10.1.7 shows the block schematic of the traditional cable TV system.



(G-170) **Fig. 10.1.7 : Traditional cable TV system**

- The receiving antenna is generally set up on the top of a tall building.

Scanned by CamScanner

- It receives the video signals from the broadcasting stations and supplies them to the cable TV office called the head end.
- The head end processes these signals and feeds them into coaxial cable.
- Amplifiers are inserted at regular intervals in order to amplify the signal passing from the head end to the user's house.
- There could be upto 35 amplifiers between the head end and the user's premises.
- The splitters are used to split the signal from one to many paths. Then the taps and the drop cables make the connections to the users residences.

Disadvantages of traditional cable system :

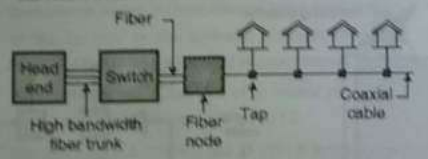
1. A large number of amplifiers are required.
2. The bandwidth of the coaxial cable is limited.
3. Due to the use of amplifiers, the system becomes unidirectional. Signals can travel only from head end to the users residence.

The biggest disadvantages of the traditional cable TV network is that this network is unidirectional.

Internet over cable / Hybrid fiber - coaxial (HFC) network :

- After the growth of cable TV system, the cables between various cities were replaced by high band width fiber.
- A system that uses optical fiber for long haul runs and a coaxial cable to the houses is called as a **Hybrid Fiber Coaxial (HFC) system.**
- The electro-optical converter which interfaces between the fiber and coaxial cable (see Fig. 10.1.8) is called as the **fiber node.**
- The bandwidth of fiber is much higher than that of the coaxial able. So it is possible for a fiber node to feed a number of coaxial cables.

The recent trend is to use the cable TV network for Internet.

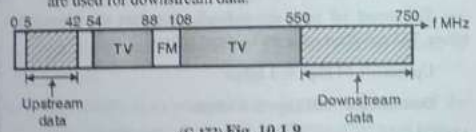


(G-171) **Fig. 10.1.8 : A cable TV system using HFC**

- But there are certain difficulties in doing so, due to the basic technical differences between the cable system and telephone system. These are to be sorted out for using the cable. TV system for Internet.
- The first difference is that the amplifiers used in cable TV system are one way amplifiers, but the amplifiers required for Internet (and telephone) are two-way amplifiers.
- Hence every one way amplifier has to be replaced by a two way amplifier.
- When used only for T.V., one cable is shared by many houses. But when the same system is to be used for Internet (or telephone) every house must have its own private local loop.
- The sharing of single cable does not pose any problem for the cable TV viewers. The number of users (10, 100 ...) also does not pose any problem.
- But if the same cable is to be used for Internet access, then the number of users (10, 100,1000 ...) plays a very important role.
- If one user decides to download a large file, then that bandwidth is being taken away from the other users.
- So more the users, more is the competition for bandwidth.
- The cable TV system has overcome this problem by splitting up long cables and connecting each one directly to the fiber node. This will solve the problem of bandwidth.
- Typically cables now a days have 500 to 2000 houses. But with increase in number of Internet users on cable, the load may become excessive which may need more splitting and more fiber nodes.

Cable TV for data transfer :

- The spectrum allocation for enabling the Internet on cable TV is as shown in Fig. 10.1.9.
- The upstream channels are introduced in the 5-42 MHz band and the frequencies at the higher end (550 MHz to 750 MHz) are used for downstream data.



(G-172) **Fig. 10.1.9**

- Fig. 10.1.9 shows that the bandwidth allocated for upstream data is much smaller than that for the downstream data.
- But there is no problem due to this asymmetrical distribution of bandwidth because most of the data traffic is likely to be downstream.
- Analog modulation is needed to be used. The QAM - 64 or QAM - 256 is generally used for downstream.
- But QAM does not produce good results for upstream data transfer. So QPSK is used.
- Alongwith the amplifiers, it is necessary to upgrade the head end as well. A digital computer system is generally used in place of the head end. The name head end is changed to CTMS (cable Modem Termination System).
- To provide Internet access bandwidth is divided into three bands :

  1. Video (TV) 2. Downstream data 3. Upstream data
- To provide Internet access bandwidth is divided into three bands :
  1. Video (TV) (54 to 550 MHz)
  2. Downstream data (550 to 750 MHz)
  3. Upstream data (5 to 42 MHz)

- The frequency range of video band is 54 to 550 MHz. This band contain more than 80 channels because each TV channel occupies 6 MHz.
- From the Internet to the subscriber premises i.e. downstream data occupies the upper band (550 to 750 MHz). Upper band is also divided into 6 MHz channels.
- Lower band is occupied by upstream data (5 to 42 MHz) i.e. from the subscriber premises to the Internet. This band is divided into 6 MHz channels.
- In QPSK there are 2 bits per baud. That means 1 Hz for each baud is standard specification. (2 bits / baud × 6 MHz) = 12 Mbps i.e. Generally data rate is less than 12 Mbps.

Sharing :

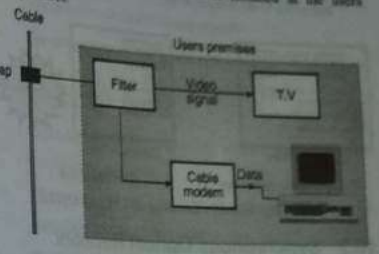
- The subscribers share both upstream and downstream bands. The bandwidth of upstream data is 37 MHz. i.e. In upstream direction six 6 MHz channels are available.
- In the upstream direction, to send data subscriber needs only one channels.
- The question arises that, in an area where more subscribers available i.e. 1000, 3000 etc. then how six channels can be shared in between them ? **Time-sharing** is the solution to overcome this problem.
- In time-sharing, band is divided into channels, in the same neighborhood these channels should be shared between subscribers.
- For a group of subscriber statically or dynamically cable provider assigns one channel.
- If any subscriber wants to transmit data, he/she competes for the channel with other subscriber who also want to access the channel. Untill the channel become available, the subscriber should have to wait.
- In the downstream direction we have similar situation like upstream direction. There are 33 channels of a 6 MHz in the downstream band.
- Between a group of subscribers each channel is shared because probably a cable provider has more than 33 subscribers.
- For the downstream direction the situation is different i.e. multicasting situation.
- If any of subscriber in the group have any data, to that channel this data is sent. The data is sent to each subscriber.
- Each subscriber has an address registration with the cable provider. Here the function of cable modem for the group is to match the address assigned by the cable provider with the address carried with the data. The data are kept if the address matches otherwise data are discarded.

Cable network for data transmission :

- In order to utilize the cable network for data transmission we have to use two devices namely CM (cable modem) and CTMS (cable modem transmission system).

Cable Modem (CM) :

- Fig. 10.1.10 shows the block schematic of cable modem. It is similar to ADSL modem and it is installed at the users premises.

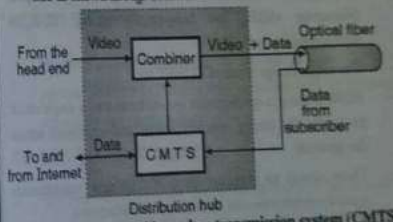


(G-173) **Fig. 10.1.10 : Cable modem (CM)**

- The cable is tapped to obtain the signal and it is applied to a filter.
- The filter separates out video and data in the incoming signal from the cable.
- The video signal is applied to TV whereas the data signal is applied to the computer via the cable modem.

Cable Modem Transmission System (CMTS) :

- The cable companies install the CMTS inside the distribution hub as shown in Fig. 10.1.11.



(G-174) **Fig. 10.1.11 : Cable modem transmission system (CMTS)**

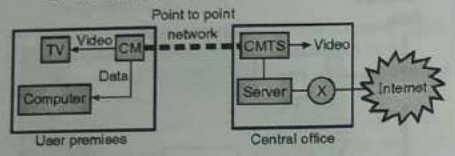
- The data from Internet is passed through the CMTS to the combiner. The video signal from the head end also is applied to the combiner.
- The combiner output contains video as well as data from the Internet. This signal is put on the optical fiber for routing it to the subscribers.
- The data from the subscribers coming via the optical fiber is applied to the CMTS, and the CMTS passes it to the Internet (upstreaming).

CM and CMTS :

- Inside the cable company the CMTS (cable modem transmission system) is installed. CMTS is like ADSL modem.
- From the Internet CMTS receives the data and it sends data to the subscriber. It also receives data from the subscriber and it sends to the Internet.
- The location of CM and CMTS is shown in Fig. 10.1.12.
- Similar to DSL technology, the cable company requires to become an Internet service provider (ISP) which can provide internet services to the subscriber / users.

Scanned by CamScanner

- Cable modem (CM) at the users premises separates the video from data and after separation it sends data to the computer and video to the television set.



User premises **Central office**

(G-2217) **Fig. 10.1.12 : Location of CM and CMTS**

10.2 Synchronous Optical Network (SONET) :

- The developments in optical communication have occurred at a rapid rate, and the backbone of telephone networks has become dominated by fiber optic digital transmission systems.
- SONET is optical transmission interface. It was proposed by Bellcore laboratories and was standardised by the American National Standard Institute (ANSI).
- **A compatible version, referred to as Synchronous Digital Hierarchy (SDH)** has been published by ITU-T in Recommendation G. 707.
- The major design goals of SONET are :
- SONET being a synchronous network requires a single clock to handle the timing synchronisation and equipment across the network.
- There should be standardisation of fiber optic transmission system equipments sold by different manufacturers.
- The physical specification and frame design must include mechanisms that will allow it to carry signals from incompatible tributary systems.
- SONET is a multiplexed transport mechanism and hence can be the carrier for broadband services such as ATM and B-ISDN.
- SONET is basically a time division multiplexing (TDM) system.

> **Note :** Thus SONET is a synchronous TDM system which is controlled by a master clock.

10.2.1 Architecture :

Let us discuss the architecture of the SONET system which includes signals, devices and connections.

10.2.2 Synchronous Transport Signals :

- A hierarchy of signaling levels is defined for SONET. Such hierarchy is called as synchronous transport signal (STS).
- There are 192 STS levels (STS-1 to STS-192). Each one supports a specific data rate is shown in Table 10.2.1.

Table 10.2.1 : SONET rates

STS	OC	RAW (Mbps)	SPE (Mbps)	User (Mbps)
STS – 1	OC – 1	51.84	50.12	49.536
STS – 2	OC – 3	155.52	150.336	148.608
STS – 3	OC – 9	466.56	451.008	445.824
STS – 4	OC – 12	622.08	601.344	594.432
STS 192	OC – 192	9953.28	9621.6	9510.9

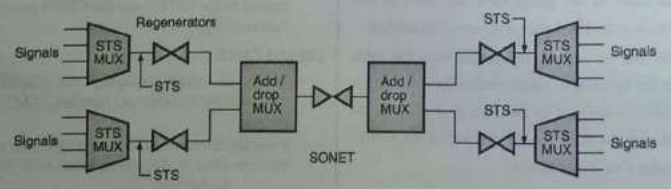
- **Optical carriers (OCs) :** The optical carriers or OCs are the physical links which are defined to carry each level of STS.
- This is similar to the T or E lines.
- The optical carrier level tell us about the conceptual and physical specifications of the optical links which are required to support the desired level of signaling.
- The most popular are OC-1, OC-3, OC-12 and OC-48.

10.2.3 SONET Devices :

- There are three basic SONET devices.

1. Synchronous transport signal (STS) multiplexers.
2. Regenerators.
3. Add/drop multiplexers.

- Fig. 10.2.1 shows an example of SONET.



(G-808) **Fig. 10.2.1 : Example of SONET**

Operation :

- The STS Multiplexer/Demultiplexer is used for two purposes. It multiplexes signals from various sources into an STS i.e. synchronous transport signal, or it demultiplexes an STS signal into various destination signals.
- The STS signal passes through a number of regenerators or repeaters while travelling from the source to destination.
- The regenerators are basically repeaters and are bidirectional devices.
- They will regenerate the STS applied to them. This will eliminate any effect of additive noise on the quality of transmission.
- The SONET regenerators function at the data link layer.
- The add/drop multiplexer is capable of adding signals from various sources or it can remove any signal and redirect it without demultiplexing the entire multiplexed signal.

10.2.4 Terminals :

We define the **terminal** as a device that uses the services of SONET network. The example of a terminal is a router.

10.3 Connections :

The SONET devices are connected to each other using sections, lines and paths.

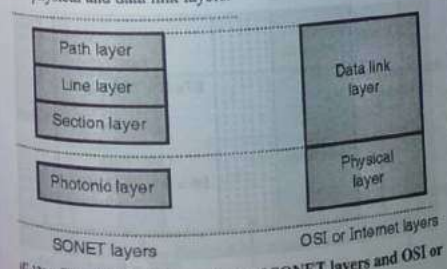
1. **Sections :** A section is defined as the optical link that connects two neighbouring devices such as multiplexer, regenerator etc.
2. **Lines :** A line is defined as the portion of network between two multiplexers.
3. **Path :** A path is defined as the end to end portion of the network between two STS multiplexer.

10.4 SONET Layers :

- The SONET standard defines four layers namely :

1. The photonic layer
2. The section layer
3. The line layer
4. The path layer

- As shown in Fig. 10.4.1 these layers correspond to the physical and data link layers.



(G-1316) **Fig. 10.4.1 : Comparison of SONET layers and OSI or internet layers**

10.4.1 Path Layer :

- The path layer has to perform the task of signal movement from source to destination.
- The optical source converts the signal from an electrical form into an optical form. Then it is multiplexed and encapsulated in a frame.
- At the destination the process followed is exactly opposite to that followed at the source.
- The received frame is demultiplexed and the optical to electrical conversion takes place.
- The path layer overhead is added at this layer and STS multiplexers provide the path layer functions.

10.4.2 Line Layer :

- This layer has to perform the task of signal movement across a physical line.
- Line layer overhead is added to the frame at this layer. STS multiplexers and add/drop multiplexers perform the functions of the line layer.

10.4.3 Section Layer :

- This layer has the responsibility of moving the signal across a physical section of performs the operations such as framing, scrambling and error control.

10.4.4 Photonic Layer :

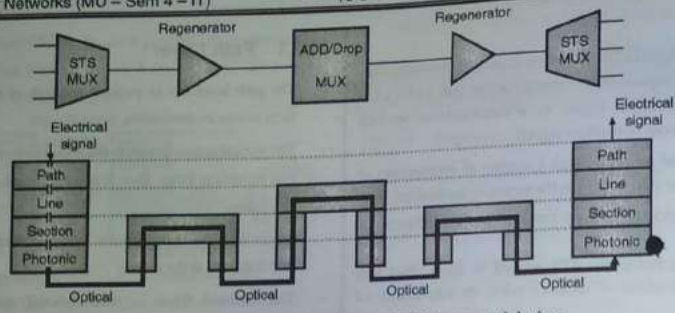
- The photonic layer is the lowest of the SONET layers and it corresponds to the physical layer of the OSI or Internet model.
- The photonic layer specifies the physical specifications of the optical fiber channel. The receiver sensitivity and multiplexing.
- The type of encoding used by SONET is the NRZ encoding as follows :

Presence of light	1
No light	0

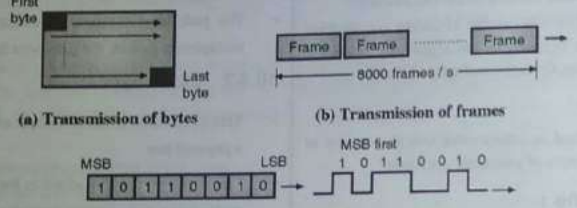
10.4.5 Relationship between Devices and Layers :

- The relationship between the four SONET layers and the SONET devices is illustrated in Fig. 10.4.2.

Scanned by CamScanner



(G-1317) **Fig. 10.4.2 : Relation between SONET layers and devices**



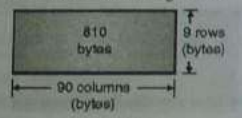
(a) Transmission of bytes **(b) Transmission of frames**

(c) Bit transmission

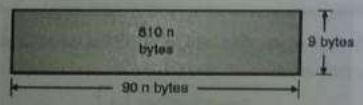
(G-1319) **Fig. 10.5.2 : Transmission of bytes, frames and bits**

10.5 SONET Frames :

- Each STS-n signal is made of 8000 frames. Each frame is a two dimensional matrix as shown in Fig. 10.5.1.
- Each frame matrix has dimensions of 9 rows by 90n columns. For example the frame matrix of STS-1 has dimensions of 9 rows × 90 columns as shown in Fig. 10.5.1.



(a) STS-1 frame



(b) STS-n frame

(G-1318) **Fig. 10.5.1 : Frame formats**

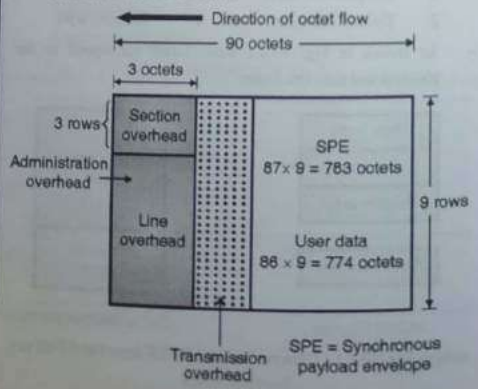
- The STS-3 signal will have the frame of dimensions 9 rows × 270 columns = 2430 bytes.

10.5.1 Frame, Byte and Bit Transmission :

- It is important to note that each STS-n signal has the same frame transmission rate of 8000 frames/sec.
- Inside each frame, the bytes are transmitted from left to right and top to bottom as shown in Fig. 10.5.2(a).
- For each byte the bits are transmitted from MSB to LSB as shown in Fig. 10.5.2(c).
- The frame transmission rate (8000 frames/sec) is same as the rate at which voice is digitised. If the voice signal is sampled and each sample is represented by a byte (8 bits) then each byte in a SONET frame can carry information about voice in the digital manner.

10.5.2 STS-1 Frame Format :

- Fig. 10.5.3 shows the SONET frame. It is basically a matrix of nine rows of 90 octets each. Thus the total number of octets is 9 × 90 = 810 octets.

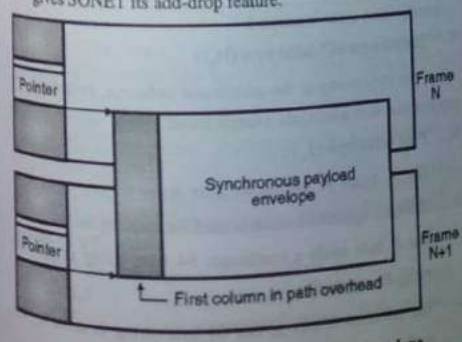


(G-809) **Fig. 10.5.3 : SONET frame**

- The first three columns i.e. 3 × 9 = 27 octets are reserved for the administration overhead.
- The remaining frame area i.e. 87 × 9 = 783 octets is called as synchronous payload envelope (SPE).
- The SPE is made of transmission overhead and user data.
- The administration overhead section is divided into two subsections namely section overhead and line overhead.
- The section overhead is used to provide framing, error monitoring and management functions. It is interpreted and modified at every section termination.
- The line overhead is used to provide synchronisation and multiplexing for the path layer as well as protection-switching capability. It is interpreted and modified at every line termination.
- The remaining 87 columns of the frame consist of the information payload that carries the path layer information. The bit rate of the information payload for the STS-1 is given as,

$$8 \times 9 \times 87 \times 8000 = 50.122 \text{ Mbps}$$

- The information payload consists of one column of path overhead information. It is not necessary that the path overhead may occupy the first column but it can be any number in the 87 columns. The line overhead contains a pointer that indicates where the path overhead starts.
- The user data and the path overhead are included in the Synchronous Payload Envelope (SPE) as shown in Fig. 10.5.4.
- As shown in the Fig. 10.5.4 the SPE consists of a byte array of 87 columns by nine rows. The path overhead constitutes the first column of this array.
- This SPE is then inserted into the STS-1 frame. As shown in the Fig. 10.5.4 the SPE can be spread over two consecutive frames.
- The use of the pointer makes it possible to add or remove a tributary signal from the multiplexed signal. This capability gives SONET its add-drop feature.



(G-810) **Fig. 10.5.4 : Synchronous payload envelope**

10.6 Overheads :

We are going to discuss three different types of overheads.

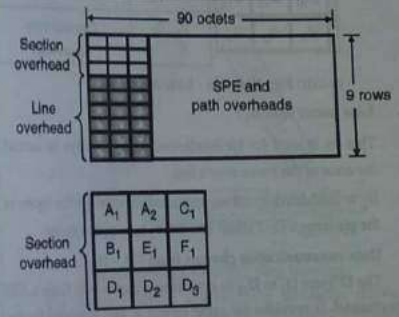
1. Section overhead
2. Line overhead
3. Path overhead.

10.6.1 Section Overheads :

- The section overhead is made of nine octets as shown in Fig. 10.6.1(a) and their functions are listed in Table 10.6.1.

Table 10.6.1 : Functions

A_1, A_2	Alignment bytes
B_1	Parity byte
C_1	Identification
D_1, D_2, D_3	Management
E_1	Order of wire byte
F_1	User



(G-1330) **Fig. 10.6.1(a) : Section overheads**

1. **Alignment bytes A_1, A_2 :**

The bytes A_1 and A_2 in the section overhead perform the following operations.

1. Framing
2. Synchronization
3. Alert the receiver that a frame is coming
4. They serve as flags.

2. **Section parity byte B_1 :**

This bit is used for bit interleaved parity, that means its value is calculated by taking all the bytes of the previous frame into consideration.

3. **Identification byte C_1 :**

This byte is used for identifying a STS-1 frame. This type of identification is necessary when multiple STS-1 frames are multiplexed.

4. **Management bytes D_1, D_2, D_3 :**

These bytes together form a data communication channel with a data rate of 192 kbps (3 × 8 ×8000). This channel is required for sending the operation, administration and maintenance (OA & M) signals.

Scanned by CamScanner

5. Order wire byte E_1 :

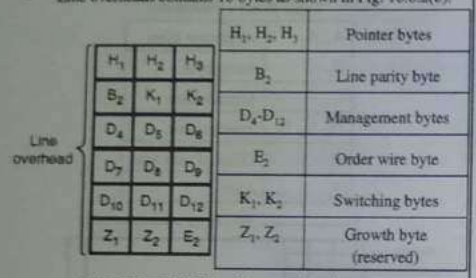
Order wire bytes in consecutive frames form a 64 kbps (8000 × 8 bits) channel which is used for communication between regenerators or between terminals and regenerators.

6. Users byte F_1 :

The users bytes in the consecutive frames form a 64 kbps (8 kbps × 8 bits per frame) which is reserved for users needs.

10.6.2 Line Overheads :

- Line overheads contains 18 bytes as shown in Fig. 10.6.2(b).



(G-1321) **Fig. 10.6.2(b) : Line overheads**

1. Line parity byte B_2 :

- This bit is used for bit interleaved parity. It helps to correct the error of the frame over a line.
- B_2 is calculated by taking into consideration all the bytes in the previous STS-1 frame and the B_2 byte of that frame.

2. Data communication channel bytes (D_4 - D_{12}) :

The D bytes D_4 to D_{12} in consecutive frames will form a 576 kbps channel. It provides the same service as that provided by the D_1 - D_3 bytes (OA & M) but the service is provided at the line level rather than the section level.

3. Order wire byte (E_2) :

The E_2 byte in the consecutive frames will form a 64 kbps channel to provide the same function as that of the E_1 byte.

The only difference is that the E_2 byte operates at the line level.

4. Pointer bytes (H_1, H_2, H_3) :

These are the pointer bytes. The bytes H_1 and H_2 are used for showing the offset of the SPE in the frame. The last byte H_3 is used for justification.

5. Protection switching bytes (K_1 and K_2) :

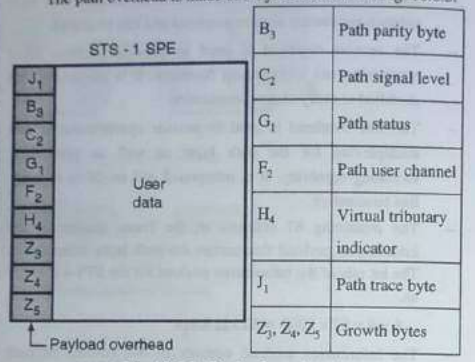
The K_1 and K_2 bytes are known as the automatic protection switching bytes. These bytes in the consecutive frames form a 128 kbps channel which is used for detecting problems automatically in the line terminating equipment.

6. Growth bytes (Z_1 and Z_2) :

The Z_1 and Z_2 bytes are reserved for the future development. Hence they are called as growth bytes.

10.6.3 Synchronous Payload Envelope (SPE) :

- The SPE contains user data and the path overhead which is the overhead related to the user data.
- The path overhead is added to the user data to create the SPE. The path overhead is made of 9 bytes as shown in Fig. 10.6.3.



(G-1322) **Fig. 10.6.3 : Payload overhead**

1. Path parity byte B_3 :

Similar to the bytes B_1 and B_2, the byte B_3 is for bit interleaved parity. However B_3 is calculated over SPE.bits.

2. Path signal level byte (BC_2) :

The byte C_2 is path identification byte which is used for identifying various higher level protocols such as IP or ATM. The data of these protocols is being carried in the SPE.

3. Path user channel byte (F_2) :

The F_2 byte in the consecutive frames form the 64 kbps channel which is reserved to take care of users needs, just like F_1 byte.

4. Path status byte (G_1) :

The receiver sends this byte to communicate its status to the sender. This byte is sent on the reverse channel if the duplex communication mode is adopted.

5. Multiframe indicator byte (H_4) :

This byte works as the multiframe indicator, to indicate the payload that does not fit into a single frame.

6. Path trace byte (J_1) :

- The J_1 bytes in the consecutive frames form a 64 kbps (8 kbps × 8) channel which is used for tracking the path.
- The J_1 byte sends a continuous 64 byte string in order to verify the connection.
- The selection of bits in this 64 byte string is done by the application program.

7. Growth bytes (Z_3, Z_4, Z_5) :

These bytes are reserved for the future growth.

10.6.4 Encapsulation :

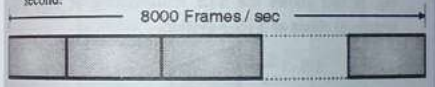
- Before sending, it is necessary to encapsulate an SPE in an STS-1 frame however encapsulation may create the following problems.
  1. Offsetting
  2. Justification.
- SONET deals with both these problems with the help of the pointer bytes (H_1 to H_3).

10.7 Frame Transmission :

- SONET frames are transmitted one after the other sequentially without any gap between them.
- This will continue even if there is no real data available for transmission. Empty frames are transmitted with dummy data.
- The first two bytes of each frame are called as alignment bytes while the third byte is for frame identification.

10.7.1 STS-1 :

- STS-1 or OC-1 is the service with lowest bit rate provided by SONET.
- Fig. 10.7.1 shows that STS-1 can transmit 8000 frames per second.



(G-1323) **Fig. 10.7.2**

- Various bit rates associated with STS-1 are as follows :
  1. Row rate = 8000 frames/s × 9 rows × 90 columns × 8 bits.
     = 51.84 Mbps.
  2. SPE rate = 8000 frames/s × 9 rows × 87 columns × 8 bits.
     = 50.12 Mbps.
  3. User rate = 8000 frames/s × 9 rows × 86 columns × 8 bits
     = 49.536 Mbps.

10.7.2 Virtual Tributaries :

Note :

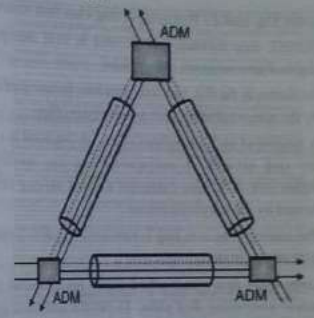
- SONET is used to carry broadband payloads but the current digital hierarchy data rates (DS-1 to DS-3) are lower than STS-1.
- To make SONET compatible with the digital hierarchy a system called Virtual Tributaries (VTs) is included in the system.
- A VT is a partial payload that can be inserted into an STS-1 and combined with other partial payloads to fill out the frame.

Types of VTs :

- There are four types of VTs as follows :
  1. VT 1.5 : It accommodates DS-1 service (1.544 Mbps).
  2. VT 2 : It accommodates European CEPT-1 service (2.048 Mbps)
  3. VT 3 : It is designed for accommodating the DS-1C service (fractional DS=1, 3-152 Mbps).
  4. VT 6 : It is designed for accommodating the DS-2 service (6-312 Mbps).

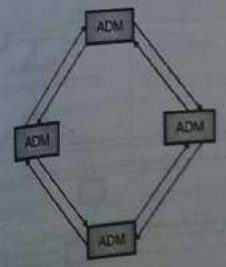
10.8 SONET Networks :

- The SONET equipment in combination with the Add-Drop Multiplexers (ADMs) allow distant switching nodes to be connected by tributaries to form SONET networks.
- SONET networks generally have the ring topology. The network shown in Fig. 10.8.1 has a physical logical ring topology.
- Each pair of nodes is connected directly by an STS-N tributary. So the three nodes shown are logically configured in a fully connected topology.
- The nodes that do not have direct physical connections can be provided with direct logical connections through the use of tributaries that are added at the source node and dropped at the destination node.



(G-811) **Fig. 10.8.1 : SONET ring topology**

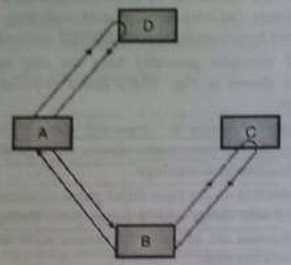
- The approach adding and dropping tributaries allows the flexibility of having arbitrary logical topologies with arbitrary link transmission rates. The configuration can also be done using software control.
- To provide a fault recovery system SONET networks use two paths between any two nodes in the ring as shown in Fig. 10.8.2.
- Fig. 10.8.2 shows a two-fiber ring in which data is copied in both fibers, one travelling clockwise and the other anti-clockwise.



(G-812) **Fig. 10.8.2 : Dual ring SONET system**

Scanned by CamScanner

- In normal operation one fiber path is operation (Usual/clockwise) and the other path is in the protect mode (anticlockwise) when the fibers between two nodes fail are broken or the nodes the ring wraps around as shown in Fig. 10.8.3 and the traffic continues to flow.



(G-812) **Fig. 10.8.3 : Wrapping of ring when fault occurs**

- SONET ring networks can be used in local metropolitan regional area as shown in Fig. 10.8.4.
- As shown in the Fig. 10.8.4 the data from the user is collected by the access networks such as a telephone office.
- A number of such a telephone offices are connected in a first-tier ring network. A metropolitan area ring operating at higher rate is in turn connected the first tier-ring network formed by the telephone offices.
- The metropolitan area ring in turn is connected to the ring of inter exchange or regional carriers.
- Large users that cannot afford failure are connected to the access node using dual paths. To provide protection against faults, rings are inter connected by using matched inter ring gateways between the interoffice ring and the metro ring and between metro ring and the regional ring.
- The traffic flow between the rings is sent simultaneously along the primary and secondary gateway. Automated protection procedures determine whether the primary or secondary incoming traffic is directed into the ring.

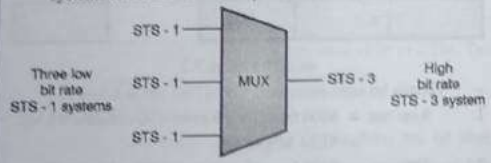
10.9 Applications of SONET :

1. SONET can be used as carrier for ISDN and B.ISDN
2. SONET can be used as carrier for ATM cells.
3. SONET can be used for applications which provide bandwidth on demand
4. SONET can be used for cable TV networks
5. SONET can be used to replace networking protocols such as switched Multimegabit Data Service (SMDS) or Fiber Distributed Data Interface (FDDI).
6. SONET can be used to replace the existing T-1 or T-3 lines.

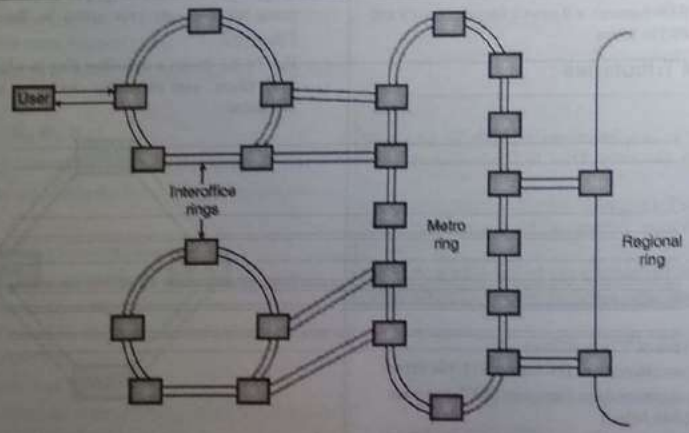
Note : A lot of fiber optic cables have already been laid down all over the world without any common protocol. Most of these cables are not being utilised to their fullest capacity.All these networks can be combined together using SONET protocol.

10.10 High Bit Rate Services (STS Multiplexing) :

- It is possible to multiplex the low rate STSs so as to make them compatible with high rate systems.
- Fig. 10.10.1 shows the STS multiplexing of three STS-1 systems to obtain an STS-3 system.



(G-1324) **Fig. 10.10.1 : STS multiplexing**

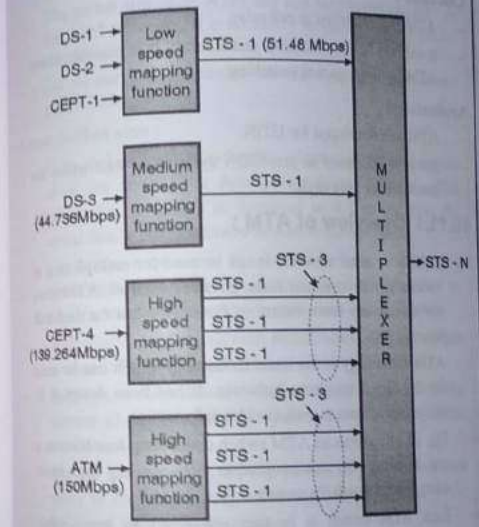


(G-813) **Fig. 10.8.4 : SONET network for local, metropolitan and regional networks**

- Similarly we can multiplex four STS-3 to get one STS-12 or multiplex 12 STS-1 to get an STS-12 etc.

SONET Multiplexing :

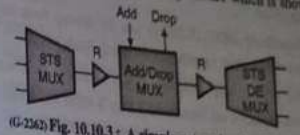
- SONET takes the advantage of the high-speed digital transmission capability of optical fiber. It has a synchronous format that simplifies the handling of lower-level digital signals.
- The SONET standard uses a 51.84 Mbps signal as a building block to extend the digital transmission hierarchy into the gigabit range.
- The Synchronous Transport Signal level-1 (STS-1) is the basic building block of the SONET hierarchy.



(G-1325) **Fig. 10.10.2 : SONET multiplexing**

- A higher level signal in the hierarchy is obtained by interleaving bytes from the lower-level component signals.
- Multiple STS-1 signals can be multiplexed to form the STS-N signal as shown in Fig. 10.10.2.
- As shown in the Fig. 10.10.2 SONET multiplexer can handle a wide range of tributary types (the term tributary means the component streams that are multiplexed together).
- A slow speed mapping function allows DS-1, (Digital Signal - 1 = 1.544 Mbps).
- DS-2 (Digital Signal - 2 = 6.312 Mbps) and CEPT-1 signals (Committee European for Post and Telegraph, 2.048 Mbps) to be combined into an STS-1 signal.
- A DS-3 (44.736 Mbps) signal can be mapped into an STS-1 signal and a CEPT-4 (139.264 Mbps) can be mapped into an STS-3 (155.52 Mbps) signal. An ATM having a data rate of 150 Mbps can also be mapped on to a STS-3 signal.
- The SONET specification defines a hierarchy of standardized digital data rates.

Refer to the simple network using SONET which is shown in Fig. 10.10.3.



(G-2362) **Fig. 10.10.3 : A simple network using SONET**

STS multiplexer/Demultiplexer :

- STS mux and demux are the starting and end points of the SONET respectively.
- They provide an interface between an electrical network and an optical network. For example an STS mux will multiplex signals from various electrical sources and creates the corresponding OC (optical carriers) signal.
- The STS demux demultiplexes an optical OC signal into corresponding electrical signals.

Add/Drop Multiplexer (ADM) :

- Add/drop multiplexer gets its input from a regenerator and feeds its output to a regenerator. Thus the input and output signal of an ADM are optical signals.
- The ADM can add the synchronous transport signals (STSs) coming from various sources into a given path or it can drop (remove) a signal from a path and redirect it without demultiplexing the entire signal. Thus actual multiplexing or demultiplexing does not take place at the ADM.
- The ADM does not rely on the timing and bit positions. Instead it uses the header information such as addresses and pointers to identify the individual streams.
- The differences between ADM and STS multiplexers are summarized in Table 10.10.1.

Table 10.10.1 : Differences between ADM and STS multiplexer

Sr. No.	Parameter	STS multiplexer	Add/Drop multiplexer
1.	Types of I/O signals	Input-electrical output-optical	Input and output both optical.
2.	Action (operation)	Actual multiplexing takes place.	Actual multiplexing/demultiplexing does not take place.

Scanned by CamScanner

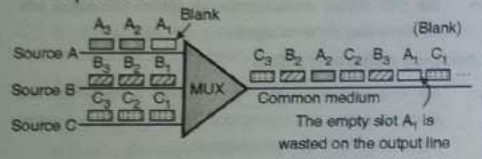
10.11 Asynchronous Transfer Mode (ATM) :

Introduction :

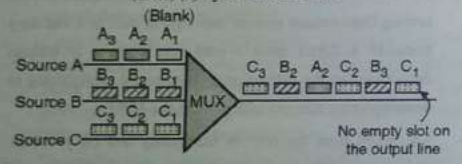
- Broadband ISDN (B-ISDN) was the driving force behind development of Asynchronous Transfer Mode (ATM).
- The speciality of ATM is that it is asynchronous in nature even though it has been derived from B-ISDN which uses the synchronous Time Division Multiplexing (TDM).
- The synchronous TDM did not come out as a very attractive option for data communication. Let us discuss why ?
- Refer Fig. 10.11.1 which shows the difference between the operating principles of synchronous and asynchronous TDM.

Synchronous TDM :

- Fig. 10.11.1(a) illustrates the principle of synchronous TDM. Here the empty slot for source-A has been kept empty in the output slot as well.



(G-408) (a) Synchronous TDM



(G-409) (b) Asynchronous TDM

Fig. 10.11.1

- This happens because the multiplexing takes place strictly on the turn by turn basis. So time slot is allotted to even that source which does not have any data to send.

Asynchronous TDM :

- Now refer Fig. 10.11.1(b) which illustrates the principle of asynchronous TDM. It is important to note that the empty slot A_1 does not appear on the output line of the multiplexer.
- Instead the output line is allotted to the next packet from another source (C_1). Thus asynchronous TDM does not waste any time slots.
- The synchronous TDM can not be used for the broadband ISDN due to its nonflexible nature. So a new technology called ATM was developed.
- ATM is a streamlined packet transfer interface.
- ATM uses packets of fixed size for the communication of data. These packets are called as ATM cells.
- ATM is used for efficient data transfer over high speed data networks.
- ATM provides real time and non real time services.
- The services provided are as follows :
  1. Synchronous TDM streams such as T - 1.
  2. Services using the constant bit rates.
  3. Compressed voice and video.
  4. Traffic which demands a specific quality using the non real time variable bit rate.
  5. IP based services using Available Bit Rate (ABR) and Unspecified Bit Rate (UBR) services.
- The ATM needs an adaption layer for supporting the information transfer protocols that are not based on ATM.

Cell relay :

- ATM is also known as cell relay.
- It exhibits better reliability and fidelity. It is possible to use ATM for faster packet switching.

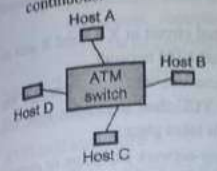
Applications :

- ATM was developed for ISDN.
- But now it is used in non-ISDN systems as well where the data rates are very high.

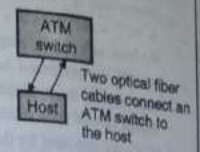
10.11.1 Overview of ATM :

- ATM is a packet network. It can be used for multiplexing of various signals over the same physical channel. ATM does not provide any error control or flow control at the data link layer.
- ATM technology is the latest technology which can be used for the digital telephone networks. It has been designed to deliver voice, data as well as video information.
- Fig. 10.11.2 shows an ATM switch connecting four hosts in a star topology. So communication between any two hosts takes place through the switch.
- Each ATM switch is in turn connected to many other switches and hosts.
- It is possible to add new hosts and switches to an ATM network easily.
- An ATM network is capable of supporting very high data rates (typically upto 155 Mbps).
- The transmission medium used for ATM is optical fibers instead of coaxial cables in order to cope up with high data rates.
- As shown in Fig. 10.11.2, a pair of optical fiber cables is used between a host and a switch. Each cable allows only one way flow of data over it.
- ATM is thus a fully duplex data transmission system.
- Due to the variety of data types (computer data, voice, video) supported, the ATM faces many problems. It has to have a high data rate for voice (neglecting the errors), then it must transmit the computer data accurately (without errors) even if the data rates are slow and it must provide a large bandwidth in order to handle the video signal. Thus ATM has to cater for conflicting requirements.

- In addition it needs to be fast enough for video signal because otherwise the motion pictures may not appear to be continuous.



(G-410) **Fig. 10.11.2 : ATM switch**



(G-411) **Fig. 10.11.3**

10.11.2 Packet Size :

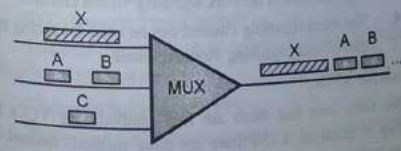
- The packet size of an ATM cell is a very important issue in the ATM networks. It is necessary to ensure that the packet size is optimised.
- Let us see the advantages and disadvantages of different packet sizes.

Large packet size :

- Each packet contains a header which contains information about the source and destination address, CRC etc. This information is known as overhead as it does not have the actual data or information to be sent to the destination.
- The header information is mandatory. If the packet size is small then the header information becomes comparable or atleast a substantial percentage of the total data per packet.
- With smaller packet size, each packet would have to have this overhead. This will be a wastage.
- So the packet size should be large enough. This will make the number of overhead bits per packet, a small portion of the total bits per packet.
- But the problem with the big packets is that they increase delay in communication, which can not be tolerated in the voice and video communication.

Variable length packets :

- The problem associated with big packet size can be eliminated by making the packet length variable.
- In this scheme, smaller packets are used for voice so as to solve the delay problem and larger packets for data.
- This approach has the disadvantages of increased complexity.
- The another disadvantage is that the smaller packets may have to wait for the bigger packets at the multiplexer as shown in Fig. 10.11.4. The small packets A, B and C have to wait till the transmission of the big packet X gets complete.

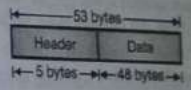


(G-412) **Fig. 10.11.4 : Problem associated with variable length packets**

- This delay faced by the smaller packets would have serious implications on the quality if they contain voice or video information. Hence variable length packet approach has not been adopted.

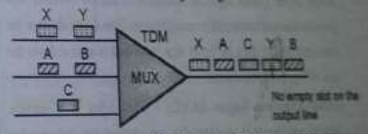
ATM packet :

- Hence the ATM packets are of fixed size but their size has been optimized.
- The ATM packet size has been optimised to ensure the following :
  1. High data rates should be achieved.
  2. Transmission delay should be minimized.
- The ATM has a fixed packet size of 53 octets (bytes). Each packet is called as a **cell**.
- Fig. 10.11.5 shows the structure of an ATM cell. The header is 5 byte long and the remaining 48 bytes are reserved to carry the data.



(G-413) **Fig. 10.11.5 : Structure of an ATM packet**

- In ATM, even if the input is in the form of long packets they are converted in small 53-byte long ATM cells.



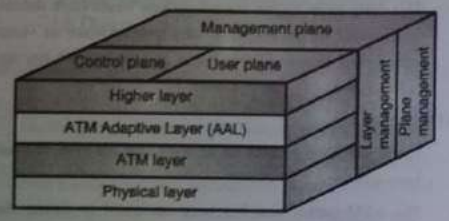
(G-414) **Fig. 10.11.6 : Multiplexing (TDM) of ATM cells**

- This ensures that, large packets do not block or force to wait the smaller packets. These packets are delivered using the principle of time division multiplexing (TDM) as shown in Fig. 10.11.6.
- Fig. 10.11.6 shows that in ATM, since all the packets are of same size, no packet has to wait. This avoids the introduction of delays.

10.12 ATM Protocol Architecture (ATM Reference Model) :

- Fig. 10.12.1 shows the ATM protocol architecture.
- ATM is a streamlined protocol. It has minimal error and flow control capabilities.
- Hence the number of overhead bits required with each cell is reduced which enables ATM to operate at high data rates.
- Also, due to the ATM cells of fixed size, the processing required at each node is simplified. This also supports the use of ATM at high data rates.

Scanned by CamScanner



(G-415) **Fig. 10.12.1 : ATM protocol architecture**

- Fig. 10.12.1 shows the ATM protocol architecture for an interface between user and network.
- The standards issued for ATM by ITU-T are based on this protocol architecture.

Physical layer :

- The physical layer of the protocol involves the specifications of a transmission medium and signal encoding scheme.
- The data rates specified at this layer are between 25.6 Mbps and 622.08 Mbps., but data rates higher and lower than these are possible.

Layers related to ATM functions :

- The two shaded layers in Fig. 10.12.1 correspond to the ATM functions. The two layers are :
  1. ATM layer 2. ATM Adaption Layer (AAL)
- **ATM layer :** This layer is common to all the services that provide the packet transfer capabilities. This layer defines the transmission of data in fixed size cells and it also defines the use of logical connections.
- **ATM Adaption Layer (AAL) :** This layer is a service dependent layer. It is used for supporting the information transfer protocol not based on ATM.
- The AAL maps the higher layer information into the ATM cell and cell is transported over the ATM network.

Various planes in the ATM protocol model :

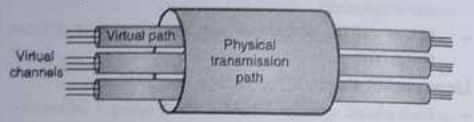
The ATM protocol architecture of Fig. 10.12.1 consists of three separate planes :

1. User plane 2. Control plane 3. Management plane

- **User plane :** It is used for transferring user information alongwith associated controls such as flow control, error control etc.
- **Control plane :** It is supposed to perform the call control and connection control functions.
- **Management plane :** It includes the plane management. The management plane performs management functions related to a system. They include :
  1. Provision of coordination between all planes
  2. Layer management
  3. Management functions relating to resources and parameters residing in its protocol entities.

10.12.1 ATM Logical Connections :

- Logical connections in ATM are called as virtual channel connections or VCCs.
- A VCC is analogous to a virtual circuit in X-25 and it acts as the basic unit of switching in an ATM network.
- A VCC is established between two end users through the network. On the established VCC then a variable rate, full duplex flow of fixed sized cells takes place.
- VCCs are also used for the user-network exchange or control signaling and network-network exchange i.e. network management and routing.
- Refer Fig. 10.12.2. It shows that for an ATM a second sublayer of processing is introduced which deals with the concept of virtual path.



(G-416) **Fig. 10.12.2 : ATM connections**

- **Virtual path connection (VPC) :** It is a bundle of VCCs having the same end points as shown in Fig. 10.12.2. Note that all the ATM cells travelling over all of the VCCs in a single VPC are switched together.
- The virtual path concept is developed specifically for the high speed networking.
- It helps to reduce the control cost by grouping connections which share a common path through the network into a single unit.

10.12.2 Control Signaling :

- In ATM it is necessary to have a mechanism to establish and release of VPCs and VCCs. VPC is virtual path connection and VCC is virtual channel connection.
- In this process, certain information gets exchanged which is called as control signaling.
- The I.150 standard specifies four methods for VCC to provide an establishment and release facility.
- Any one or combination of the following four methods is used in a given network :
  1. Semi permanent VCCs used for user to user exchange.
  2. Meta-signaling channel which is a low data rate channel which can be used for call control.
  3. Use of a user to network signaling virtual channel.
  4. The meta-signaling channel can be used for setting up a user-to-user signaling virtual channel.

Methods for VPCs :

We have seen that there are four methods for VCCs but according to standard. I.150 there are three methods defined for VPCs as follows :

1. To establish a VPC on a semipermanent basis with no control signaling is required.

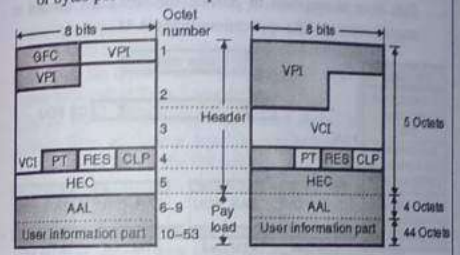
2. The establishment / release of VPC may be customer controlled.
3. On the other hand, the VPC establishment / release may be network controlled. Here the network establishes a VPC for its convenience.

10.12.3 ATM Cells :

The ATM makes use of fixed size cells.

ATM cell structure :

- Fig. 10.12.3 shows the structure of an ATM cell.
- As shown in Fig. 10.12.3 an ATM cell consists of a 5-byte header followed by 48 bytes of information. The total number of bytes per frame is 53 per cell.



(a) User network interface	(b) Network node interface
AAL = ATL adaption layer	PT = Payload Type (2 bits)
CLP = Cell loss priority (1 bit)	RES = Reserved (1 bit)
GFC = Generic flow control	VCI = Virtual channel Identifier
HEC = Header error control	VPI = Virtual path identifier (8 bit for UNI; 12 bit for NNI)

(G-418) **Fig. 10.12.3 : ATM cell structure**

- The total number of such cells transmitted per unit time is dependent on the rate of service.
- These cells are multiplexed at the user-network interface using a label for identification of a cell. This also allows switching through ATM nodes in the network.
- The header is used to identify the payload and to provide the routing information. Fig. 10.12.3 shows that there are two cell header structures one corresponding to the User Network Interface (UNI) and the other is Network Node Interface (NNI).

Functions of header subfields :

Refer Fig. 10.12.3(a) for the subfields of the header. They perform the following functions :

1. **GFC (Generic Flow Control) :**

   This field controls the flow of information from the customer for different types of services.

2. **Virtual Path Identifier (VPI) :**

   This is used for establishing a path for network routing.

3. **Virtual Channel Identifier (VCI) :**

   It is used for establishing a connection through the use of nodal tables.

4. **Payload Type (PT) :**

   This subfield indicates whether the cell is containing user or network information.

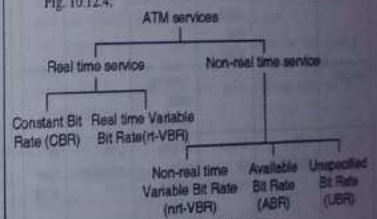
5. **Cell Loss Priority (CLP) :**

   It identifies the cell lower priority which can be discharged depending on the network connections.

6. **Header Error Control (HEC) :**
   - This subfield provides a CRC (Cyclic Redundancy Code) calculation over the header field for error detection and correction.
   - This avoids the incorrect routing of a cell and cell loss due to transmission error.
   - The virtual channels will allow different services at fixed rate as well as at variable bit rate.
   - The Virtual Path (VP) is a group of Virtual Channel (VC) which share the same VPI value.
   - Such virtual channels are transmitted over the same transmission facility and they are switched as a unit.
   - The different Virtual Paths (VPs) which are carried using the same transmission facility are distinguished from each other by their VPI values.

10.12.4 ATM Service Categories :

- The classification of ATM service categories is as given in Fig. 10.12.4.



(G-424) **Fig. 10.12.4 : ATM services**

10.12.5 ATM Adaptation Layer :

- We have already stated that, the use of ATM needs an adaptation layer in order to support the information transfer protocols which are not based on ATM.
- The examples of such protocols are PCM (Pulse Code Modulation) voice and the Internet Protocol (IP).
- In mixed environment, networks based on one type of protocol (say IP) are to be connected to the networks operating on the other type of protocol (say ATM).
- In such environment, such two networks can be integrated by mapping the IP packets into ATM cells.
- In this case one IP packet is segmented into a number of cells on transmission and reassembled the frame from cells on reception because the size of an IP packet is larger than that of an ATM packet.

Scanned by CamScanner

10.12.6 ATM Adaptation Layer (AAL) Services :

- The general examples of services provided by AAL are as follows :
  1. To provide the flow control and timing control.
  2. Handling of transmission errors.
  3. To take care of segmentation and reassembly. With this service larger blocks of data can be carried via the information field of ATM cells.
  4. Handling of lost and misinserted cell conditions.
- In order to meet different types of needs, we need to use different AAL protocols.
- To minimize the number of different AAL protocols, the ITU-T has defined four classes of service to cover a broad range of requirements.
- Table 10.12.1 shows the relation between four AAL protocols to the various service categories defined by the ATM forum.

Table 10.12.1 : AAL protocols and services

Protocol	CBR	rt-VBR	nrt-VBR	ABR	UBR
AAL – 1	Circuit emulation, ISDN, voice over ATM				
AAL 2		VBR voice and video			
AAL3/4			General data services		
AAL 5	LAN emulation	Voice on demand	Frame relay ATM, LAN emulation	LAN emulation	IP over ATM

Circuit emulation :

The circuit emulation corresponds to the synchronous TDM transmission systems such as T-1 over the ATM network.

VBR voice and video :

- These are the real time applications in which the transmitted data is in the compressed form.
- Due to compression, it is possible to support the variable bit rate.

General data services :

These are non real time services that include messaging and transaction services.

IP over ATM :

Here transmission of IP packets takes place using ATM cells.

LAN emulation :

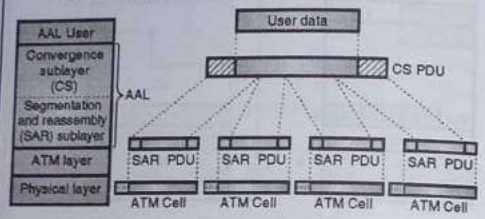
- Support of LAN-to-LAN traffic across ATM networks with emulation of LAN broadcast capability (a transmission from one station reaches many other stations).
- LANE is designed to allow an easy transmission from a LAN environment to an ATM environment.

10.13 AAL Protocols :

- The ATM adaptation layer (AAL) protocols are related to the adaptation layer.
- The AAL layer is divided into two sublayers as shown in Fig. 10.13.1. They are :
  1. Convergence Sublayer (CS)
  2. Segmentation and Reassembly (SAR) sublayer.

10.13.1 Conversion Sublayer (CS) :

- This layer is supposed to provide the functions needed to support some specific applications using AAL.

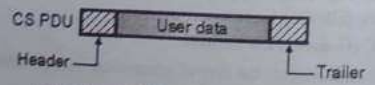


(G-426) **Fig. 10.13.1(a) : AAL protocol and PDUs**

- Each AAL user gets connected to AAL at a Service Access Point (SAP). SAP is nothing but the address of the application.

10.13.2 Segmentation and Reassembly (SAR) Sublayer :

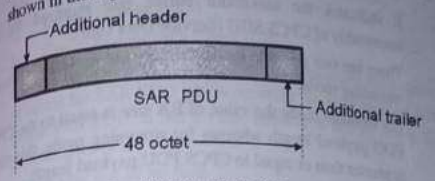
- The SAR does the job of packaging the information received from CS into cells for transmission at the sending end and unpackaging the information at the receiving end.
- We have seen that at the ATM layer, each cell consists of a 5 byte (or octet) header and a 48 octet information field.
- Hence SAR has to pack any SAR headers and trailers and the CS information into 48 octet blocks.
- Fig. 10.13.1(a) shows the general protocol architecture for AAL.
- It shows that the data block from the higher layer is encapsulated in a single Protocol Data Unit (PDU) that consists of a header and trailer as shown in the Fig. 10.13.1(b).



(G-427) **Fig. 10.13.1(b) : CS PDU redrawn**

- The header and trailer contain the protocol information at the CS level.
- This CS PDU is then passed to the SAR sublayer and segmented into a number of blocks as shown in Fig. 10.13.1(a).

- Each of such blocks is encapsulated in a single 48 byte SAR PDU which may include an additional header and trailer as shown in the Fig. 10.13.2.

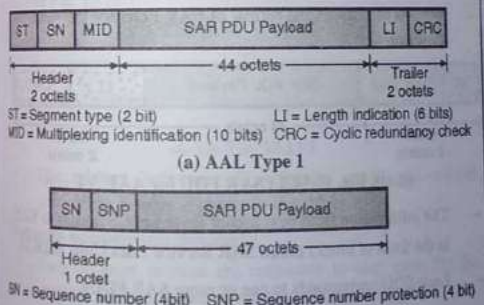


(G-428) **Fig. 10.13.2 : SAR PDU redrawn**

- Finally each SAR PDU forms the pay load of a single ATM cell, is shown in Fig. 10.13.1(a).
- The ITU-T defined four AAL protocol types namely Type 1 through Type 4. Each protocol type consists of two protocols, one for CS sublayer and the other for SAR sublayer.
- Later on the types 3 and 4 were merged into a type 3/4 and a new type called Type 5 was defined.
- In all the AAL protocols mentioned above, the data block taken from the higher layer is encapsulated into a Protocol Data Unit (PDU) at the CS sublayer.
- Hence this sublayer is called as Common Part Convergence Sublayer (CPCS).
- The CPCS PDU is then passed to the SAR sublayer where it is divided into the SAR PDUs and finally into ATM cells.
- Each 48-octet SAR-PDU fits into a single ATM cell.

In short for different types of AAL protocols, the CPCS-PDU is common but the formats of SAR-PDU are different.

Fig. 10.3.3 shows the formats of Protocol Data Units (PDUs) at the SAR level. The format for type 2 is not yet defined hence it has not been shown in Fig. 10.13.3.



(G-430) **Fig. 10.13.3 : SAR PDUs for different types of AAL protocols**

10.14 AAL Type 1 :

- The AAL type 1 protocol is designed to deal with a Constant Bit Rate (CBR) source.
- So the SAR protocol has only two operations to perform. First is to pack the bits into cells for the purpose of transmission and then to unpack them at the receiving end.
- The SAR PDU format for AAL Type 1 is shown in Fig. 10.13.3(a). Each block has a header which is one octet (1 byte) long.
- The header is split into two four bit fields called SN (Sequence Number) and SNP (Sequence Number Protection).
- SN is used so that the errored PDU can be tracked. This field consists of a Convergence Sublayer Indication (CSI) bit and 3-bit Sequence Count (SC).

Sequence Number Protection (SNP) :

- The Sequence Number Protection (SNP) field is an error code for error detection and correction on the sequence number field.
- It consists of a 3 bit Cyclic Redundancy Check (CRC) and a parity bit.
- The parity bit is adjusted in such a way that the parity of 8 bit SAR header is even.
- CS PDU has not been defined for Type 1 AAL.
- The CS sublayer for Type 1 has a limited role to play. It does only clocking and synchronization. So separate CS header is not required.

AAL Type 2 :

- The remaining protocol types (2, 3/4 and 5) are designed to deal with Variable Bit Rate (VBR) information.
- The Type 2 AAL is expected to be used for the analog applications such as audio and video. Such applications require timing information but they can operate on the variable bit rate.

AAL Type 3/4 :

- The services provided by AAL Type 3/4 can be characterized as follows :

1. **Connectionless or connection oriented :**
   - The service provided by AAL type 3/4 can be connectionless or connection oriented.
   - For the connectionless service, each block of data is presented to the SAR layer i.e. to the SAR service data unit.
   - For connection oriented service we can define multiple SAR logic connections over a single ATM connection.
2. **Message mode or streaming mode :**
   - The AAL 3/4 service can be of two types namely : message mode or streaming mode type.
   - In the message mode service, the data is transferred in the form of frames.
   - Hence we can use any OSI related protocol. LAPD or frame relay can be suitable for this mode.
   - The streaming mode service is used for the transfer of low speed continuous data with low delay requirements.

Scanned by CamScanner

- The data is presented to AAL in fixed size blocks which can be very small (of the order of 1 octet or byte). One block is transferred per cell.
- The type 3/4 AAL provides its data transfer service by accepting blocks of data from the next higher layer and then transmitting it to the correct destination (AAL user).

The sequence of operation in AAL 3/4 :

1. A block of data from a higher layer such as a PDU is transformed into CPCS PDU as discussed earlier.
2. Pass CPCS PDU to SAR sublayer.
3. The CPCS PDU is broken up into 44 - octet payload blocks at the SAR sublayer. These are SAR PDUs.
4. Each 48-octet SAR PDU fits into a single ATM cell.

The CPCS PDU :

The CPCS PDU is shown in Fig. 10.14.1. The header of CPCS PDU consists of three fields namely CPI, Btag and BA size.

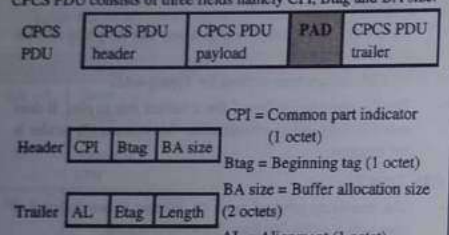


Fig. 10.14.1 : AAL type 3/4

Header fields :

The three fields of the CPCS PDU header have the following functions to perform.

Common Part Indicator (CPI) :

- This field is 1 octet (8 bit) long.
- It is supposed to indicate the interpretation of the remaining fields in the CPCS PDU header.
- Current however only one interpretation has been defined as follows.
- The CPI value of 0 indicates that the BA size field defines the buffer allocation requirement in octets and the length field defines the length of CPCS PDU payload in octets.

Beginning Tag (B Tag) :

- This field is 1 octet long.
- It is actually a number associated with a particular CPCS PDU.
- The same number appears in the B tag field in the header and E tag field in the trailer.
- This value is changed by the user for each successive CPCS PDU. This enables the receiver to associate correctly the header and trailer of each CPCS PDU.

Buffer Allocation Size (BA Size) :

- This field is 2 octet long.
- It indicates the maximum buffer size required for the reassembly of CPCS SDU (Service Data Unit).
- There are two possible modes namely the message mode and streaming mode.
- For message mode the value of BA size is equal to the CPCS PDU payload length whereas for streaming mode, this value is greater than or equal to CPCS PDU payload length.

Pad :

As shown in Fig. 10.14.1, the payload from the next higher layer is padded out so that the trailer always begins on a 32-bit boundary.

CPCS PDU Trailer :

The CPCS PDU trailer contains three fields as shown in Fig. 10.14.1 :

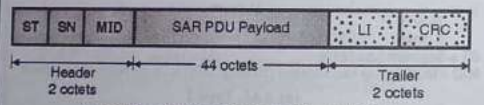
1. Alignment (AL) 2. End tag (E tag) 3. Length

- **Alignment (AL) :** This is a 1 octet field. It is only a filler octet which is used to make the length of CPCS PDU equal to 32 bits.
- **Eng tag :** This field also is 1 octet long. It is used with the B tag field in the header.
- **Length :** This is a 2 octet long field. It indicates the length of the CPCS PDU payload field.

The conclusion of the discussion is that the CPCS layer alerts the receiver that a block of data is coming in segments and a buffer space should be allocated for its reassembly.

10.14.1 Format of SAR PDU :

- Fig. 10.14.2 shows the format of SAR PDU for the AAL 3/4 protocol.



(G-432) **Fig. 10.14.2 : SAR PDU for AAL 3/4**

- The information from next higher layer i.e. CS comes to SAR in the form of blocks called SAR Service Data Units (SDUs).
- Each SDU corresponds to one or more SAR PDUs.
- Each SAR PDU is transmitted in a single ATM cell.

SAR PDU Header :

The SAR PDU header consists of the following fields as shown in Fig. 10.14.2 :

1. Segment Type (ST)
2. Sequence Number (SN)
3. Multiplexing Identification (MID)

- The Multiplexing Identification (MID) is a 10 bit field.
- It acts as a unique identifier that is associated with the set of SAR PDUs which carry a single SAR SDU.

SAR PDU Trailer :

- The SAR PDU trailer consists of the following fields :
  1. Length Indicator (LI)
  2. Cyclic Redundancy Check (CRC)
- **Length Indicator (LI) :** It is used for indicating the number of octets for SAR SDU which occupies the segmentation unit of the SAR PDU. It has a value between 4 and 44 octets, in the multiples of 4.
- **CRC :** This is a 10 bit field.

10.14.2 Features of AAL 3/4 :

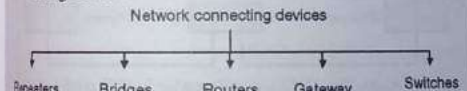
- It can multiplex various data streams on the same virtual ATM connection.
- Each logical connection between AAL user is assigned a unique MID value.

10.14.3 AAL Type 5 :

- This is the latest version of AAL protocols.
- The purpose of introducing this protocol is to provide a streamlined transport facility for the higher layer protocols which are connection - oriented.
- The advantages of AAL type 5 are as follows :
  1. Reduces protocol processing overheads.
  2. Reduces the transmission overheads.
  3. It has adaptability to the existing transport protocols.

10.15 Network Connecting Devices :

- Different types of network connecting devices are as shown in Fig. 10.15.1.

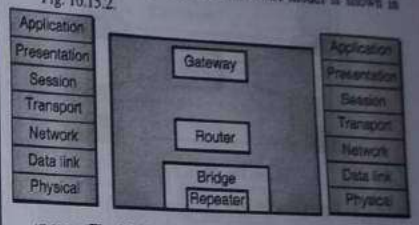


(G-348) **Fig. 10.15.1**

- The relation between OSI reference model and various connecting devices is shown in Fig. 10.15.2.

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. 10.15.2.



(G-906(a)) **Fig. 10.15.2 : Connecting devices and OSI model**

Categories of connecting devices :

Fig. 10.15.2 shows the relationship between the connecting devices and various layers of the internet model.

Table 10.15.1 : 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.

10.16 Hubs :

MU : May 15, Dec. 15, Dec. 16

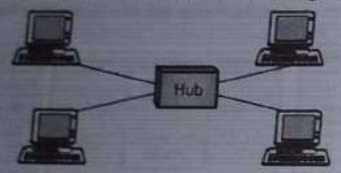
University Questions

Q. 1 Write short notes on : Hubs, switches and bridges. **(May 15, 5 Marks)**

Q. 2 Explain the following with example. Hubs. **(Dec. 15, Dec. 16, 2 Marks)**

Scanned by CamScanner

- 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. 10.16.1.
- There are three main types of hubs :
  1. Passive hubs 2. Active hubs 3. Intelligent hubs



(G-350) **Fig. 10.16.1 : Hub**

10.16.1 Passive Hubs :

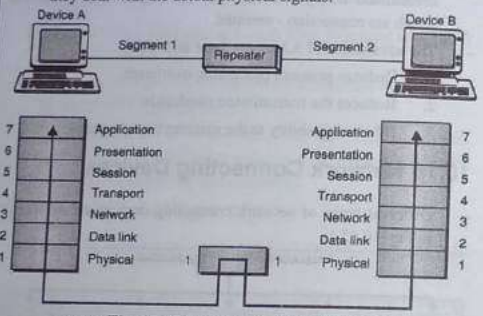
- A passive hub simply combines the signals of a network segments. There is no signal processing or regeneration. It merely acts as a connector.
- A passive hub reduces the cabling distance by half because it does not boost the signals and in fact absorbs some of the signal.
- With a passive hub, each 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.

0.17 Repeaters : MU : Dec. 15, Dec. 16

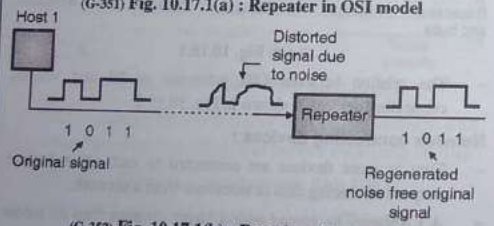
University Questions

Q.1 Explain the following with example : Repeater. **(Dec. 15, Dec. 16, 2 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. 10.17.1(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. 10.17.1(a) and (b).
- A repeater does not connect two LANs. It connects only two devices connected in the same LAN.
- 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. 10.17.1(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-351) **Fig. 10.17.1(a) : Repeater in OSI model**



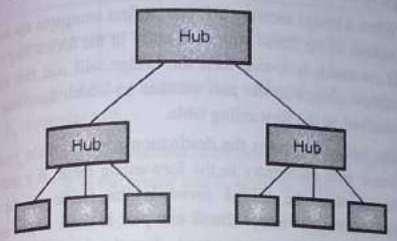
(G-352) **Fig. 10.17.1(b) : Function of a repeater**

10.17.1 Active Hubs :

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

10.17.2 Intelligent Hubs :

- In addition to signal regeneration, intelligent hubs perform some other intelligent functions such as network management and intelligent path selection.
- A switching hub chooses only the port of the device where the signal needs to go, rather than sending the signal along all paths.
- Hubs can also be used to create multiple levels of hierarchy as shown in Fig. 10.17.2.



(I-446) **Fig. 10.17.2 : Hubs to create multiple levels of hierarchy**

10.18 Bridges : MU : May 15, Dec. 15, May 16, Dec. 16

University Questions

Q.1 Write short notes on : Hubs, Switches and Bridges **(May 15, 5 Marks)**

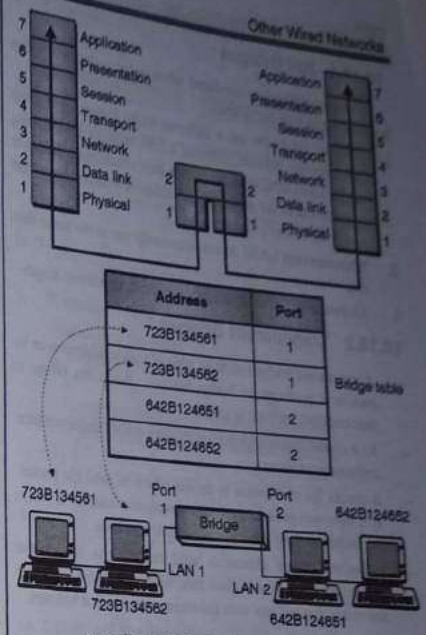
Q.2 Explain the following with example : Bridges **(Dec. 15, Dec. 16, 2 Marks)**

Q.3 Write short note on : Bridges, Router, Switches. **(May 16, 5 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.



(G-354) **Fig. 10.18.1 : Bridge and bridge table**

- In order to achieve this a bridge has a table relating the addresses and ports as shown in Fig. 10.18.1.
- 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. 10.18.1 a two port bridge is shown but in reality a bridge has more than two ports.
- It is important to note that the bridges do not change the physical address contained in the frame.

Types of bridges :

- The bridges are of two types :
  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.

Scanned by CamScanner

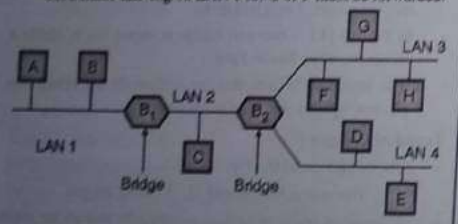
10.18.1 802 Bridges :

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.

10.18.2 Transparent Bridges :

- 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. 10.18.2. As shown in the Fig. 10.18.2 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. 10.18.2 : 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 10.18.1.

Table 10.18.1 : Format of a forwarding table

MAC address	Port

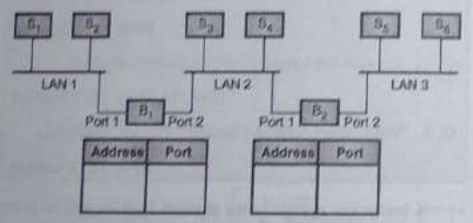
- Note that in practice there are a few thousand entries in a forwarding table.
- Let us see how to fill up these forwarding tables. It is filled up by a process called as "bridge learning".
- The basic bridge learning process is as follows :

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.

Example on bridge learning :

Consider the network shown in Fig. 10.18.3(a). Assume that forwarding tables of both the bridges are initially empty.



(L-449) **Fig. 10.18.3(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. 10.18.3(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. 10.18.3(b).

B_1

Address	Port
S_2	1
S_1	1

B_2

Address	Port

Fig. 10.18.3(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. 10.18.3(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. 10.18.3(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	1
S_1	1
S_5	2
S_4	2

$S_2 \rightarrow S_1$

$S_5 \rightarrow S_4$

B_2

Address	Port
S_5	2
S_4	1

$S_5 \rightarrow S_4$

Fig. 10.18.3(c) : Forwarding tables after $S_5 \rightarrow S_4$

   - The table entries for the remaining transmissions are given in Figs. 10.18.3(d) and (e).

3. **S_3 transmits to S_6 :**

B_1

Address	Port
S_2	1
S_1	1
S_5	2
S_4	2
S_3	2

$S_2 \rightarrow S_1$

$S_5 \rightarrow S_4$

$S_3 \rightarrow S_5$

B_2

Address	Port
S_5	2
S_4	1
S_3	2

$S_5 \rightarrow S_4$

$S_3 \rightarrow S_5$

Fig. 10.18.3(d) : Tables after $S_3 \rightarrow S_6$

4. **S_1 transmits to S_2 :**
   No change in the tables.
5. **S_6 transmits to S_3 :**

B_1

Address	Port
S_2	1
S_1	1
S_5	2
S_4	2
S_3	2

$S_2 \rightarrow S_1$

$S_5 \rightarrow S_4$

$S_3 \rightarrow S_5$

B_2

Address	Port
S_5	2
S_4	1
S_3	2
S_6	2

$S_5 \rightarrow S_4$

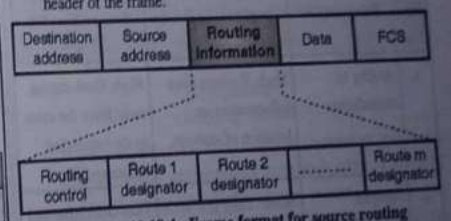
$S_3 \rightarrow S_5$

$S_6 \rightarrow S_3$

Fig. 10.18.3(e) : Table after $S_6 \rightarrow S_3$

10.18.3 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.



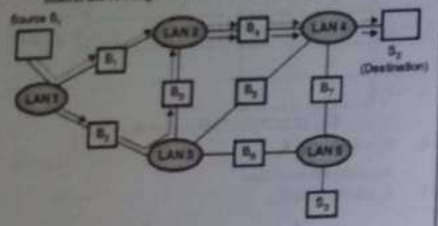
(L-454) **Fig. 10.18.4 : Frame format for source routing**

- The frame format for source routing is shown in Fig. 10.18.4.
- Note that the routing information field is inserted only if the two communicating stations are on different LANs.
- Fig. 10.18.5 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 $\rightarrow B_1 \rightarrow$ LAN 2 $\rightarrow B_4 \rightarrow$ LAN 4.
- Many more routes are available for the same source destination pair.

Scanned by CamScanner

- 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. 10.18.5 : LANs interconnected with source routing bridges**

How to discover a route ?

To discover a route the basic idea is as follows :

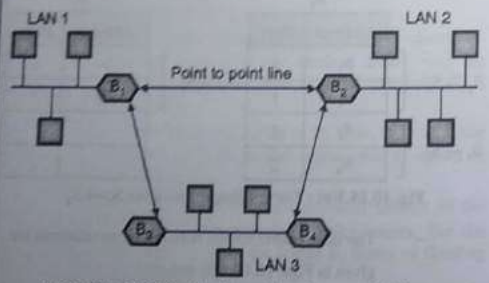
1. The station who wants to discover a route first broadcasts a special frame called single route broadcast frame.
2. This frame will visit every LAN exactly once and eventually reaches the destination.
3. Then the destination station responds with another special frame called the all routes special 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.

10.18.4 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.	Station responsibilities	None. They just send the frames and let the bridges do the work.	They determine and maintain addresses.
3.	Bridge 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.

10.18.5 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. 10.18.6.
- 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. 10.18.6 : Configuration of remote bridges**

10.19 Routers :

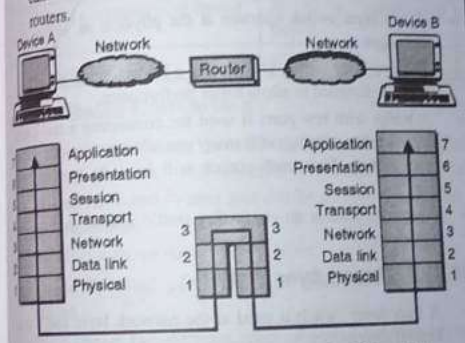
MU : Dec. 15, May 16, Dec. 16

University Questions

Q. 1 Explain the following with example : Router **(Dec. 15, Dec. 16, 2 Marks)**

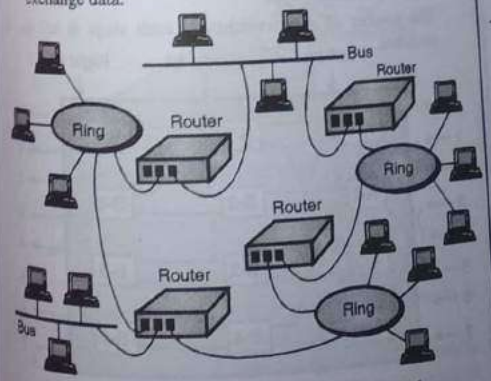
Q. 2 Write short note on : Bridges, Router, Switches. **(May 16, 5 Marks)**

- Routers are devices that connect two or more networks as shown in Figs. 10.19.1(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. 10.19.1(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. 10.19.1 (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. 10.19.1(b) : Routers in an internet**

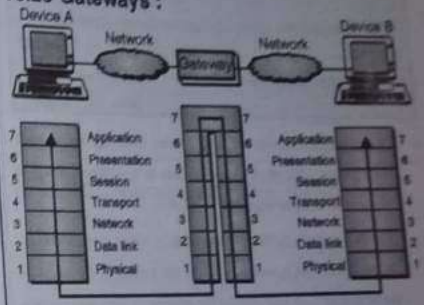
- Data is grouped into packets, or blocks of data. Each packet has a physical device address as well as logical network address.
- The network address allows routers to calculate the optimal path to a workstation or computer.
- Route discovery is the process of finding the possible routes through the 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.

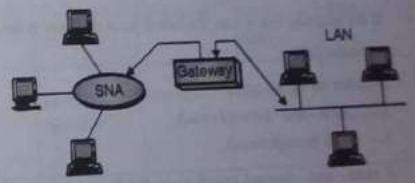
Note :

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

10.20 Gateways :



(a) **A gateway in the OSI model**



(b) **A gateway**

(G-366) **Fig. 10.20.1**

- 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. 10.20.1(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.

Scanned by CamScanner

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.

10.21 Switches :

MU - May 15, Dec. 15, May 16, Dec. 16

University Questions

Q. 1 Write short notes on : Hubs, Switches and Bridges **(May 15, 5 Marks)**

Q. 2 Explain the following with example : Switches **(Dec. 15, Dec. 16, 2 Marks)**

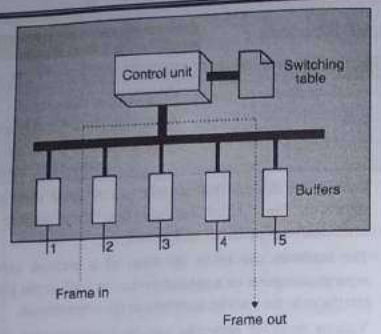
Q. 3 Write short note on : Bridges, Router, Switches. **(May 16, 5 Marks)**

- 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. 10.21.1. As shown in the Fig. 10.21.1 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. 10.21.1 : Switch**

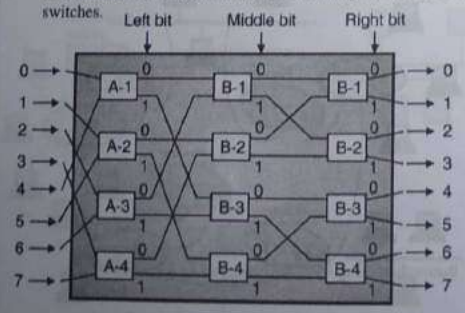
Note : Routing switches use the network layer destination address to find the output link to which the packet should be forwarded.

10.21.1 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.

10.21.2 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. 10.21.2.
- 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. 10.21.2 : 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 = $\log_2(n) = \log_2 8 = 3$.

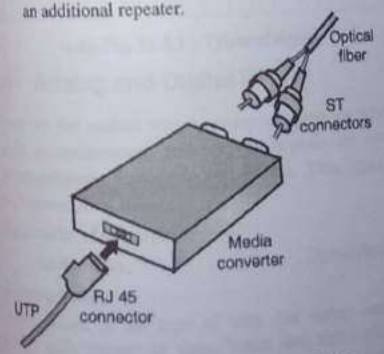
10.21.3 Comparison of Hub and Switch :

Sr. No.	Hub	Switch
1.	It is a broadcast device.	It is a point to point device.
2.	It operates at physical layer.	It operates at datalink layer.
3.	It is not an intelligent device.	It is an intelligent device.
4.	It simply broadcasts the incoming packet.	It uses switching table to find the correct destination.
5.	It can not 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.

10.21.4 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. 10.21.4 shows the media converter.
- Various functions performed by a media converter are as follows :

1. Connect two different types of wiring systems without an additional repeater.



(G-369) **Fig. 10.21.3 : Media converter**

2. Connect two 10 Base T or 100 Base TX networks in different buildings using fiber-optic cable.
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.

10.21.5 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.

10.21.6 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

Scanned by CamScanner

Review Questions

Q. 1 What is SONET ?

Q. 2 Explain SONET frame.

Q. 3 Write a short note on : SONET network.

Q. 4 What are the applications of SONET ?

Q. 5 Explain different types of overheads in SONET.

Q. 6 Explain the frame, bit and byte transmission in SONET.

Q. 7 Write a note on SONET layers.

Q. 8 Explain the function of repeaters. Is it as amplifier ?

Q. 9 Compare repeater and hub.

Q. 10 Write a note on : Bridges.

Q. 11 What is the use of bridge table ?

Q. 12 With the help of suitable explanatory diagram, explain the routers and gateways.

Q. 13 Explain different types of switches.

Q. 14 Compare switches and hub.

Q. 15 What is backbone network ? What are its types ?

Q. 16 What is ATM ? Where is it required ?

Q. 17 With the help of block diagram explain the ATM protocol architecture.

Q. 18 Write a note on : overview of ATM.

Q. 19 Explain the packet size of ATM.

Q. 20 With the help of illustrative diagrams explain the structure of ATM cells.

Q. 21 Write a note on : Transmission of ATM cells.

Q. 22 What are the ATM service categories ?

Q. 23 Explain the real time services.

Q. 24 State the typical examples of non-real time variable bit rate services.

Q. 25 Write a note on : AAL

Q. 26 State and explain the services provided by the AAL layer.

Q. 27 Write a note on AAL protocols.

Q. 28 Explain clearly the AAL protocol AAL-Type 1.

Q. 29 Explain the causes of congestion and principle of congestion control.

Q. 30 What is QoS in ATM ?

Q. 31 Explain switching in ATM.

Q. 32 State various types of ATM switches and explain their operation.

❑❑❑

CHAPTER 11

Module VI

Data and Signal

Syllabus :
Analog and digital, Transmission impairment, Data rate limits, Performance.

11.1 Analog and Digital Signals :

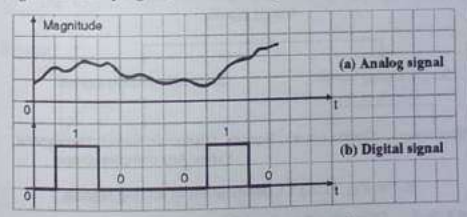
- Signals can be of two types :
  1. Analog signals. 2. Digital signals.

1. Analog signal :

It is the signal in which the signal magnitude varies in a smooth fashion without any break with respect to time, as shown in Fig. 11.1.1(a).

2. Digital signal :

It is the signal in which the signal magnitudes has a constant level for some period of time, then it changes suddenly to another constant level as shown in Fig. 11.1.1(b). The examples of digital signal are binary signal, hexadecimal signal etc.



(L-24) **Fig. 11.1.1 : Types of signals**

11.1.1 Analog and Digital Data :

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

1. Analog data :

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

2. Digital data :

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

11.1.2 Sources of Digital Signal :

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

11.1.3 Advantages of Digital Signals :

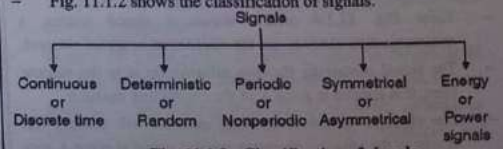
1. Digital signals can be processed and transmitted more efficiently and reliably than analog signals.
2. It is possible to store the digital data.
3. Play back or further processing of the digital data is possible.
4. The effect of "noise" (unwanted voltage fluctuations) is less. So digital data does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

11.1.4 Comparison of Digital and Analog Signals :

Sr. No.	Parameter	Analog signals	Digital signals
1.	Number of values	Infinite	Finite (2, 8, 16 etc.)
2.	Nature	Continuous	Discrete
3.	Sources	Signal generators, transducers etc.	Computers, A to D converters
4.	Examples	Sinewave, triangular wave	Binary signal

11.1.5 Classification of Signals :

- Fig. 11.1.2 shows the classification of signals.



(G-1250) **Fig. 11.1.2 : Classification of signals**

- Out of these we will concentrate only on periodic or non periodic signals.

Scanned by CamScanner

11.1.6 Periodic and Non-periodic Signals :

Periodic signal :

- A signal which repeats itself after a fixed time period is called as a periodic signal. The periodicity of a signal can be defined mathematically as follows :

  $x(t) = x(t + T_o)$: Condition of periodicity ...(11.1.1)

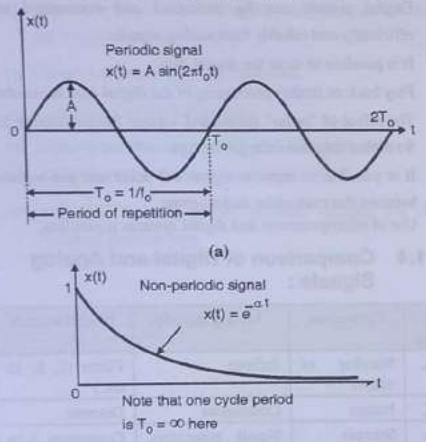
- Where T_o is called as the period of signal x (t), in other words, signal x (t) repeats itself after a period of T_o sec.
- Examples of periodic signals are sine wave, cosine wave, square wave etc. Fig. 11.1.3(a) shows a sine wave which is periodic because it repeats itself after a period T_o.

Non-periodic signal :

- A signal which does not repeat itself after a fixed time period or does not repeat at all is called as a non-periodic or aperiodic signal.
- The non-periodic signals do not satisfy the condition of periodicity stated in Equation (11.1.1).

∴ For a non-periodic signal $x(t) \neq x(t + T_o)$ ...(11.1.2)

- Sometimes it is said that an aperiodic signal has a period $T_o = \infty$. Fig. 11.1.3(b) shows a decaying exponential signal.

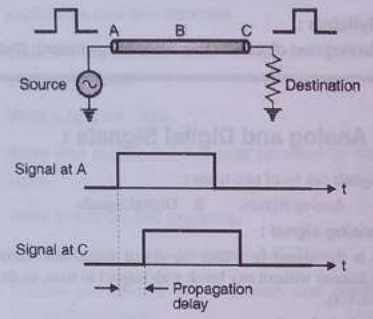


(G-1251) **Fig. 11.1.3 : Periodic and non-periodic signals**

- This exponential signal is non-periodic but it is deterministic because we can mathematically express it as $x(t) = e^{-\alpha t}$.

11.1.7 Signal Propagation :

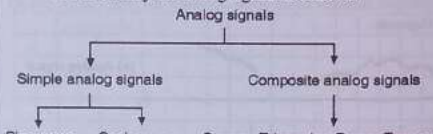
- Refer Fig. 11.1.4 which shows a signal source, a communication channel and the destination or signal receiver.
- The signal containing the data information is in the electric form. It is applied at point A of the conducting medium.
- The electrons in the conducting medium will transfer the charge to the adjacent electrons and the signal at point A gets transferred to B and then to C which is the receiving point.
- The shape of the signal at the receiver (point C) is almost same as that at the source (point A), but the signal reaches point C after a finite delay called **propagation delay.**
- The signal producing source in Fig. 11.1.4 can be a person talking on the phone or a computer producing a data signal or a video camera producing a video signal etc.
- Thus if we apply a signal at one end of the conducting medium then eventually this signal gets propagated to the other end of the medium with some time delay.



(G-1252) **Fig. 11.1.4 : Signal propagation**

11.2 Analog Signals :

We can classify the analog signals as follows :



(L-770) **Fig. 11.2.1 : Classification of analog signals**

11.2.1 Simple Analog Signal :

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

11.2.2 Composite Analog Signal :

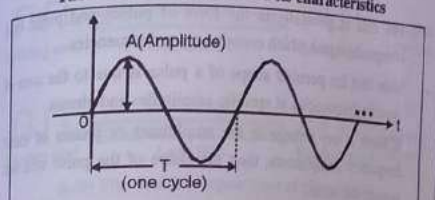
- A composed analog signal is made of multiple sine or cosine waves of different amplitudes added to / subtracted from each other.
- Examples of composite analog signals are square wave, triangular wave, ramp, trapezoidal signal, pulse etc.

11.2.3 Sinewaves :

- It is the most basic type of periodic analog signal. That means it is the simple analog signal.

- Table 11.2.1 shows the graphical representation along with some of its characteristics.

Table 11.2.1 : Sinewave and its characteristics



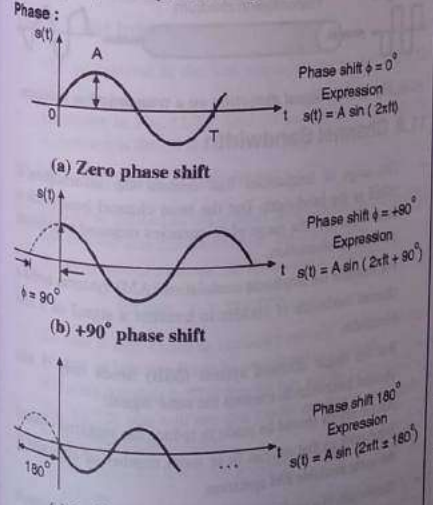
(L-771)

Mathematical expression	:	$s(t) = A \sin(2\pi ft + \phi)$
Peak amplitude	:	A
Frequency	:	f Hz = 1 / T
Period	:	T = (1/f) sec.
Phase	:	ϕ radians

Important points about frequency and time period :

1. Frequency and time period (T) are reciprocals of each other.
2. Frequency can be defined as rate of change of magnitude with respect to time. Change of signal magnitude in a shorter time span corresponds to high frequency.
3. Change of signal magnitude over a long time span corresponds to low frequency.
4. The signal which does not change at all has zero frequency. Example of such a signal is dc signal.
5. The signal that changes instantaneously has an infinite frequency. Example is delta signal or an impulse.

Phase :



(L-772) **Fig. 11.2.2 : Concept of phase shift**

- The letter ϕ in the mathematical expression for a sinewave denotes phase of the sinewave.
- It describes the position of the waveform with respect to time zero (i.e. t = 0). This is explained in Fig. 11.2.2.

Wavelength :

- Wavelength is another important characteristics of a signal travelling through a transmission medium.
- Wavelength relates the frequency of a sinewave with the speed of propagation as follows :

$$\text{Wavelength } \lambda = \frac{\text{Propagation speed}}{\text{Frequency}}$$

$$= \text{Propagation speed} \times \text{period}$$

$$\therefore \lambda = \frac{C}{f} = C \times T \quad \text{...(11.2.1)}$$

- Wavelength of a signal is dependent on the medium. In data communication the wavelength is used to describe the transmission of light in an optical fiber.
- Wavelength is the distance travelled by a signal or an electromagnetic wave during the time period of one cycle of the signal.
- In vaccum the speed of light (c) is 3×10^8 m/s but it does not remain same in a cable. Hence the wavelength of the same signal will be different in air and on a cable.

11.3 Time and Frequency Domain :

It is possible to display a signal in either time domain or in frequency domain.

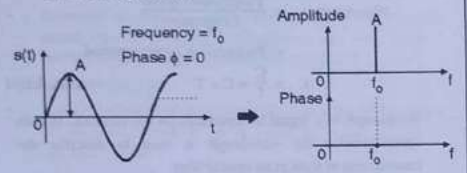
11.3.1 Time Domain Display of Analog Signals :

- It is the graph of signal magnitude with respect to time. That means on the x-axis we plot the time t and on the y-axis the magnitude is plotted. (Refer Fig. 11.3.1(a)).
- A time domain display tell us about the following :
  1. Shape of the signal.
  2. Its frequency.
  3. Type of the signal (periodic or nonperiodic).
  4. One cycle period.
- But we cannot know anything about what frequency components are present and in what proportion they have been mixed in order to obtain the particular shape of the signal.
- All this information can be obtained from the line spectrum of a signal.
- The phase and frequency cannot be explicitly measured from the time domain plot.
- In case of a composite waveform, which is composed of multiple sinewaves of different amplitudes, frequencies and phases, the time domain plot does not reveal any information about the relationship between amplitude, frequencies and phases of the various sinewaves.

Scanned by CamScanner

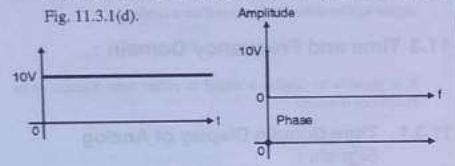
11.3.2 Frequency Domain Display of a Signal :

- It is the graph of signal amplitude (peak or sometimes rms), plotted on Y-axis with respect to frequency plotted on the x-axis.
- It is also possible to plot phase ϕ with respect to frequency as shown in Fig. 11.3.1.



(a) Time domain display (b) Frequency domain display
(L-773) **Fig. 11.3.1**

- Now refer Fig. 11.3.1(c) which shows a dc signal with amplitude 10 V. The frequency and phase both will be zero. The frequency domain display of this signal is shown in Fig. 11.3.1(d).



(c) Time domain display (d) Frequency domain display
(L-774) **Fig. 11.3.1 : DC signal**

Conclusions :

1. In the frequency domain we can show two characteristics of the signal using one vertical line. First is the amplitude and second is the frequency of the signal.
2. We can also show the phase angle.
3. The analog signal is best represented in the frequency domain.

11.4 Composite Signals :

- Sine and cosine waves are the basic and purest signals but they are not useful in data communication.
- To use the sinewave for data communication, we have to change one or more of its characteristics, such as amplitude in accordance with the data to be transmitted.
- But then the sinewave does not remain the simple sinewave, instead it becomes a **composite signal** which is made up of many simple sinewaves.

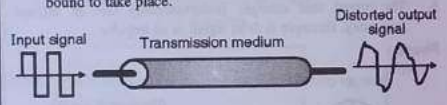
Thus when we change amplitude, frequency or phase of a single frequency signal, it gets transformed into a **composite signal** made of many frequencies.

11.5 Composite Signal and Transmission Medium :

- The data is generally in the form of pulses and pulse is a composite signal which contains many frequencies.
- Note that the peculiar shape of a pulse is due to the sum of specific frequencies at specific amplitudes and phases.
- If there is any change in the amplitudes or phases of these frequency components, then the shape of the pulse will not remain the same.

11.5.1 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. 11.5.1.
- 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.

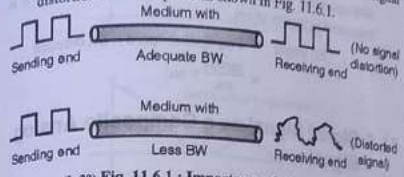


(G-82) **Fig. 11.5.1 : Signal distortion on a transmission medium**

11.6 Channel Bandwidth :

- The range of frequencies that contain the information is called as the bandwidth. But the term channel bandwidth is used to describe the range of frequencies required to transmit the desired information.
- For example the amplitude modulation (AM) systems needs a channel bandwidth of 10 kHz to transmit a signal of 5 kHz bandwidth.
- But the single sideband system (SSB) needs only 5 kHz channel bandwidth to transmit the same signal.
- All the efforts should be made to reduce the required channel bandwidth so that we can fit in more number of channels in the same available EM spectrum.
- Bandwidth of a medium (also called as channel bandwidth) is defined as the maximum frequency it can allow to pass through it without attenuating it and without distorting the shape of the signal.

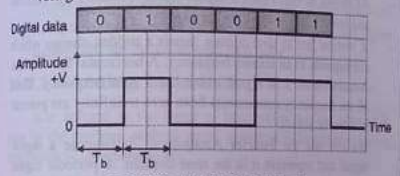
- If the medium has less bandwidth than required, then signal distortion will take place as shown in Fig. 11.6.1.



(L-30) **Fig. 11.6.1 : Importance of channel BW**

11.7 Digital Signals :

- The input data which is either analog or digital can also be represented by a digital signal.
- A digital signal is a discrete time signal having finite number of amplitudes. For example see the digital signal shown in Fig. 11.7.1.
- A 0 is represented by zero volts and a 1 by some positive voltage.



(L-26) **Fig. 11.7.1 : Digital signal**

11.7.1 Bit Interval (T_b) :

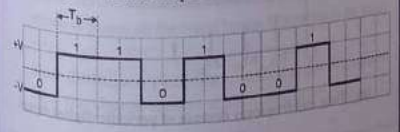
- The bit interval is the time corresponding to one single bit (0 or 1).
- As shown in Fig. 11.7.2, time corresponding to a 0 or a 1 is T_b hence it is the bit interval or bit length.

11.7.2 Bit Rate (Data Rate) :

- Bit rate is defined as the number of bits transmitted or sent in one second. It is expressed in bits per second (bps).
- Relation between bit rate and bit interval is as follows :

$$\text{Bit rate} = \frac{1}{\text{Bit interval}}$$

- Bit rate is also called as signalling rate and is defined as the number of bits which can be transmitted in a second.
- If the bit duration is "T_b" then bit rate will be $1 / T_b$. Look at Fig. 11.7.2, you will see that the bit duration is necessarily equal to the pulse duration.
- In Fig. 11.7.2 the first pulse is of two bit duration.

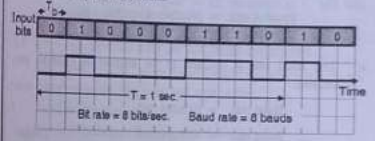


(L-27) **Fig. 11.7.2 : A bit stream**

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

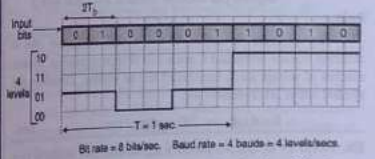
11.7.3 Bauds (or Baud Rate) :

- Baud is the unit of signalling speed or modulation rate or the rate of symbol transmission.
- It indicates the rate at which a signal level changes over a given period of time.
- When binary bits are transmitted as an electrical signal with two levels "0" and "1" the bit rate and the modulation rate i.e. baud rate are same. This is as shown in Fig. 11.7.3(a).
- Note that for a two level signal (binary signal) the bit rate and bauds are equal.
- Now consider Fig. 11.7.3(b) where four different levels are used to represent the data.



(L-28) **Fig. 11.7.3(a) : Baud rate for two level modulation**

- Each level is being represented by a combination of two bits i.e. 00 or 01 etc.
- The bit rate is therefore not equal to the baud rate.
- The bit rate is 8 bits/sec. but baud rate is only 4 bauds as there are 4-levels per second.



(L-29) **Fig. 11.7.3(b) : Baud rate for a four level modulation**

Ex. 11.7.1 : For a binary PCM system, the number of bits per transmitted word is 8 and the sampling frequency f_s = 8 kHz. Calculate the bit rate and baud rate.

Soln. :

Given : N = 8, f_s = 8 kHz

Bit rate = $N \times f_s = 8 \times 8$ kHz = 64 k bits/sec.

Baud rate = Bit rate = 64 kHz
(as transmission is binary)

Ex. 11.7.2 : For the same data in the previous example, calculate the bit rate and baud rate if a QPSK system is used.

Scanned by CamScanner

Soln. :

In the QPSK system, two successive bits are clubbed together to form one message. Hence one symbol corresponds to 2 bit duration.

$\therefore$ Baud rate $= \frac{1}{2} \times$ bit rate $= 32$ k bits/sec.

Bit rate does not change.

Ex. 11.7.3 : A system sends a signal that can assume 8 different voltage levels. It sends 400 of these signals per second. What are the baud and bit rates ?

Soln. :

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

   $\therefore$ Number of bits / symbol = 3

2. The system sends 400 signal / sec. Hence the number of symbols transmitted per second is also 400.

   $\therefore$ Symbol rate = Number of symbols / sec.

   = 400 symbols / sec.

3. The baud rate is defined as the number of symbols per second.

   $\therefore$ Baud rate = Symbol rate.

   $\therefore$ Baud rate = 400 symbols / sec. **...Ans.**

4. We are using 3 bit to represent each symbol.

   So bit rate $= 3 \times$ symbol rate $= 3 \times 400$

   = 1200 bits / sec. **...Ans.**

Ex. 11.7.4 : A system sends a signal that can assume 4 different voltage levels. It sends 200 of such signals per second. What is the baud rate ?

Soln. :

This example is similar to Ex. 11.7.3. A system has 4 different voltage levels and it sends 200 of such signals/sec. Hence number of voltage levels transmitted will be 200/sec. Therefore the symbol rate is 200 symbols / sec.

$\therefore$ Baud rate = 200 symbols / sec. **...Ans.**

Ex. 11.7.5 : A system sends a signal that can assume two different voltage level. It sends 100 of signal per second, what is baud rate ?

Soln. :

1. As the signal assumes 2 different voltage levels we need. 1 bit digital signal to have 2 different combinations. Hence the number of bits per voltage is 1. Let each voltage level represent one symbol.

   $\therefore$ Number of bits / symbol = 1

2. The system sends 100 signals / sec. Hence the number of symbols transmitted per second is also 100.

   $\therefore$ Baud rate = 100 symbols / sec.

11.7.4 Bit Length :

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

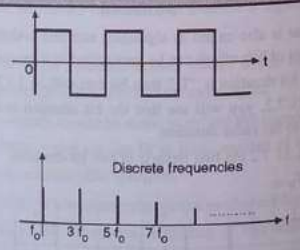
$\therefore$ Bit length = Propagation speed $\times$ Bit duration.

$= \frac{\text{meters}}{\text{sec}} \times \text{sec}$

11.8 Digital Signal as a Composite Analog Signal :

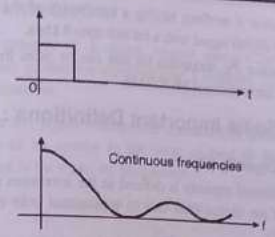
- The digital signal changes its amplitude instantaneously. As mentioned earlier, an instantaneous change in amplitude corresponds to infinite number of frequencies. So a digital signal contains infinite frequency components.
- Hence a digital signal is actually a composite signal. That means the bandwidth of a digital signal is infinite.
- So as to preserve the shape of the digital signal the medium over which it is sent should also have an infinite bandwidth. But practically it does not happen that way.
- As shown in Fig. 11.8.1 a digital signal is made from vertical and horizontal lines in time domain.
- A vertical line in time domain means a sudden change which corresponds to an infinite frequency. A horizontal line in time domain means a dc signal which has a zero frequency. Thus all the frequency components from zero to infinity are present in a digital signal.
- We can use the **Fourier Analysis** to decompose a digital signal and represent it in the time domain. A periodic digital signal (Fig. 11.8.1(a)) can be decomposed into different frequency components as shown in its frequency spectrum of Fig. 11.8.1(a).
- Thus the frequency domain representation of a periodic digital signal has an infinite bandwidth and infinite discrete frequency components as we use Fourier series.
- If the digital signal is nonperiodic as shown in Fig. 11.8.1(b) then also its bandwidth is infinite but the frequencies are continuous as shown in its frequency spectrum of Fig. 11.8.1(b) as we use the Fourier transform.

Note : Bandwidths of both types of digital signals is infinite but the periodic signal has discrete frequency components whereas the nonperiodic signal has continuous frequencies.



(a) Time and frequency domain of periodic digital signal

Fig. 11.8.1 (Contd....)



(b) Time and frequency domain of a nonperiodic signal

(L-776)Fig. 11.8.1

11.9 Digital Versus Analog Bandwidth :

- If we are sending analog data over a medium, then the analog bandwidth of that medium should be considered. Analog bandwidth is expressed in Hz.
- But if the digital data is being sent over a medium, then we should consider its digital bandwidth. The digital bandwidth is expressed in bits per second (bps). The analog and digital bandwidths are different from each other.

11.9.1 Analog Bandwidth :

It is defined as the range of frequencies that are allowed to pass by the medium without much reduction in amplitude. Analog bandwidth is measured in Hz.

11.9.2 Digital Bandwidth :

- It is defined as the maximum bit rate that a medium is able to pass or support. The digital bandwidth is expressed in bits per second (bps).
- Both analog and digital bandwidths should be as large as possible. Ideally they are infinite.
- Now we will discuss the most important question, i.e. whether to use analog signal or digital.
- The choice between analog and digital signals depends on the available bandwidth.

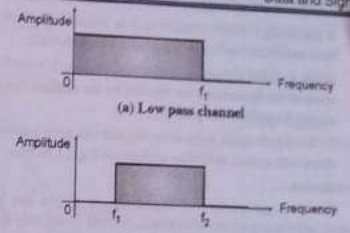
11.9.3 Types of Channels (Mediums) :

There are two types of communication channels or mediums namely :

1. Lowpass channel
2. Bandpass channel

11.9.4 Low-pass Channel :

- As shown in Fig. 11.9.1(a), a low pass channel is that channel whose bandwidth extends right from 0 Hz to f_1 Hz. That means it passes all the signal having frequencies in the range 0 to f_1.
- Since the frequency response is identical to that of a lowpass filter, this channel is called as a low pass channel.



(a) Low pass channel

(b) Band pass channel

(L-775) Fig. 11.9.1 : Types of channels

11.9.5 Bandpass Channel :

- A bandpass channel is a channel which has a bandwidth extending from f_1 to f_2 as shown in Fig. 11.9.1(b).
- It will allow all the signal frequencies in the range f_1 to f_2 only. Any frequency component lying outside this range is not allowed to pass through.
- The lowest frequency signal in the passband is f_1 and not 0 like the low pass signal.

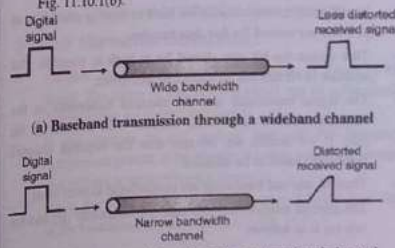
11.10 Transmission of Digital Signals :

The digital signals can be transmitted from one point to the other using one of the following two approaches :

1. Baseband transmission
2. Bandpass transmission (with modulation)

11.10.1 Baseband Transmission :

- A baseband digital signal is the original signal without any modulation. In the modulation process the baseband digital signal is converted into analog signal.
- Baseband transmission is the transmission of baseband digital signal.
- A baseband signal occupies bandwidth from 0 to f_1 Hz.
- Hence baseband transmission requires the use of low pass channel. This low pass channel can have a narrow bandwidth or wide bandwidth.
- If we send the digital signals over the low pass channel with a small bandwidth (telephone cable) then same frequency components in the digital signal get blocked and the shape of the received signal will be badly distorted as shown in Fig. 11.10.1(b).



(a) Baseband transmission through a wideband channel

(b) Baseband transmission through a narrowband channel

(G-1301) Fig. 11.10.1

Scanned by CamScanner

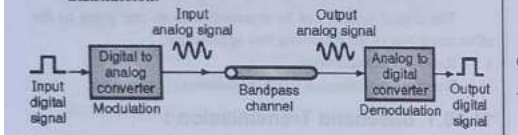
- A practically available medium such as coaxial cable does not have an infinite bandwidth but it has a wide bandwidth.
- When a digital signals is transmitted over such a medium, some of the frequencies are blocked by the medium but still enough frequencies are passed.
- So the digital signal at the receiving end will have a different shape with a small distortion as shown in Fig. 11.10.1(a).

Conclusion :

Baseband transmission of digital signals over a low pass channel without waveform distortion is possible if and only if the channel has a wide or infinite bandwidth.

11.10.2 Broadband Transmission (with modulation) :

- A baseband signal is passed through a D to A converter to obtain an equivalent analog signal. This is modulation and the modulated analog signal is called as a broadband signal.
- Transmission of a broadband signal is known as broadband transmission of digital signal. The spectrum of a broadband signal extends from f_1 to f_2 so it is a bandpass spectrum.
- We have to use a bandpass channel to carry this transmission. Fig. 11.10.2 shows the modulation process and broadband transmission.



(G-1302) **Fig. 11.10.2 : Broadband transmission of digital signal**

- Note that the output digital signal is distortion free.
- We can send the digital signals over a bandlimited medium. The best example of this is the data transfer over telephone cables in Internet.
- The most important question here is that what should be minimum bandwidth of the medium (B Hz) if we want to transmit a signal of n bps.
- The answer to this question will be given when we study the Nyquist theorem and Shannon capacity.

11.10.3 Relation between Required Bandwidth and Bit Rate :

- In computer communication we have to send as many bits as possible per second for fast data transfer.
- That means the bit rate should be as high as possible. But increase in bit rate has an undesired side effect.
- The signal bandwidth and the required bandwidth of the medium (channel bandwidth) increase with increase in bit rate. If we double the bit rate then the required channel bandwidth needs to be doubled.
- Thus bit rate and bandwidth are proportional to each other.
- The general relation between required bandwidth (B) and bit rate (n) is as follows

$$B \geq \frac{n}{2} \text{ or } n \leq 2B.$$

- Thus over a medium having a bandwidth of 4 kHz we can send a digital signal with a bit rate upto 8 kbps.
- In practice the maximum bit rate can be more than 30 kbps using the traditional MODEMS.

11.11 Some Important Definitions :

Channel Capacity (C) :

- The channel capacity is defined as the maximum data rate at which the digital data can be transmitted over the channel reliably.
- The various other concepts related to channel capacity are as follows :
  1. Data rate 2. Bandwidth
  3. Noise 4. Error rate

Data Rate :

- It is defined as the number of bits transmitted by the transmitter per second. It indicates how fast a signal can be transmitted reliably over the given medium.
- This capability depends on the following factors :
  1. The amount of energy put into transmitting each signal.
  2. Distance to be travelled.
  3. Noise.
  4. Channel bandwidth

Channel bandwidth :

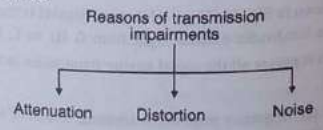
- The bandwidth of the communication medium should be large enough to transmit the digital signal reliably.
- An inadequate bandwidth will distort the signal and introduce errors into the received signal.

Noise : This is the average level of noise over the communication path.

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

11.12 Transmission Impairments :

- In any communication system, the received signal is never identical to the transmitted one due to some transmission impairments.
- The quality of analog signals will deteriorate due to the transmission impairment whereas errors get introduced if the signal is digital.
- The most important reasons for the impairments are as follows :
  1. Attenuation and attenuation distortion
  2. Delay distortion
  3. Noise.



(G-86) **Fig. 11.12.1 : Impairment types**

11.12.1 Attenuation :

- The strength of a signal (signal energy) decrease with increase in distance travelled over a medium. This is known as attenuation.
- When any signal travels over a medium or channel, it loses some of its energy in the form of heat in the resistance offered to the signal by the medium.
- Attenuation is expressed in decibels as,

$$\text{Attenuation (dB)} = 10 \log_{10} \frac{P_{out}}{P_{in}} \quad \text{...(11.12.1)}$$

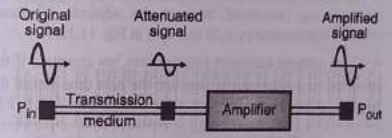
Where P_{in} = Power at the sending end

P_{out} = Power at the receiving end.

- Attenuation decides the signal strength and hence the signal to noise ratio and the quality of received signal.

Remedy to reduce attenuation :

We can introduce amplifiers to compensate for any loss of signal as shown in Fig. 11.12.2. Note that amplification and attenuation are exactly opposite to each other.



(G-87) **Fig. 11.12.2 : Concept of attenuation**

Ex. 11.12.1 : Calculate the attenuation in dB if input power is three times higher than the received power.

Soln. :

$$P_{in} = 3 P_{out}$$

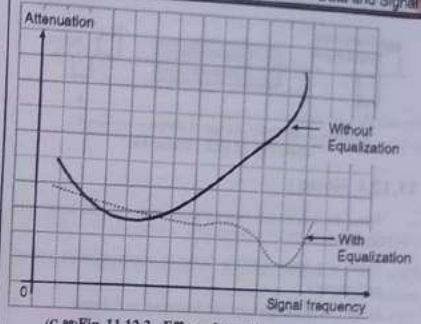
$$\therefore \frac{P_{out}}{P_{in}} = \frac{1}{3}$$

$$\therefore \text{Attenuation in dB} = 10 \log_{10} \frac{P_{out}}{P_{in}} = 10 \log_{10} (1/3)$$

$$= -4.8 \text{ dB} \quad \text{...Ans.}$$

Effect of frequency on attenuation :

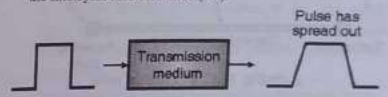
- Attenuation increases with increase in signal frequency.
- The SNR can be improved by using amplifiers or repeaters to boost the signal strength.
- The effect of frequency on attenuation is important if the signal is analog. This effect can be reduced by using equalizers. Another way to do this is to use an amplifier that amplifies the higher frequencies more than lower frequencies.
- The effect of equalization on attenuation is illustrated in Fig. 11.12.3.



(G-88) **Fig. 11.12.3 : Effect of equalizer on attenuation**

11.12.2 Delay Distortion :

- This problem is particularly present in the wired media.
- This distortion is caused due to a property which states that the velocity of propagation of a signal through a medium varies with frequency.
- The velocity is maximum near the center frequency and reduces as the signal frequency deviates away from the center frequency on both sides of frequency spectrum.
- Hence various frequency components of a signal arrive at the receiver at different instants of time resulting in phase shifts between different frequencies.
- This distorts the signal and the distortion is called as delay distortion.
- Delay distortion is particularly important for digital data.
- Due to delay distortion a digital pulse transmitted over a medium tends to spread out as shown in Fig. 11.12.4 causing the intersymbol interference (ISI).



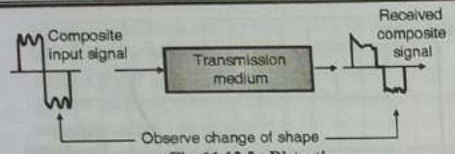
(G-89) **Fig. 11.12.4 : Delay distortion**

- The Intersymbol interference (ISI) put a major limitation on the maximum bit rate over a transmission channel.
- Delay distortion can be reduced by using equalizers.

11.12.3 Harmonic Distortion :

- Another meaning of distortion is change in shape of the signal. The shape of the received signal can be substantially different than the transmitted signal.
- If the medium is not prefect, then all the frequency components present at the input will not be equally attenuated and will not be proportionally delayed.
- Hence the shape of the received signal is different from that of the transmitted signal as shown in Fig. 11.12.5.

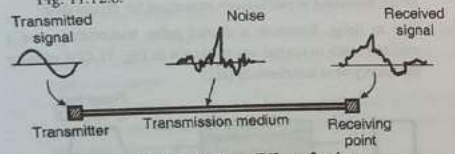
Scanned by CamScanner



(G-90) **Fig. 11.12.5 : Distortion**

11.12.4 Noise :

- When the data travels over a transmission medium, noise gets added to it.
- Noise is a major limiting factor in communication system performance.
- Noise can be categorized into four types as follows :
  1. Thermal noise
  2. Intermodulation noise
  3. Crosstalk
  4. Impulse noise
- Thermal noise is due to the random motion of electrons in a wire. But the noise induced into a wire is generated by the sources such as electric motors and various appliances.
- Crosstalk is the interference caused by one wire to the other one. Here one wire radiates its signal by acting as a sending antenna and the other one acts as a receiving antenna to induce voltage into it.
- Impulse noise is in the form of a high energy spike. It is basically a pulse of short duration which comes from power lines, lightning etc.
- The effect of noise on a signal has been illustrated in Fig. 11.12.6.



(L-779) **Fig. 11.12.6 : Effect of noise**

Thermal Noise :

- It is due to thermal agitation of electrons.
- Thermal noise is present in all electronic devices and the transmission media.
- Thermal noise is proportional to temperature and it is uniformly distributed across the frequency spectrum. So it is called as white noise.
- We cannot eliminate the thermal noise completely. So it puts a limit on the performance of the communication system.
- The thermal noise power is given by,

$$N = kTB \text{ Watts} \quad \text{...(11.12.2)}$$

where k = Boltzman's constant

T = Absolute temperature °K

B = Bandwidth

It can be expressed in dBW as :

$$N = 10 \log k + 10 \log T + 10 \log B$$

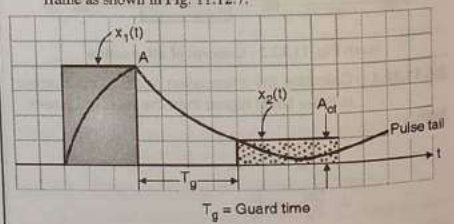
- Thermal noise can be reduced by reducing temperature or bandwidth.

Intermodulation Noise :

- If signals at different frequencies are transmitted simultaneously on a common transmission medium (e.g. FDM) then it results in intermodulation noise.
- The intermodulation produces frequency components at sum and difference frequencies of the frequencies travelling on the medium.
- Suppose signals of frequencies f_1 and f_2 are travelling simultaneously over the same medium, then due to intermodulation produces frequency components $(f_1 + f_2)$ and $(f_1 - f_2)$, which are called intermodulation noise.
- This is similar to a mixer. So whenever there is any non-linearity in the transmitter or channel, the intermodulation noise is produced.

Crosstalk :

- Crosstalk basically means interference between the adjacent telephone channels.
- It is the unwanted coupling of information from one channel to the other adjacent channels. The guard time (T_g) is the time spacing introduced between the adjacent telephone channels represented by $x_1(t)$ and $x_2(t)$ in Fig. 11.12.7.
- A signal without baseband filtering also has crosstalk if the pulse tail or postcursor overlaps into the next time slot of the frame as shown in Fig. 11.12.7.



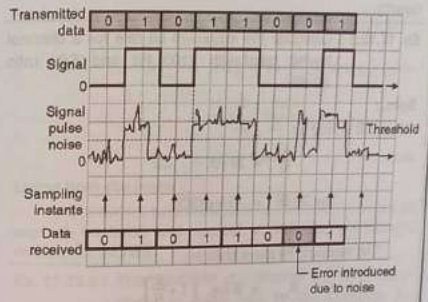
(G-91) **Fig. 11.12.7 : Crosstalk**

- Pulse overlap shown in Fig. 11.12.7 can be controlled by using "guard time" (T_g) between the pulses. The guard time (T_g) is analogous to the guard bands between the channels in the FDM systems.
- In practice crosstalk can be experienced while using a telephone. We can hear another conversation due to crosstalk.
- It can occur due to electrical coupling between nearby twisted pairs or sometimes even in the coaxial cables.
- Typically the magnitude of crosstalk is almost same as that of the thermal noise.

Impulse Noise :

- All the types of noise discussed so far are reasonably predictable and their magnitude is relatively constant.
- So it is a bit easier for the system engineers to deal with them.

- But impulse noise is completely different from the other types. It is non continuous, by nature and it is made of noise spikes of short duration of high amplitude. These noise pulses occure irregularly and they are extremely unpredictable.
- Impulse noise gets generated due to many reasons such as external electromagnetic disturbances, lightning etc.
- Impulse noise does not affect the quality of analog signal to a great extent but it affect the digital data badly because it introduces errors in the digital data as shown in Fig. 11.12.8.
- It is possible to recover the original data by means of sampling as shown in Fig. 11.12.8.



(G-92) **Fig. 11.12.8 : Effect of impulse noise**

11.12.5 Signal to Noise Ratio :

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

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

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

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

Note :

1. A high SNR indicates that the signal is less degraded due to noise.
2. A low SNR indicates that the signal is heavily degraded due to the noise.

11.13 Data Rate Limits :

- In data communication a large data is required to be transferred from one place to the other.
- It is necessary to transfer it as quickly as possible. In other words the data rate in bits per second over a channel should be as high as possible.
- The data rate is decided by the following factors :
  1. The maximum bandwidth.
  2. The signal level.
  3. The noise presented by the channel.
- Two theorems were developed to calculate the data rate and we can use them on the basis of the type of channel as follows :
  1. A noiseless channel : Nyquist theorem
  2. A noisy channel : Shannon's theorem

11.13.1 Noiseless Channel : Nyquist Bit Rate :

- As we know a transmission channel is a medium over which the electrical signals from a transmitter travel to the receiver. Two important characteristics of a transmission channel are :
  1. Signal to Noise ratio (SNR) and
  2. Channel bandwidth.
- These two characteristics will ultimately decide the maximum capacity of a channel to carry information.
- Nyquist and Shannon worked on finding the maximum channel capacity of a bandlimited channel.
- Nyquist's theorem states that if the bandwidth of a transmission channel is "B" which carries a signal having "L" number of levels, then the maximum data rate "R" on this channel is given by,

$$R = 2B \log_2 L \quad \text{...(11.13.1)}$$

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

$$C = 2B \log_2 L \quad \text{...(11.13.2)}$$

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

11.13.2 Noisy Channel : Shannon's Channel Capacity :

- A noiseless channel is not possible in the real world, so Shannon introduced a theorem called Shannon's capacity theorem to determine the highest possible data rate on the noisy channel.
- We have seen the Nyquist bandwidth earlier in this book.
- Shannon extended Nyquist's work. He included the effect of noise present on the transmission channel.
- According to Shannon's theorem, if (S/N) is the signal to noise ratio then the maximum data rate is given by

$$C = R_{max} = B \log_2 \left[1 + \frac{S}{N}\right] \text{ bits/sec} \quad \text{...(11.13.3)}$$

- Shannon's theorem puts a limit on the maximum number of levels for a given (S/N) ratio and bandwidth. This expression shows that the maximum data rate for a communication channel is dependent on the channel bandwidth B and signal to noise ratio (S/N).
- It is important to note that the Shannon's formula does not indicate the signal level. It says no matter how much is the signal level, it is not possible to achieve a data rate (R) which is greater than the capacity of the channel (C).

Scanned by CamScanner

Importance of channel bandwidth :

- Bandwidth of the communication channel should be higher than the bandwidth of the signal that is to be transmitted over it.
- This is essential in order to preserve the shape of the signal being transmitted.
- If the channel bandwidth is less than the signal bandwidth then the signal shape will be distorted when it travels over this channel.

11.13.3 Solved Examples :

Ex. 11.13.1 : A channel has a bandwidth of 5 kHz and a signal to noise power ratio 63. Determine the bandwidth needed if the S/N power ratio is reduced to 31. What will be the signal power required if the channel bandwidth is reduced to 3 kHz ?

Soln. :

1. To determine the channel capacity :

It is given that B = 5 kHz and $\frac{S}{N} = 63$. Hence using the Shannon Hartley theorem the channel capacity is given by,

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

$$= 5 \times 10^3 \log_2 [1 + 63]$$

$$\therefore \quad C = 30 \times 10^3 \text{ bits/sec.} \quad ...(1)$$

2. To determine the new bandwidth :

The new value of $\frac{S}{N} = 31$. Assuming the channel capacity "C" to be constant we can write,

$$30 \times 10^3 = B \log_2 [1 + 31]$$

$$\therefore \quad B = \frac{30 \times 10^3}{5} = 6 \text{ kHz} \quad ...(2)$$

3. To determine the new signal power :

Given that the new bandwidth is 3 kHz. We know that noise power $N = N_o B$.

Let the noise power corresponding to a bandwidth of 6 kHz be $N_1 = 6\ N_o$ and the noise power corresponding to the new bandwidth of 3 kHz be $N_2 = 3\ N_o$.

$$\therefore \quad \frac{N_1}{N_2} = \frac{6\ N_o}{3\ N_o} = 2 \quad ...(3)$$

The old signal to noise ratio $= \frac{S_1}{N_1} = 31$

$$\therefore \quad S_1 = 31\ N_1 \quad ...(4)$$

The new signal to noise ratio $= \frac{S_2}{N_2}$. We do not know its value, hence let us find it out.

$$30 \times 10^3 = 3 \times 10^3 \log_2 \left(1 + \frac{S_2}{N_2}\right)$$

$$\therefore \quad \frac{S_2}{N_2} = 1023 \quad ...(5)$$

$$\therefore \quad S_2 = 1023\ N_2$$

But from Equation (3), $N_2 = \frac{N_1}{2}$, substituting we get,

$$\therefore \quad S_2 = 1023 \frac{N_1}{2} \quad ...(6)$$

Dividing Equation (6) by Equation (4) we get,

$$\therefore \quad \frac{S_2}{S_1} = \frac{1023\ N_1}{2 \times 31\ N_1} = 16.5$$

$$\therefore \quad S_2 = 16.5\ S_1 \quad ...\textbf{Ans.}$$

Thus if the bandwidth is reduced by 50% then the signal power must be increased 16.5 times i.e. 1650% to get the same capacity.

Ex. 11.13.2 : Calculate the maximum bit rate for a channel having bandwidth 3100 Hz and S/N ratio 20 dB.

Soln. :

Given : B = 3100 Hz

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

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

$$\therefore \quad S/N = 100$$

The maximum bit rate is given by,

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

$$= 3100 \log_2 [1 + 100]$$

$$= \frac{3100 \log_{10} 101}{\log_{10} 2}$$

$$= 20{,}640 \text{ bits/sec.} \quad ...\textbf{Ans.}$$

Ex. 11.13.3 : Calculate the maximum bit rate for a channel having bandwidth 3100 Hz and S/N ratio 10 dB.

Soln. :

Given : B = 3100 Hz

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

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

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

$$\therefore \quad \text{Maximum bit rate} = R_{max} = B \log_2 \left[1 + \frac{S}{N}\right]$$

$$= 3100 \log_2 (1 + 10)$$

$$= \frac{3100 \log_{10} 11}{\log_{10} 2}$$

$$= 10{,}724 \text{ bits/s} \quad ...\textbf{Ans.}$$

Ex. 11.13.4 : Calculate the maximum bit rate for a channel having bandwidth 1600 Hz if :

(a) S/N ratio is 0 dB

(b) S/N ratio is 20 dB.

Soln. :

Given : B = 1600 Hz

(a) R_{max} for S/N = 0 dB :

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

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

$$\therefore \quad R_{max} = B \log_2 (1 + S/N) = 1600 \log_2 (1 + 1)$$

$$= 1600 \text{ bits/sec} \quad ...\textbf{Ans.}$$

(b) R_{max} for S/N = 20 dB :

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

$$\therefore \quad 20 = 10 \log_{10} (S/N) \qquad \therefore \frac{S}{N} = 100$$

$$\therefore \quad R_{max} = B \log_2 \left(1 + \frac{S}{N}\right) = 1600 \log_2 (101)$$

$$= \frac{1600 \log_{10} (101)}{\log_{10} (2)}$$

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

Using both the limits :

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

Ex. 11.13.5 : The bandwidth of a channel is 2 MHz and its signal to noise ratio is 63. Calculate the appropriate bit rate and signal level.

Soln. :

Step 1 : Calculate the upper limit using Shannon's theorem :

$$C = B \log_2 \left(1 + \frac{S}{N}\right) = 2 \times 10^6 \log_2 (1 + 63)$$

$$= 12 \text{ M bits / sec.}$$

This is the upper limit. For ensuring a better performance we select a somewhat lower value say 8 Mbps.

Step 2 : Calculate number of signal levels using Nyquist theorem :

$$C = 2 B \log_2 L$$

$$\therefore \quad 8 \times 10^6 = 2 \times 2 \times 10^6 \log_2 L$$

$$\therefore \quad 2 = \log_2 L$$

$$\therefore \quad L = 4 \quad ...\textbf{Ans.}$$

Ex. 11.13.6 : Calculate the maximum bit rate of channel having bandwidth 1200 Hz if :

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

Soln. :

Given :

1. B = 1200 Hz.

R_{max} for S/N = 0 dB

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

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

$$\therefore \quad R_{max} = B \log_2 \left(1 + \frac{S}{N}\right)$$

$$= 1200 \log_2 (1 + 1)$$

$$= 1200 \text{ bits/sec} \quad ...\textbf{Ans.}$$

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

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

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

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

$$\therefore \quad R_{max} = B \log_2 \left(1 + \frac{S}{N}\right)$$

$$= 1200 \log_2 (101)$$

$$= 1200 \frac{\log_{10} (101)}{\log_{10} (2)}$$

$$= 7990 \text{ bits/sec}$$

Maximum bit rate = 1200 bits/sec for 0 dB ...**Ans.**

Maximum bit rate = 7990 bits/sec for 20 dB

Ex. 11.13.7 : Find the number of coding or symbol levels if C = 31000 bits/s and B is 3100 Hz.

Soln. : C is the channel capacity while B is the bandwidth.

According to Shannon's theorem,

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

where S/N is the signal to noise ratio.

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

$$\therefore \quad \log_2 \left(1 + \frac{S}{N}\right) = 10$$

$$\therefore \quad \frac{S}{N} = 1023 \text{ or } 30\text{dB}$$

$$\left(\frac{S}{N}\right) dB = 1.8 + 6\ NdB$$

$$\therefore \quad 30 = 1.8 + 6N$$

where N = Number of bits per word.

$$\therefore \quad N = 4.72 = 5$$

Number of symbol levels $Q = 2^N = 2^5 = 32$ ...**Ans.**

Ex. 11.13.8 : Calculate the channel capacity for a noisy channel having bandwidth = 5 kHz and SNR = 0 using appropriate formula.

Soln. :

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

Find : Channel capacity.

1. To determine channel capacity :

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

$$= 5 \times 10^3 \log_2 [1 + 0]$$

$$C = 0 \text{ bits/sec.} \quad ...\textbf{Ans.}$$

Scanned by CamScanner

Ex. 11.13.9 : An analog signal has a bit rate of 8000 bps and a baud rate of 1000 baud. How many data elements are carried by each signal element ? How many signal elements do we need ?

Soln. :

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

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

Step 1 : Calculate R :

Bit rate = Numbers of data elements per signal × baud rate

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

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

Step 2 : Calculate L :

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

Ex. 11.13.10 : State and explain the Nyquist theorem and Shannon capacity and solve the following example :

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

Soln. : For Nyquist theorem and Shannon capacity refer sections 11.13.1 and 11.13.2.

Given : B = 3000 Hz, L = 2

To find : Maximum bit rate

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

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

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

11.14 Performance :

- The performance of a data communication network can be measured with the help of the following parameters :
  1. Bandwidth 3. Jitter.
  2. Delay 4. Throughput
- We will discuss them one by one in the following sections.

11.15 Bandwidth :

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

BW in Hz :

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

BW in bits per second :

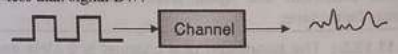
We can also define bandwidth as the number of bits per second (bps) that a channel or network can transmit. For example the BW of Fast Ethernet is 100 Mbps i.e. that network can transmit 100 Mbps.

Relationship :

- There is a clear relationship between the bandwidth in Hz and BW in bps. With increase in BW in Hz, there is an increase in bps bandwidth.
- The relation between them depends on whether baseband transmission is being used or transmission with modulation is being used.

11.15.1 Signal and Channel Bandwidths :

- We can define two different bandwidths :
  1. Signal bandwidth 2. Channel bandwidth
- Signal bandwidth B_s is defined as the range of frequencies contained in the signal.
- Whereas the bandwidth of a channel B_c is the range of frequencies that is passed by a channel.
- If the bandwidth of the input signal is larger than the channel bandwidth, then the output of the channel will not contain all the frequencies of the input signal.
- Fig. 11.15.1 shows a typical digital signal at the input and the output is of different shape than input, if the channel BW is less than signal BW.



(G-698) **Fig. 11.15.1 : Effect of $B_c < B_s$**

- If the signaling rate of input signal is increased, then the channel bandwidth has to be increased so as to pass the signal without any change in shape of the signal.
- The maximum rate at which pulses can be transmitted through the channel is given by,

$$r_{max} = 2 \text{ W pulses/sec.}$$

where, $W = 1/2\tau$ and τ = Smallest pulse width of input signal.

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

$$C = B_c \log_2 \left(1 + \frac{S}{N}\right) \text{ bits/sec.} \qquad \text{...(11.15.1)}$$

- The channel capacity should be as high as possible and to increase C. We have to increase the channel bandwidth B_c.
- For a telephone channel B_c = 3.4 kHz. If SNR = 10,000 then the channel capacity is given by,

$$C = 3400 \log_2 (1 + 10000)$$

$$= 45,200 \text{ bits/sec.}$$

- That means we can transmit at a maximum rate of 45.2 kbits per second on the telephone channel.

11.16 Throughput (T) :

- The throughput is a parameter that is used to know the speed of data transmission over a network.

- The throughput of a system is defined as the actual rate at which the information is sent over the channel. It is measured in bits/second or frames/second.
- Throughput is a measure of performance of any network.
- The definitions of bandwidth and throughput appear to be the same but they are not. They are different.
- If B is the bandwidth and T is the throughput of a network then T is always less than and at the most equal to B.
- Thus bandwidth is the theoretical measurement while throughput is the actual measurement of how fast data can be sent.

Ex. 11.16.1 : A network has a bandwidth of 20 Mbps. It can pass 15,000 frames per minute and each frame contains 10,000 bits. Calculate the throughput. Comment on the result.

Soln. :

Given : $B = 20 \times 10^6$ bps, Number of frames = 15000 per min, Number of bits per frame = 10,000.

Throughput T = Number of frames per sec. × Number of bits per frame

$$= \frac{15000}{60} \times 10{,}000 = 3.5 \text{ Mbps.} \qquad \text{... Ans.}$$

Comment :

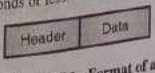
The value of B = 20 Mbps shows the potential of the network and T = 3.5 Mbps shows the actual capability.

11.17 Latency (Delay) :

- The latency or delay is defined as the time required for an entire message to reach its destination from the instant at which the first bit was sent out from the source.
- Latency is the sum of four delay components viz :
  1. Processing delay 2. Queueing delay
  3. Transmission delay 4. Propagation delay.
- The sum of all these delays amounts to the total delay or latency.

1. Processing delay :

- A packet consists of a header and a data field as shown in Fig. 11.17.1. The header contains the destination address.
- The time required to examine the packet header and deciding the direction in which the packet is to be sent is a part of the processing delay.
- The processing delay may also include some other factors such as the time required to check the errors.
- The processing delay is of the order of few microseconds or less.



(G-696(a)) **Fig. 11.17.1 : Format of a packet**

2. Queueing delay :

- At the queue, the packets experience a queueing delay, when they wait to get transmit on the links.
- The queueing delay depends on the number of packets arrived earlier in the queue.
- With no waiting packets in the queue, the queueing delay will be equal to zero.
- Queueing delays can be of the order of microseconds or milliseconds in practice.

3. Transmission delay :

- The packets are transmitted on the first come first served basis. So a particular packet can get transmitted only after all the earlier packets are transmitted.
- Transmission delay is also called as store and forward delay. It is the time required to push (transmit) all the packet bits into the link.
- Typically, the transmission delay is of the order of microseconds or milliseconds in practice.

$$\text{Transmission delay} = \frac{\text{Message size}}{\text{Bandwidth}}$$

4. Propagation delay :

- The time required for the packet bits to reach from the beginning of the link to the desired router is called as propagation delay.
- The signals travel at a speed which is slightly less than that of light.
- So propagation delay is the ratio of the distance to be travelled by the signal to the speed of propagation.
- Practically the propagation delays are of the order of few milliseconds.

$$\text{Propagation delay} = \frac{\text{Distance}}{\text{Propagation speed}}$$

11.18 Jitter :

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.

Scanned by CamScanner

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.

11.18.1 Difference between Delay and Jitter :

End to end delay :

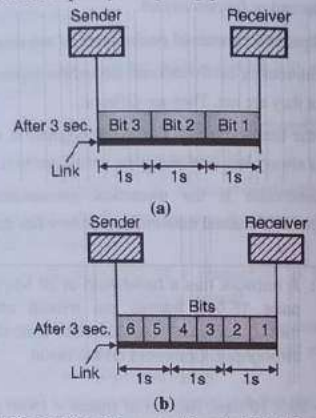
- End to end delay is the time required for the signal to travel from transmitter to receiver.
- This delay is due to the time required for buffering, queueing, switch and routing.
- This time delay remains the same for all the types of packets in the same flow.

Jitter :

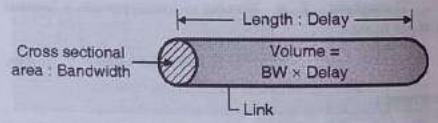
Jitter is defined as the variation in delay for the packets belonging to the same flow. This is the difference between end to end delay and jitter.

11.19 Bandwidth Delay Product :

- Bandwidth and delay are the two most important performance parameters of a link. But more important than them individually is their product i.e. the Bandwidth Delay Product.
- The bandwidth delay product indicates the number of bits that can fill the entire link from the sender to receiver as shown in Fig. 11.19.1(a).
- Assume that the BW is 1 bps and delay is 3 sec. Then the bandwidth delay product will amount to 3 bits then the bandwidth delay product is equal to 1 bps × 3s = 3 bits.
- With 1 bit per second and 3 second delay, the first bit will reach the destination after 3 seconds as shown in Fig. 11.19.1(a). After 3 seconds the entire link will be filled and there will be 3 bits on the link as shown.
- Now consider that the bandwidth is 2 bps and delay is same i.e. 3 second. Then as shown in Fig. 11.19.1(b) the number of bits filling the entire link will be 6 = 2 bps × 3 sec.
- Thus the bandwidth delay product give us the number of bits that can fill the entire link.
- We may think of the link between the sender and receiver as a pipe as shown in Fig. 11.19.1(c). Then the cross-sectional area of the pipe will represent the bandwidth and the length of the pipe will represent the delay.
- Hence the volume of the pipe will represent the bandwidth delay product. More the volume higher the number of bits required to completely fill up the pipe.



(G-1545) **Fig. 11.19.1 : Concept of bandwidth delay product**



(G-700) **Fig. 11.19.1(c) : BW delay product**

Review Questions

Q. 1 What is Shannon's channel capacity ?

Q. 2 State and explain the term Nyquist's bandwidth.

Q. 3 What is the significance of channel capacity ?

Q. 4 Explain the effect of channel bandwidth.

Q. 5 What is meant by impulse noise ?

Q. 6 Write a short note on crosstalk and guard time.

Q. 7 What is delay distortion and what is its effect ?

Q. 8 State and explain various transmission impairments.

Q. 9 Define bandwidth in Hz and in bps.

Q. 10 What is throughput ? How is it different from bandwidth ?

Q. 11 Define latency and its four components.

Q. 12 What is jitter ?

Q. 13 Explain the concept of bandwidth delay product.

Q. 14 Define analog and digital signals.

Q. 15 Define signal bandwidth and channel bandwidth.

Q. 16 Define : Bit interval, Bit rate, Baud rate.

CHAPTER 12

Module VI

Digital and Analog Transmission

Syllabus :

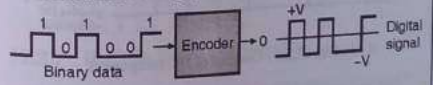
Digital to digital conversion, Analog to digital conversion, Analog transmission : Digital to analog conversion, Analog to analog conversion.

12.1 Digital Transmission :

- To send information from one point to other a computer network is designed.
- But for transmission it is necessary that, this information is to be converted to either analog or digital signal.
- In the following sections we will discuss digital-to-digital conversion and analog-to-digital signal.
- We have to use **digital-to-digital conversion** technique if data is digital and **analog-to-digital** conversion technique if data is analog.

12.2 Digital to Digital Conversion :

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

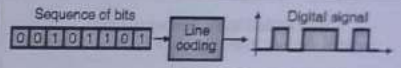


(L-254) **Fig. 12.2.1 : Digital to digital conversion**

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

12.2.1 Definition of Line Coding :

- The line coding is defined as the process of converting binary data, a sequence of bits to a digital signal.
- The digital data such as text, numbers, graphical images, audio and video are stored in computer memory in the form of sequences of bits.
- Line coding converts these sequences into digital signals as shown in Fig. 12.2.2.



(L-255) **Fig. 12.2.2**

12.2.2 Some Important Characteristics of Line Coding :

Some of the important characteristics of line coding are :

1. Signal level and data level
2. Pulse rate and bit rate
3. DC component
4. Self synchronization

12.2.3 Signal Level and Data Level :

- A digital such as binary, octal, hex signal has a limited number of values. However all of them are not used to represent the data. Instead some of them only are used for representing the data.
- The remaining values are used for some other purpose.

Signal levels :

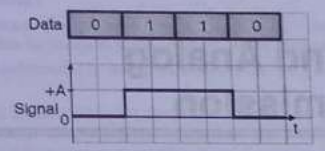
The number of values allowed in a particular signal is defined as the number of signal levels. Refer Fig. 12.2.3 for better understanding.

Data levels :

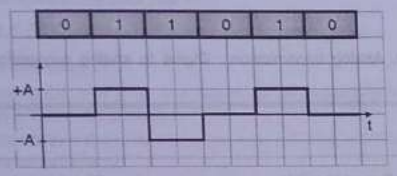
The number of values to represent data is called as the number of data levels. The binary data has two values 0 and 1.

- Fig. 12.2.3 gives you a clear idea about signal levels and data levels.
- Fig. 12.2.3 (a) has two signal levels (0 and A) and two data levels (0 and 1) whereas Fig. 12.2.3(b) has three signal levels (0, + A and – A) and two data levels.

Scanned by CamScanner



(a) Two signal levels, two data levels



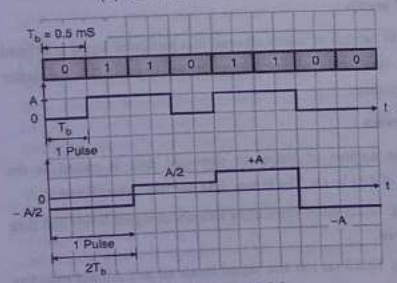
(b) Two data levels, three signal levels
(L-256) **Fig. 12.2.3**

12.2.4 Pulse Rate and Bit Rate :

- **Pulse Rate** is defined as the number of pulses per second and a pulse is defined as the minimum amount of time required to transmit a symbol.
- **Bit Rate** is defined as the number of bits per second. It one pulse corresponds to one bit then the pulse rate is equal to the bit rate. But if a pulse carries more than 1 bit then the pulse rate is lower than bit rate.
- The relation between bit rate and pulse rate is as follows.

$$\text{Bit rate} = \text{Pulse rate} \times \log_2 L \quad \ldots(12.2.1)$$

Ex. 12.2.1 : For the signals shown in Fig. P. 12.2.1(a) and (b) calculate the bit rate and pulse rate.



(L-257) **Fig. P. 12.2.1**

Soln. :

- The data has two levels and the bit duration $T_b = 0.5$ mS.
- Refer Fig. P. 12.2.1(a) which shows that there are two signal levels (0 or A).

$$\therefore \text{ Pulse rate} = \frac{1}{0.5 \times 10^{-3}}$$

$$= 2000 \text{ pulses / sec.}$$

$$\text{and Bit rate} = 2000 \times \log_2 2 = 2000 \text{ bps}$$

- Refer Fig. P. 12.2.1(b). Now one pulse corresponds to a duration of $2\,T_b$.

$$\text{So pulse duration} = 2\,T_b = 1 \text{ mS.}$$

$$\therefore \text{ Pulse rate} = \frac{1}{1 \times 10^{-3}}$$

$$= 1000 \text{ pulses / sec.}$$

$$\text{And Bit rate} = \text{Pulse rate} \times \log_2 L$$

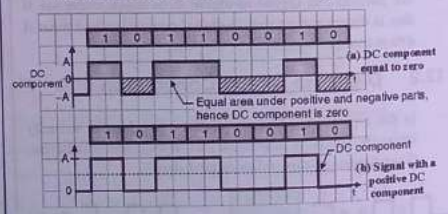
$$\text{Here } L = 4 \text{ levels}$$

$$\text{Bit rate} = 1000 \times \log_2 4$$

$$= 2000 \text{ bps.}$$

12.2.5 DC Component :

- Over one cycle period of a waveform, if all the positive voltages are cancelled by negative voltages then the DC component of the waveform is zero. (See Fig. 12.2.4(a)).



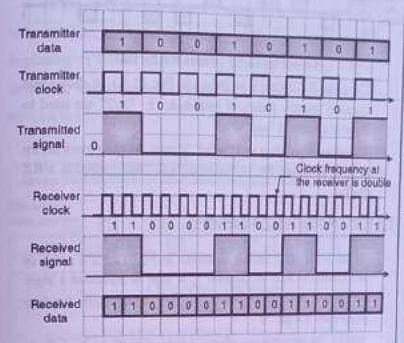
(L-258) **Fig. 12.2.4 : Concept of DC component**

- But the waveform of Fig. 12.2.4(b) has a positive dc component because the instantaneous voltage can be either zero or positive.
- In line coding, the signal with a non-zero dc component is treated as a distorted one and it can create errors in the received signal.
- The signals with a dc component cannot pass through a transformer. Hence the signals with zero dc component are preferred.

12.2.6 Self Synchronization :

- If the receiver's bit intervals correspond exactly to the sender's bit intervals, only then it is possible to receive (recognize) a signal correctly.

- The clock frequency of the transmitter and receiver should be the same.
- If the clock frequency at the receiver is slower or faster then the bit intervals are not matched and the received signal is different that the transmitted one.
- Fig. 12.2.5 illustrates the effect of change in clock frequency. The receiver clock frequency is twice that of the transmitter frequency. So received data is totally different than the transmitted one.



(L-259) **Fig. 12.2.5 : Concept of synchronization**

- Such thing would not happen if the receiver clock is **synchronized** with the transmitter clock.
- To achieve this, the transmitted digital signal includes the timing information. This will force the self synchronization.
- For achieving synchronization, the transmitted signal should cross the zero frequently. So if the transmitted signal consists of long trains of 0's or 1's, then the synchronization is affected.

12.2.7 Built in Error Detection :

A line code should have a built in error detection capability, so that at least some if not all the errors which have been introduced during the transit can be detected. Some encoding schemes discussed in this chapter have the error detection capability.

12.2.8 Immunity to Noise Interference :

Noise immunity is another desirable property of a line code. The noise interference should not be allowed to induce errors in the line codes.

12.2.9 Complexity :

A line code should be as simple as possible. A line coding scheme which uses four signal levels is more complex than that using two signal levels.

12.2.10 Bandwidth :

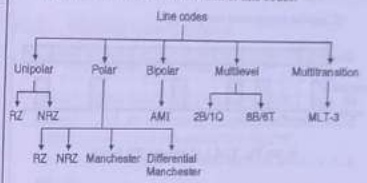
- Most digital signals that we come across have a finite bandwidth. This is not the absolute bandwidth but it is the effective bandwidth.
- The bandwidth is proportional to the signal rate (baud rate). The minimum bandwidth is given by,

$$B_{min} = C \times N \times \frac{1}{r}$$

Where C = Case factor, N = Data rate bps

12.3 Classification of Line Codes :

- Fig. 12.3.1 shows the classification of line codes.



(L-260) **Fig. 12.3.1 : Classification of line codes**

The line codes are basically divided into three categories :

1. Unipolar codes
2. Polar codes
3. Bipolar codes

1. Unipolar codes :

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

2. Polar codes :

- Polar coding using two voltage levels other than zero such as + A/2 and – A/2 volts.
- This will bring the dc level for some codes to zero which is a desired characteristics.

3. Bipolar codes :

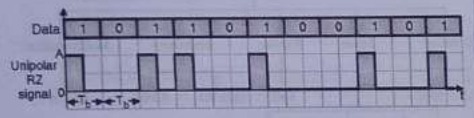
- Bipolar coding uses three voltage levels positive, negative and zero which is similar to polar codes.
- But here the zero level is always used for representing the "0" in the data stream at the input.

Scanned by CamScanner

12.4 Unipolar Line Codes :

12.4.1 Unipolar RZ Format :

- The return to zero (RZ) unipolar format is as shown in Fig. 12.4.1.
- In this format each "0" is represented by an off pulse (0) and each "1" by an on pulse with amplitude A and a duration of $T_b/2$, followed by a return to zero level.
- Therefore this is called as return to zero (RZ) format. As the voltage level is either + A or zero, this is a unipolar format. (Unipolar means only one polarity).

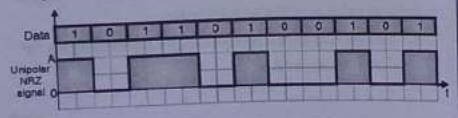


(L-262) **Fig. 12.4.1 : Unipolar RZ format**

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

12.4.2 Unipolar NRZ Format :

- A non-return to zero (NRZ) format is as shown in Fig. 12.4.2.
- In this format a logic "1" is represented by a pulse of full bit duration T_b and amplitude + A while a logic "0" is represented by an off pulse or zero amplitude.
- During the on time, the pulse does not return to zero after half bit period. Therefore the name NRZ format.
- As the pulses have either + A or 0 amplitude it is called as a unipolar format.
- Internal computer waveforms are usually of this type. Due to the unipolar nature, the unipolar NRZ format also will have a nonzero average (dc) value which does not carry any information.
- Due to longer pulse duration, the NRZ pulses carry more "energy" than the RZ pulses. But they need synchronization at the receiver as there is no separation between the adjacent pulses.

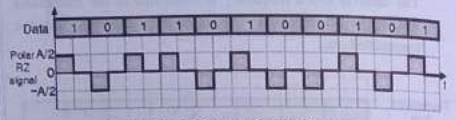


(L-263) **Fig. 12.4.2 : Unipolar NRZ format**

12.5 Polar Line Codes :

12.5.1 Polar RZ Format :

- The disadvantage of the two unipolar formats discussed earlier is that they result in a dc component that does not carry any information and wastes power.

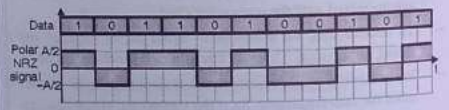


(L-264) **Fig. 12.5.1 : Polar RZ format**

- The polar RZ format is as shown in Fig. 12.5.1. It shows that opposite polarity pulses of amplitude ± "A/2" are used to represent logic "1" and "0".
- Therefore it is called as a "polar" format. As the pulses return to zero after half the bit duration "$T_b/2$" this format is a RZ format.

12.5.2 Polar NRZ Format :

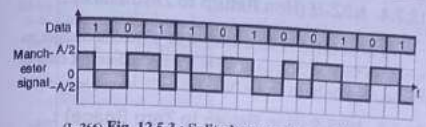
- In the polar NRZ format, as shown in Fig. 12.5.2 a pulse of amplitude "+ A/2" of duration T_b is used to represent a logic "1" and a pulse of amplitude "– A/2" of the same duration represents a logic "0".
- Unlike the unipolar waveform, a polar waveform has no dc component if the 0s and 1s in the input data occur in equal proportion.



(L-265) **Fig. 12.5.2 : Polar NRZ format**

12.5.3 Split Phase Manchester Format :

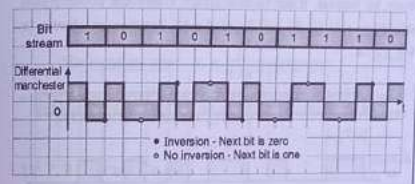
- The split phase Manchester format is as shown in Fig. 12.5.3.
- In this format, symbol "1" is represented by transmitting a positive pulse of "+ A/2" amplitude for one half of the symbol duration, followed by a negative pulse of amplitude "– A/2" for remaining half of the symbol duration.
- For symbol "0" these two pulses are transmitted in reverse order.
- This waveform does not have any dc component.
- The Manchester format has a built in synchronization capability as it crosses zero at regular intervals. But this capability is attained at the expense of a bandwidth requirement of twice that of the NRZ unipolar, polar and bipolar formats.
- Local Area Networks (LAN) such as Ethernet and Cheapernet are increasingly using the Manchester code for signal transmission over the network.



(L-266) **Fig. 12.5.3 : Split phase manchester format**

12.5.4 Differential Manchester Code :

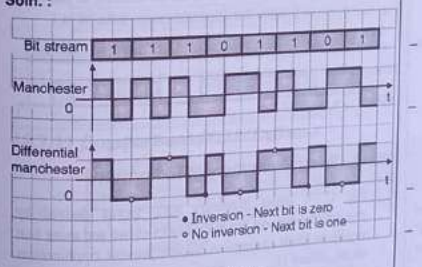
In this code there is always a transition in the middle of a bit interval. The binary zero has an additional transition at the beginning of the bit interval. This is as shown in Fig. 12.5.4 as inversion. There will be no additional transition (inversion) if the next bit is a 1.



(L-286(a)) **Fig. 12.5.4 : Differential Manchester Coding**

Ex. 12.5.1 : Show the Manchester and differential Manchester encoding pattern for the bit stream 11101101.

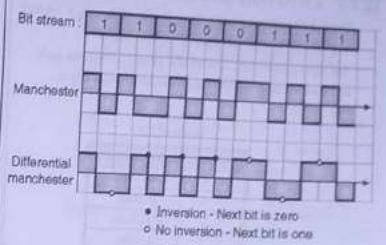
Soln. :



(L-287) **Fig. P. 12.5.1**

Ex. 12.5.2 Show Manchester and differential Manchester encoding pattern for the bit stream 11000111.

Soln. :

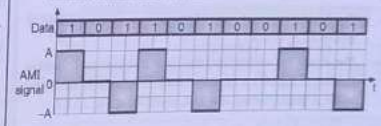


(L-288) **Fig. P. 12.5.2**

12.6 Bipolar Line Codes :

12.6.1 Bipolar NRZ Format (AMI) :

- The bipolar NRZ format is as shown in Fig. 12.6.1. Here the successive "1s" are represented by pulses with alternating polarity, and no pulse is transmitted for a logic "0".
- Note that in this representation there are three levels : + A, 0 and – A.
- Therefore this is also known as "pseudoternary or alternative mark inversion (AMI)" format.



(L-268) **Fig. 12.6.1 : Bipolar NRZ format (AMI)**

- An attractive feature of the bipolar format is the absence of a dc component eventhough the input binary data may contain long strings of "0s" and "1s".
- Moreover the bipolar format eliminates ambiguity that may arise because of polarity inversion during the course of transmissions. (This problem is observed in the switched telephone networks).
- This is the reason why the bipolar NRZ format is used in the PCM-TDM T_1 system for digital telephony.
- The absence of dc component allows the use of transformers for coupling.

12.7 Some other Line Codes :

Some other line codes have been created for some special applications. They are :

1. 2 BIQ
2. Polar Quaternary
3. MLT - 3
4. Biphase M
5. Biphase S

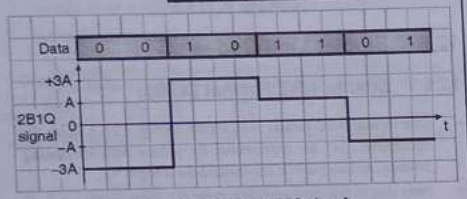
Scanned by CamScanner

12.7.1 2 B1Q (Two Binary, One Quaternary) :

- The 2 BIQ code uses four voltage levels – 3A, – A, + 3A and + A in order to represent the digital input sequence.
- The input data bits are divided into groups of two bits each and each group is represented by one level as shown in Fig. 12.7.1.

Table 12.7.1

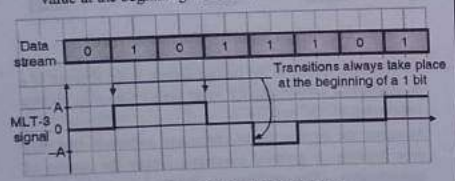
Message	Level assigned
0 0	– 3A Volts
0 1	– A Volts
1 0	+ 3A Volts
1 1	+ A Volts



(L-269) **Fig. 12.7.1 : 2 BIQ signal**

12.7.2 MLT-3 (Multi Line Transmission, Three Level) :

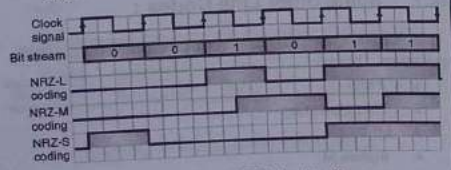
- The MLT-3 is similar to NRZ-I but it uses three levels of signals (+ A, 0, – A).
- The signal will change its value from one level to the next at the beginning of a 1 bit and there is no change in the signal value at the beginning of a 0 bit, as shown in Fig. 12.7.2.



(L-271) **Fig. 12.7.2 : MLT-3 signal**

12.7.3 NRZ-L (Non Return to Zero Level) :

- In NRZ-L coding a bit 0 or 1 is represented by a voltage level which remains constant during the bit duration. A binary "1" is represented by a high level and "0" is represented by a low level.



(L-272) **Fig. 12.7.3 : NRZ signal coding**

12.7.4 NRZ-M (Non Return to Zero Mark) :

As shown in Fig. 12.7.3, in NRZ-M the waveform changes its level when the binary digit is "1". The waveform does not change its level when the binary digit is "0".

12.7.5 NRZ-S (Non Return to Zero Space) :

As shown in Fig. 12.7.3, in NRZ-S the waveform changes its level when the binary digit is "0". The waveform does not change its level when the binary digit is "1".

The other line codes are RZ (return to zero), AMI, manchester etc.

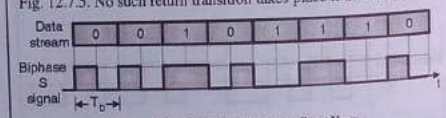
12.7.6 Biphase-M Code :

In this code, there is always a transition at the beginning of every bit interval. If the bit is a binary 1 then the coded signal returns to zero in the middle of the bit duration as shown in Fig. 12.7.4.

(L-273) **Fig. 12.7.4 : Biphase-M coding**

12.7.7 Biphase-S Code :

In this code also there is always a transition at the beginning of every bit interval. If the data bit is a binary 0 then the coded signal returns to zero in the middle of the bit duration as shown in Fig. 12.7.5. No such return transition takes place if the bit is 1.



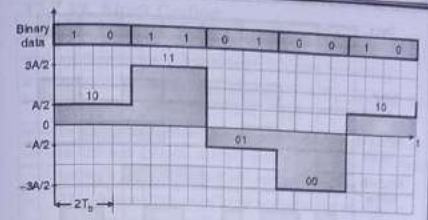
(L-274) **Fig. 12.7.5 : Biphase-S coding**

12.7.8 Polar Quaternary NRZ Format :

- Fig. 12.7.6 shows quaternary NRZ format derived by grouping the message bits in the blocks of two and using four amplitude levels to represent the four possible combinations 00, 01, 10 and 11.
- To these four combinations, four amplitude levels are assigned, as shown in Table 12.7.2.

Table 12.7.2

Message combination	$x(t) = a_k$
0 0	– 3 A/2
0 1	– A/2
1 0	A/2
1 1	3 A/2



(L-275) **Fig. 12.7.6 : Polar quaternary NRZ format**

- In the waveforms of Fig. 12.7.6, the first combination of two bits is "10" hence it is represented by a level "A/2".
- The second combination is "11" hence it is represented by a level of "3A/2". Thus here for a message of two bits only one pulse of duration $D = 2\,T_b$ is transmitted.

$$\therefore\ D = 2\,T_b \qquad ...(12.7.1)$$

$$\text{The signaling rate :}\quad r = \frac{1}{2\,T_b}\ \text{messages/sec} \qquad ...(12.7.2)$$

- If there are "M" levels obtained from the combination of "k" bits (here M = 4 and k = 2) then :

$$M = 2^k \qquad ...(12.7.3)$$

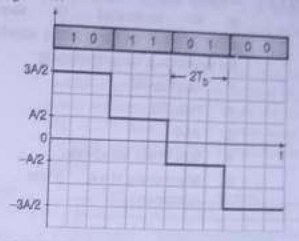
12.7.9 Gray Code :

- There is another scheme used for coding the quaternary format. It is called as the gray code.
- The gray coding scheme is illustrated in the following table. The adjacent bits are arranged in such a way that they differ by only one bit.

Table 12.7.3 : Gray encoding

Message combination	x (t)
0 0	– 3 A/2
0 1	– A/2
1 1	A/2
1 0	3 A/2

- The polar quaternary format with gray coding is shown in Fig. 12.7.7.



(L-276) **Fig. 12.7.7 : Polar quaternary format with gray coding**

12.7.10 Differential Encoding :

- The differential encoding format is shown in Fig. 12.7.8.
- The advantage of differential encoding is that it is immune from the polarity inversion-ambiguity problem.
- Differential encoding starts with an arbitrary initial bit.
- Corresponding to every 0 at the input, the differential encoding format make a transition from + A to – A or – A to + A whereas no transition takes place corresponding to a logic 1 at the input.

(L-277) **Fig. 12.7.8 : Differential encoding format**

- The original binary information can be recovered by sampling the received wave and comparing the polarities of the adjacent samples.

12.7.11 Comparison of Line Codes :

Sr. No.	Parameter	Polar RZ	Polar NRZ	AMI	Manchester	Polar Quaternary NRZ
1.	Transmission of DC component	Yes	Yes	No	No	Possible
2.	Signaling rate	$1/T_b$	$1/T_b$	$1/T_b$	$1/T_b$	$1/2T_b$
3.	Noise immunity	Low	Low	High	High	High
4.	Synchronizing capability	Poor	Poor	Very good	Very good	Poor
5.	Bandwidth required	$1/T_b$	$1/2T_b$	$1/2T_b$	$1/T_b$	$1/2T_b$
6.	Crosstalk	High	High	Low	Low	Low

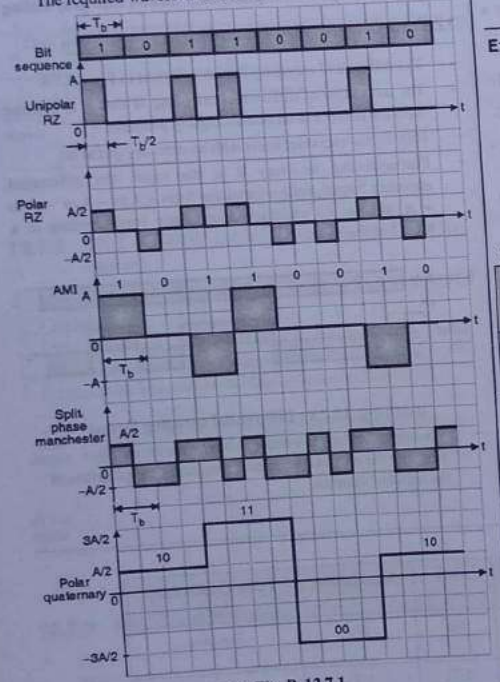
Scanned by CamScanner

Ex. 12.7.1 : Consider that the bit sequence given below is to be transmitted. Bit sequence = 10110010. Draw the resulting waveform if the sequence is transmitted using :

1. Unipolar RZ
2. Polar RZ
3. AMI
4. Split Phase Manchester
5. M-ary where M = 4. (Polar quaternary)

Soln. :

The required waveforms are as shown in Fig. P. 12.7.1.



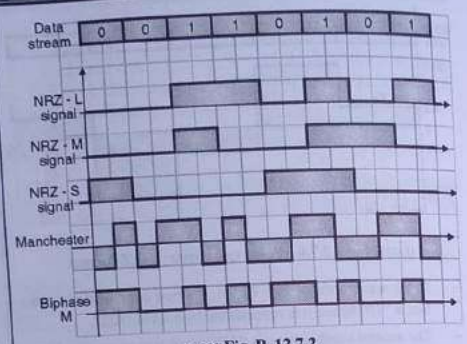
(L-279) **Fig. P. 12.7.1**

Ex. 12.7.2 : Sketch the signal waveforms when 0011 0101 is transmitted in the following signal codes :

1. NRZ-L
2. NRZ-M
3. NRZ-S
4. Manchester code
5. Biphase-M.

Soln. :

The required waveforms are as shown in Fig. P. 12.7.2.



(L-280) **Fig. P. 12.7.2**

Ex. 12.7.3 : How many amplitude levels are there for each of the following methods ?

1. NRZ-L
2. NRZ-S
3. Manchester
4. RZ
5. Differential Manchester
6. NRZ-M.

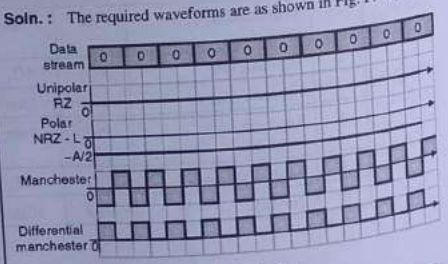
Soln. :

Name of the format	NRZ-L	NRZ-S	Manchester	RZ	NRZ-M
Number of amplitude levels	2	2	2	2	2

Ex. 12.7.4 : Assume a data stream is made of ten 0's. Encode this stream using the following schemes. How many changes can you find in each scheme ?

(a) Unipolar RZ (b) Polar NRZ-L
(c) RZ
(d) Manchester
(e) Differential Manchester

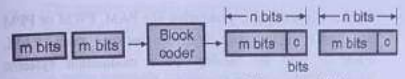
Soln. : The required waveforms are as shown in Fig. P. 12.7.4.



(L-281) **Fig. P. 12.7.4**

12.7.12 Block Coding :

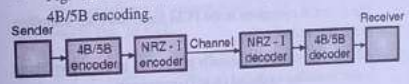
- In order to ensure better error performance and synchronization, it is necessary to introduce redundancy.
- Block coding is one of the ways to introduce redundancy and enhance the performance of line coding.
- In general block coding is a technique that changes a block of m bits into a block of n bits with n > m. Therefore block coding is referred to as mB/nB coding technique.
- The additional bits added to the original m bits are called as the parity bits or check bits.



m = message bits, c = parity bits or check bits

(L-282) **Fig. 12.7.9 : Concept of block coding**

- The examples of block codes are 4B/5B encoding in which a 4 bit code is converted into a 5 bit code or an 8B/10B code in which the 8 bit codes are converted into 10 bit codes.
- Fig. 12.7.10 shows the block diagram of a system using 4B/5B encoding.



(L-283) **Fig. 12.7.10 : 4B/5B system**

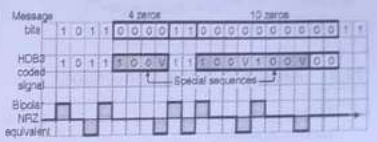
12.7.13 Scrambling :

- The Biphase schemes that are suitable for the dedicated links in a LAN prove to be unsuitable for long distance communication as they require large bandwidths.
- The combination of block coding and NRZ line coding also proves to be unsuitable due to the presence of DC component.
- The AMI scheme has smaller BW and no DC component but a long sequence of 0s can create problems for its synchronization.
- For long distance communication, a technique is needed to be found which has small BW, no DC component and no synchronization problems.
- One of the solutions is to use **scrambling**. We can modify AMI for scrambling. Two commonly used scrambling techniques are :

1. B8ZS 2. HDB3 encoding

1. High density bipolar (HDB) signalling :

- In case of the bipolar NRZ or AMI signal, the transmitted signal is equal to zero when a binary "0" is to be transmitted. This is true even for the unipolar RZ and unipolar NRZ signals.
- The absence of transmitted signal can cause problems in synchronization at the receiver, if long sequence of binary "0"s are being transmitted.
- This problem can be solved by adding (transmitting) pulses when long strings of 0's exceeding a number n are being transmitted. This type of coding is called High Density Bipolar coding. It is denoted by HDBN. Here N = 1, 2, 3 ..... The most widely used HDB format is with N = 3 i.e. HDB3.
- In the string of message bits when (N + 1) or more number of zeros occur, they are replaced by special binary sequences of (N + 1) length. As shown in Fig. 12.7.11, these sequences contain some binary 1's which are necessary for synchronization at the receiver.

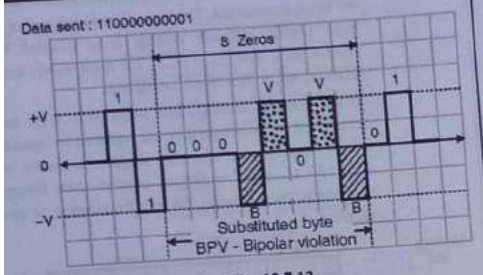


(L-284) **Fig. 12.7.11**

2. B8ZS line code :

- The long form of B8ZS is bipolar with 8-zero substitution.
- We have discussed about the line codes in this chapter. We know that in order to have synchronization between the transmitter and receiver, the line code needs to cross the zero line frequently.
- As per U.S. T1 standard, not more than 15 0's can be sent in succession to ensure proper synchronization.
- In order to solve the problems related to synchronization a new line code calledB8ZS (Binary 8-zeros suppression) was developed.
- Whenever eight successive 0's are detected, the implementation of this line code will automatically insert a special 8 bit sequence containing a bipolar violation.
- This can be easily detected and corrected by the CSU/DSU (channel service unit/digital service unit).
- Refer Fig. 12.7.12 to get a clear idea about the B8ZS line code.
- The violations (BPV in Fig. 12.7.12), will distinguish a byte substituted for all 0's from a normal byte which contains 1's.
- The B8ZS does not allow more than 8 - consecutive 0's and the bipolar violation pattern uniquely identifies the eight 0's.
- Note that the voltage levels in the "violating byte", has a zero average (dc) value.

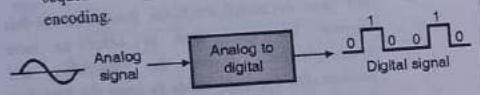
Scanned by CamScanner



(L-285) **Fig. 12.7.12**

12.8 Analog to Digital Conversion :

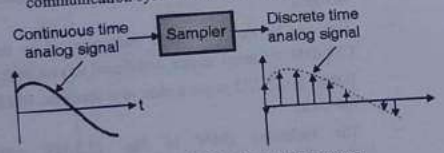
- The process of converting the analog data to digital signal is known as digitisation.
- This process is essential in all the digital communication systems such as Pulse Code Modulation (PCM) or Delta Modulation (D.M).
- In order to carry out this transformation, one has to follow a sequence of operations such as sampling, quantization and encoding.



(L-218) **Fig. 12.8.1 : Transformation from Analog signal to digital signal**

12.9 Sampling Process :

- In the pulse modulation and digital modulation systems, the signal to be transmitted must be in the discrete time form.
- If the message signal is coming from a digital source (e.g. a digital computer) then it is in the proper for a digital communication system to be processed.



(L-156) **Fig. 12.9.1 : Sampling process**

- But this is not always the case. The message signal can be analog in nature (e.g. speech or video signal).
- In such a case it has to be first converted into a discrete time signal. We use the "sampling process" to do this.
- Thus using the sampling process we convert a continuous time signal into a discrete time signal.
- For the sampling process to be of practical utility it is necessary to choose the sampling rate properly. The sampling process should satisfy the following requirements :

1. Sampled signal should represent the original signal faithfully.
2. We should be able to reconstruct the original signal from its sampled version.

- Fig. 12.9.1 summarizes the sampling process.

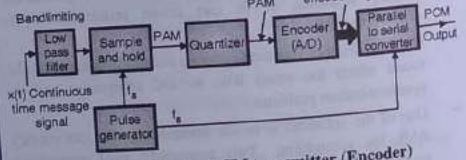
Thus sampling is the process of converting a continuous analog signal to a discrete analog signal and the sampled signal is the discrete time representation of the original analog signal.

12.10 Pulse Code Modulation (PCM) :

- PCM is a type of pulse modulation like PAM, PWM or PPM but there is an important difference between them. PAM, PWM or PPM are "analog" pulse modulation systems whereas PCM is a "digital" pulse modulation system.
- That means the PCM output is in the coded digital form. It is in the form of digital pulses of constant amplitude, width and position.
- The information is transmitted in the form of "code words". A PCM system consists of a PCM encoder (transmitter) and a PCM decoder (receiver).
- The essential operations in the PCM transmitter are sampling, quantizing and encoding.
- All these operations are usually performed in the same circuit called as analog-to-digital (A to D) converter.
- It should be understood that the PCM is not modulation in the conventional sense.
- Because in modulation, one of the characteristics of the carrier is varied in proportion with the amplitude of the modulating signal. Nothing of that sort happen in PCM.

12.10.1 PCM Transmitter (Encoder) :

- Block diagram of the PCM transmitter is as shown in Fig. 12.10.1.



(L-221) **Fig. 12.10.1 : PCM transmitter (Encoder)**

Operation of PCM transmitter :

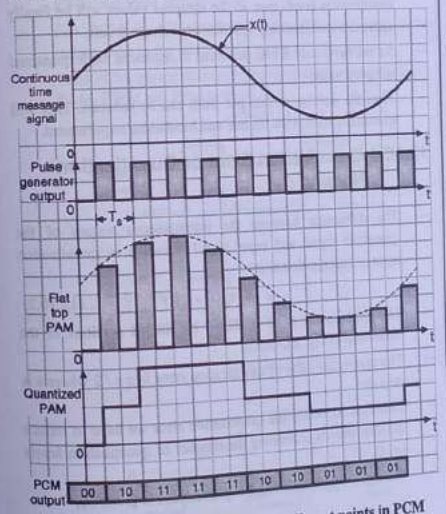
Operation of the PCM transmitter is as follows :

- The analog signal x (t) is passed through a bandlimiting low pass filter, which has a cut-off frequency f_c = W Hz. This will ensure that x (t) will not have any frequency component higher than "W". This will eliminate the possibility of aliasing.
- The band limited analog signal is then applied to a sample and hold circuit where it is sampled at adequately high sampling rate. Output of sample and hold block is a flat topped PAM signal.

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

Waveforms :

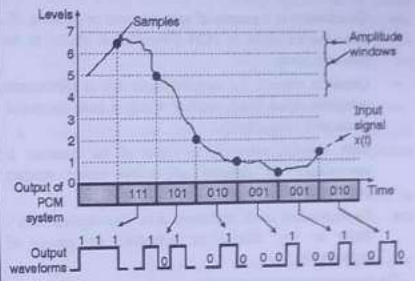
The waveforms at various points in the PCM transmitter are as shown in Fig. 12.10.2.



(L-222) **Fig. 12.10.2 : Waveforms at different points in PCM transmitter**

12.10.2 Shape of the PCM Signal :

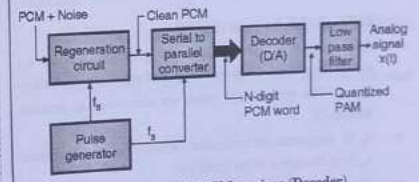
- Fig. 12.10.3 shows input to and output of a PCM system. It is important to understand that the output is in the form of binary codes. Each transmitted binary code represents a particular amplitude of the input signal. Hence the "information" is contained in the "code" which is being transmitted.
- The range of input signal magnitudes is divided into 8-equal levels. Each level is denoted by a three bit digital word between 000 and 111.
- Input signal x (t) is sampled. If the sample is in the 5th - window of amplitude then a digital word 101 is transmitted. If the sample is in the 2nd - window then the transmitted word is 010 and so on.
- In this example we have converted the amplitudes into 3 bit codes, but in practice the number of bits per word can be as high as 8, 9 or 10.



(L-223) **Fig. 12.10.3 : Input and output waveforms of a PCM system**

12.10.3 PCM Receiver (Decoder) :

- Fig. 12.10.4 shows the block diagram of a PCM receiver.



(L-224) **Fig. 12.10.4 : PCM receiver (Decoder)**

Operation of PCM receiver :

- A PCM signal contaminated with noise is available at the receiver input.
- The regeneration circuit at the receiver will separate the PCM pulses from noise and will reconstruct the original PCM signal.
- The pulse generator has to operate in synchronization with that at the transmitter. Thus at the regeneration circuit output we get a "clean" PCM signal.
- The reconstruction of PCM signal is possible due to the digital nature of PCM signal. The reconstructed PCM signal is then passed through a serial to parallel converter.

Scanned by CamScanner

- Output of this block is then applied to a decoder.
- The decoder is a D to A converter which performs exactly the opposite operation of the encoder.
- The decoder output is the sequence of a quantized multilevel pulses. The quantized PAM signal is thus obtained, at the output of the decoder.
- This quantized PAM signal is passed through a low pass filter to recover the analog signal, x (t).
- The low pass filter is called as the reconstruction filter and its cut off frequency is equal to the message bandwidth W.

12.10.4 Quantization Process :

- Quantization is a process of approximation or rounding off. The sampled signal in PCM transmitted is applied to the quantizer block.
- Quantizer converts the sampled signal into an approximate quantized signal which consists of only a finite number of predecided voltage levels.
- Each sampled value at the input of the quantizer is approximated or rounded off to the nearest standard predecided voltage level.
- These standard levels are known as the "quantization levels". Refer to Fig. 12.10.5 to understand the process of quantization.

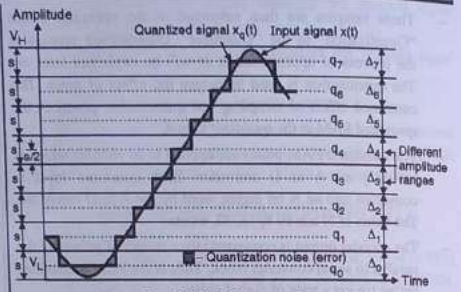
The quantization process takes place as follows :

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

$$s = \frac{V_H - V_L}{Q} \quad ...(12.10.1)$$

In Fig. 12.10.5, the value of Q = 8

- At the center of these ranges, the quantization levels q_0, q_1,...q_7 are placed. Thus the number of quantization levels is Q = 8. The quantization levels are also called as decision thresholds.
- x_q (t) represents the quantized version of x (t). We obtain x_q (t) at the output of the quantizer.
- When x (t) is in the range Δ_0, then corresponding to any value of x (t), the quantizer output will be equal to "q_0".
- Similarly for all the values of x (t) in the range Δ_1, the quantizer output is constant equal to "q_1".
- Thus in each range from Δ_0 to Δ_7, the signal x (t) is rounded off to the nearest quantization level and the quantized signal is produced.
- The quantized signal x_q (t) is thus an approximation of x (t). The difference between them is called as **quantization error or quantization noise.**
- This error should be as small as possible.
- To minimize the quantization error we need to reduce the step size "s" by increasing the number of quantization levels Q.



(L-225) **Fig. 12.10.5 : Process of quantization**

Why is quantization required ?

- If we do not use the quantizer block in the PCM transmitter, then we will have to convert each and every sampled value into a unique digital word.
- This will need a large number of bits per word (N). This will increase the bit rate and hence the bandwidth requirement of the channel.
- To avoid this, if we use a quantizer with only 256 quantization levels then all the sampled values will be finally approximated into only 256 distinct voltage levels.
- So we need only 8 bits per word to represent each quantized sampled value.
- Thus the number of bits per word can be reduced. This will eventually reduce the bit rate and bandwidth requirement.

12.10.5 Quantization Error or Quantization Noise ∈ :

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

$$\in = x_q(t) - x(t) \quad ...(12.10.2)$$

- The quantization error is shown by shaded portions of the waveform in Fig. 12.10.5.
- The maximum value of quantization error is ± s / 2 where s is step size.
- Therefore to reduce the quantization error we have to reduce the step size by increasing the number of quantization levels i.e. Q.
- The mean square value of the quantization is given by,

$$\text{Mean square value of quantization error} = \frac{s^2}{12} \quad ...(12.10.3)$$

- The relation between the number of quantization levels Q and the number of bits per word (N) in the transmitted signal can be found as follows :
  - Because each quantized level is to be converted into a unique N bit digital word, assuming a binary coded output signal,

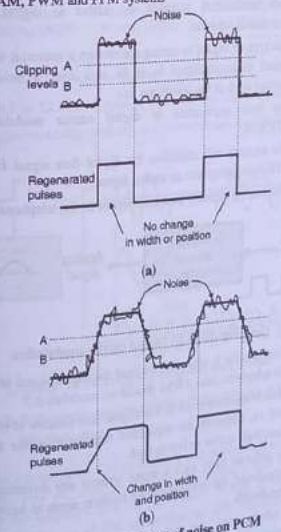
  - The number of quantization levels Q = Number of combinations of bits/word.

$$\therefore \quad Q = 2^N \quad ...(12.10.4)$$

  - Thus if N = 4 i.e. 4 bits per word then the number of quantization levels will be 2^4 i.e.16.

12.10.6 Effect of Noise on the PCM System :

- Look at the two Figs. 12.10.6(a) and 12.10.6(b) which illustrate the effect of noise on the transmitted pulses.
- Consider Fig. 12.10.6(a) first. Due to the noise superimposed on the pulses, only the PAM system will be affected.
- However the PWM, PPM and PCM systems will remain unaffected. The regeneration of the pulses is achieved by using a clipper circuit with reference levels A and B.
- Now consider Fig. 12.10.6(b). Here the sides of the transmitted pulse are not perfectly vertical. In practice the transmitted pulses usually have slightly sloping sides (edges).
- As the noise is superimposed on them, the width and the position of the regenerated pulses is changed.
- Now this is going to distort the information contents in the PWM and PPM signals.
- But PCM is still unaffected as it does not contain any information in the width or the position of the pulses.
- Thus PCM has much better noise immunity as compared to PAM, PWM and PPM systems



(L-229) **Fig. 12.10.6 : Effect of noise on PCM**

12.11 Advantages, Disadvantages Applications of PCM :

- The PCM is considered to be the best modulation scheme to transmit the voice and video signals.
- All the advantages of PCM are due to the fact that it uses coded pulses for the transmission of information.

12.11.1 Advantages of PCM :

1. Very high noise immunity (Noise does not affect the information content).
2. Due to digital nature of the signal, repeaters can be placed between the transmitter and the receivers. The repeaters actually regenerate the received PCM signal. This is not possible in analog systems. Repeaters further reduce the effect of noise.
3. It is possible to store the PCM signal due to its digital nature.
4. It is possible to use various coding techniques so that only the desired receiver can decode the received signal. This makes the communication secure.
5. The increased channel bandwidth requirement for PCM is balanced by the improved SNR. This is the due to the fact that PCM obeys an exponential law.
6. There is a **uniform format** used for the transmission of different types of base band signals. Hence it is easy to integrate all these signals together and send them on the common network.
7. It is easy to drop or reinsert the message sources in a PCM-TDM system.

12.11.2 Disadvantages of PCM :

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

12.11.3 Applications of PCM :

Some of the applications of PCM are as follows :

1. In telephony (with the advent of fibre optic cables).
2. In the space communication, space craft transmits signals to earth. Here the transmitted power is very low (10 to 15W) and the distances are huge (a few million km). Still due to the high noise immunity, only PCM systems can be used in such applications.

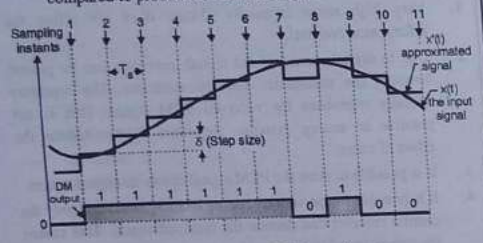
12.12 Linear Delta Modulation (D.M.) :

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

Scanned by CamScanner

Principle of operation :

- Delta modulation transmits only one bit per sample instead of N bits transmitted in PCM. This reduces its signaling rate and bandwidth requirement to a great extent.
- In the basic or linear D.M., a staircase approximated version of the sampled input signal is produced as shown in Fig. 12.12.1.
- The original signal and its staircase representation are then compared to produce a difference signal.



(L-235) **Fig. 12.12.1 : D.M. waveforms**

- And this difference signal is quantized into only two levels namely ± δ corresponding to positive and negative difference respectively.
- That means if the approximated signal x′ (t) lies below x (t) at the sampling instant, then the approximated signal is increased by "δ". (See instants 1, 2, 3, 4, 5 and 6 in Fig. 12.12.1.)
- Whereas if x′ (t) is greater than x (t) at the sampling instant, then x′ (t) is decreased by "δ" (see instants 7, 9 and 10 in Fig. 12.12.1.)

D.M. output :

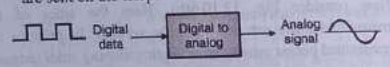
- As shown in Fig. 12.12.1, the D.M. output is 1 if the staircase signal x′ (t) is increased by "δ" i.e. at sampling instants 1, 2, 3, 4, 5 and 6.
- Whereas D.M. output is 0 if x′ (t) is decreased by "δ" i.e. at sampling instants 7, 9 and 10.
- In delta modulation, the present sample value x (t) is compared with the approximate value x′ (t) and the result of this comparison is transmitted.
- Thus we are sending the information of whether the present sample value is higher than or lower than the approximate value. Note that the actual sampled value is not being transmitted.

12.13 Analog Transmission :

- If we have low-pass channel, digital transmission is desirable and analog transmission is used when we have a bandpass channel.
- Conversion of digital data into a bandpass analog signal is known as **digital to analog conversion**.
- Analog-to-analog conversion is conversion of low pass analog signal to a bandpass analog signal.
- These two types of conversions are discussed in the following sections.

12.14 Digital to Analog Conversion :

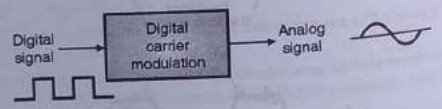
- In the process of D to A conversion the digital data at the input is converted into an analog signals. These analog signals are transmitted over the transmission medium.
- The most familiar application of D to A conversion is for transmitting digital data through the public telephone network.
- The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



(L-791) **Fig. 12.14.1 : Digital data to analog signal**

12.14.1 Need of Digital Continuous Wave Modulation :

- PCM converts analog message signal into a digital signal. Now we will learn some techniques which convert the digital message signal into an analog signal and then transmits it.
- Such modulation schemes are called as digital carrier modulation schemes.
- This type of digital to analog conversion is essential when the digital message signal is to be sent over a bandlimited channel such as the telephone line.
- The best application of digital carrier modulation is MODEM.
- The modem will modulate the digital data signal from the DTE (computer) into an analog signal.
- This analog signal is then transmitted on the telephone lines.



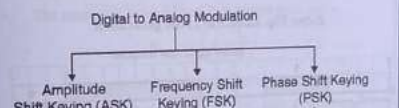
(L-61) **Fig. 12.14.2 : Digital carrier modulation**

- The question is why can't we send the digital signal as it is on the telephone lines ? Why should we modulate it ?
- Here is the answer for it. The digital data consists of binary 0s and 1s, therefore the waveform changes its value abruptly from high to low or low to high.
- In order to carry such a signal without any distortion being introduced, the communication medium needs to have a large bandwidth.
- Unfortunately the telephone lines do not have high bandwidth. Therefore we have to convert the digital signal

first into an analog signal which needs lower bandwidth by means of the modulation process.

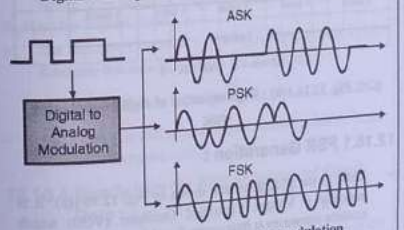
12.14.2 Types of Digital Carrier Modulation :

- There are three basic types of modulation techniques for the transmission of digital signals.
- These methods are based on the three characteristics of a sinusoidal signal; amplitude, frequency and phase. The corresponding modulation methods are then called as :
  1. Amplitude Shift Keying (ASK)
  2. Frequency Shift Keying (FSK)
  3. Phase Shift Keying (PSK)
  4. Quadrature Phase Shift Keying (QPSK) or 4-psk.
  5. Quadrature Amplitude Modulation (QAM).
- QPSK is a multilevel modulation in which four phase shifts are used for representing four different symbols.
- At high bit rates, a combination of ASK and PSK is employed in order to minimize the errors in the received data.
- This method is known as "Quadrature Amplitude Modulation (QAM)". Let us discuss these methods one by one.
- Fig. 12.14.3 shows the classification of digital to analog modulation systems.



(L-62) **Fig. 12.14.3 : Types of digital to analog modulation**

- Digital to analog modulation is demonstrated in Fig. 12.14.4.



(L-63) **Fig. 12.14.4 : Digital to analog modulation**

12.14.3 Advantages and Disadvantages of CW Modulation :

1. The advantage of CW modulation techniques such as ASK, PSK, FSK etc. used for transmission of data is that we can use the telephone lines for transmission of high speed data. Due to the use of CW modulation the BW requirement is reduced.
2. The disadvantage of CW modulation is we need to use a MODEM alongwith every computer. This makes the system costly and complex.

12.15 Amplitude Shift Keying (ASK) or Digital Amplitude Modulation :

Definition :

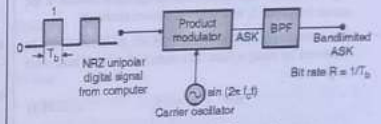
ASK is the digital carrier modulation in which the amplitude of the sinusoidal carrier will take one of the two predetermined values in response to 0 or 1 value of digital input signal.

Generation and waveforms :

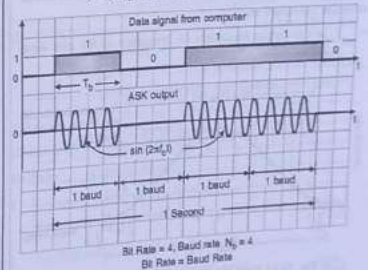
- Amplitude Shift Keying (ASK) is the simplest type of digital CW modulation. Here the carrier is a sinewave of frequency f_c. We can represent the carrier signal mathematically as follows :

$$e_c = \sin(2\pi f_c t) \quad ...(12.15.1)$$

- The digital signal from the computer is a unipolar NRZ signal which acts as the modulating signal. The ASK modulator is nothing but a multiplier followed by a band pass filter as shown in Fig. 12.15.1(a).
- Due to the multiplication, the ASK output will be present only when a binary "1" is to be transmitted.
- The ASK output corresponding to a binary "0" is zero as shown in Fig. 12.15.1(b).



(L-64) **Fig. 12.15.1(a) : ASK generator**



(L-65) **Fig. 12.15.1(b) : ASK waveforms**

- From the waveforms of Fig. 12.15.1(b) we can conclude that the carrier is transmitted when a binary 1 is to be sent and no carrier is transmitted when a binary 0 is to be sent.

Scanned by CamScanner

- The ASK signal can be mathematically expressed as follows :

$$V_{ASK}(t) = d \sin(2\pi f_c t) \quad ...(12.15.2)$$

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

$$\therefore V_{ASK}(t) = \sin(2\pi f_c t) \quad \text{when } d = 1$$
$$\text{and } V_{ASK}(t) = 0 \quad \text{when } d = 0 \quad ...(12.15.3)$$

12.15.1 Baud Rate (N_b) :

- For ASK we use 1 bit (0 or 1) to represent one symbol. So the rate of symbol transmission i.e. the baud rate will be same as the bit rate.
- N_b will be same as bit rate R as shown in Fig. 12.15.1(b).

$\therefore$ Baud rate = Bit rate

$$N_b = f_b$$

12.15.2 Transmission Bandwidth of the ASK Signal :

- The bandwidth of ASK signal is dependent on the bit rate f_b. Where bit rate $f_b = 1/T_b$ as shown in Fig. 12.15.1(a). For a bit rate of "f_b" bits/sec. the maximum bandwidth required for an ASK signal is

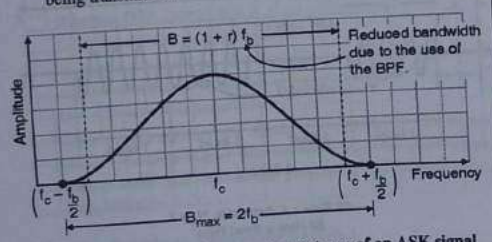
$$BW_{(max)} = f_b \text{ Hz} \quad ...(12.15.4)$$

- The frequency spectrum of an ASK signal is shown in Fig. 12.15.1(c) which shows that the spectrum consists of the carrier frequency f_c with upper and lower sidebands.
- The transmission bandwidth BW of the ASK signal can be restricted by using a filter. The restricted value of bandwidth is given as :

$$BW = (1 + r) f_b \quad ...(12.15.5)$$

where "r" is a factor related to the filter characteristics and its value lies between 0 and 1.

- f_c is the carrier frequency i.e. frequency of the sine wave being transmitted.



(L-66) **Fig. 12.15.1(c) : Frequency spectrum of an ASK signal**

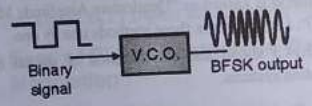
12.15.3 Multilevel ASK :

- In the above discussion, there were only two amplitude levels of the input digital data involved. But we can have multilevel ASK in which the digital data can have multiple amplitude levels (e.g. 4, 8, 16 levels etc.). This is possible if we consider a group of consecutive data bits as one symbol.
- 4 levels correspond to 2 bits at a time. Similarly 8 and 16 levels correspond to 3 and 4 bits at a time. Thus multiple bits/symbol would result in multilevel ASK.
- This principle is actually not implemented with pure ASK but it is implemented with QAM.

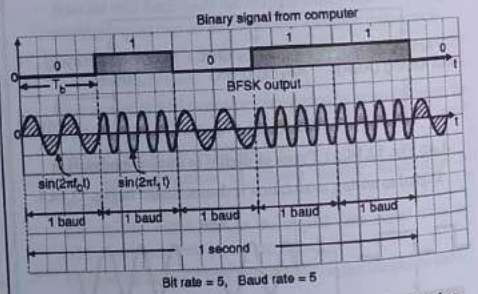
12.16 Frequency Shift Keying (FSK) :

Definition and waveforms :

- In "Frequency Shift Keying (FSK)", the frequency of a sinusoidal carrier is shifted between two discrete values, in response to the value (0 or 1) of the digital input signal.
- One of these frequencies (f_1) represents a binary "1" and the other value (f_0) represents a binary "0".
- The representation of digital data using FSK is as shown in Fig. 12.16.1(b). Note that there is no change in the amplitude of the carrier.



(L-785) **Fig. 12.16.1(a) : FSK generation**



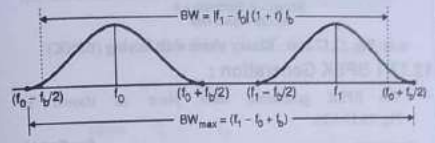
(L-72) **Fig. 12.16.1(b) : Representation of digital signal using FSK**

12.16.1 FSK Generation :

- Refer to the FSK generator shown in Fig. 12.16.1(a). It is basically a Voltage Controlled Oscillator (VCO) which produce sinewaves at frequencies f_1 and f_0, respectively.
- Corresponding to binary 0 input, the VCO produces a sinewave of frequency f_0 whereas corresponding to binary 1 input, the VCO produces a sinewave of frequency f_1. ($f_1 > f_0$).
- Thus we obtain the Binary FSK (BFSK) signal at the output of VCO corresponding to the input digital data bits.

12.16.2 Frequency Spectrum of Binary FSK Signal :

- The FSK signal can be considered to be containing two ASK signals, with the carrier frequencies f_1 and f_0.
- Therefore the frequency spectrum of the FSK signal is as shown in Fig. 12.16.1(c) which is identical to that of ASK for each of the two frequencies.



(L-73(b)) **Fig. 12.16.1(c) : Frequency spectrum of a binary FSK signal**

12.16.3 Bandwidth of FSK Signal :

- The bandwidth of FSK signal is dependent on the pulse width T_b or bit rate $f_b = 1/T_b$ and the separation between the frequencies f_0 and f_1, as shown in Fig. 12.16.1(c).
- The maximum bandwidth of FSK system is given by,

$$B_{max} = \left(f_1 + \frac{f_b}{2}\right) - \left(f_0 - \frac{f_b}{2}\right)$$
$$= (f_1 - f_0 + f_b) \quad ...(12.16.1)$$

- The bandwidth can be restricted by using a bandpass filter after the VCO in the FSK generator. The restricted bandwidth is given as :

$$B = |f_1 - f_0| + (1 + r)\frac{f_b}{2} \quad ...(12.16.2)$$

Where "r" is the factor related to the filter characteristics and its value lies between 0 and 1.

- The separation between f_1 and f_0 is kept at least $2 f_b/3$. Substitute this value in Equation (12.16.2) to get

$$B_{max} = \frac{2}{3} f_b + f_b = \frac{5 f_b}{3} \quad ...(12.16.3)$$

- This shows that FSK requires larger bandwidth than ASK and PSK (to be discussed next).

12.16.4 Bandwidth for FSK in terms of Baud Rate :

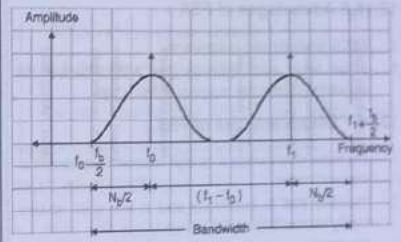
- For FSK also bit rate is equal to baud rate. This is due to the fact that each data bit at the input is treated as a separate symbol.
- We can imagine the FSK spectrum to be a combination of two ASK spectrums centered at frequencies f_1 and f_0 as shown in Fig. 12.16.1(d).
- From Fig. 12.16.1(d) the expression for bandwidth is given by

$$BW = \frac{N_b}{2} + (f_1 - f_0) + \frac{N_b}{2}$$
$$= (f_1 - f_0) + N_b \quad ...(12.16.4)$$

Where N_b = Baud rate = Bit rate = f_b

- Minimum bandwidth will correspond to the situation in which $(f_1 - f_0) = N_b$

$$\therefore BW_{(min)} = N_b + N_b = 2 N_b = 2 f_b \quad ...(12.16.5)$$



(L-74) **Fig. 12.16.1(d) : Spectrum of FSK**

Ex. 12.16.1 : Calculate the bandwidth of an FSK system in which, the transmission takes place at 4000 bits per second rate and the frequency difference between the two carriers is 3000 Hz.

Soln. :

Given : $(f_1 - f_0) = 3000$ Hz, Bit rate = 4000 bps.

To find : Bandwidth

- Bandwidth = $(f_1 - f_0) + N_b$
- But N_b = baud rate = bit rate = 4000

$\therefore$ BW = 3000 + 4000 = 7000 Hz ...Ans.

Ex. 12.16.2 : For a half duplex FSK transmission, the bandwidth of medium is 8000 Hz. If the frequency difference between the two carriers is 4000 Hz calculate the maximum bit rate.

Soln. :

Given : FSK, half duplex, BW = 8000 Hz, $f_1 - f_0 = 4000$ Hz

To find : Maximum bit rate

1. $BW = (f_1 - f_0) + N_b$

$\therefore 8000 = 4000 + N_b \quad \therefore N_b = 4000$ bands/sec.

2. For FSK system baud rate is equal to bit rate.

$\therefore$ Bit rate = 4000 bits per second ...Ans.

12.16.5 Multilevel FSK (MFSK) :

- In BFSK (Binary FSK) we use two frequencies to represent two levels of signal amplitude (0 or 1). But if there are multiple levels of signal amplitude, then it is possible to use more frequencies to represent them.

Scanned by CamScanner

- As discussed in multilevel ASK, even here we use multiple data bits to represent one symbol.
- If 2 bits are used at a time then there will be $2^2 = 4$ levels. So we have to assign four different frequencies (f_0, f_1, f_2, f_3) to represent these levels.
- The bandwidth requirement of MFSK is higher than that of BFSK.

12.16.6 Advantages of FSK :

1. FSK is relatively easy to implement.
2. It has better noise immunity than ASK. Therefore the probability of error free reception of data is high.

12.16.7 Disadvantages of FSK :

1. The major disadvantage is its high bandwidth requirement as discussed earlier.
2. Therefore FSK is extensively used in low speed modems having bit rates below 1200 bits/sec.
3. The FSK is not preferred for the high speed modems because with increase in speed, the bit rate increases.
4. This increases the channel bandwidth required to transmit the FSK signal.
5. As the telephone lines have a very low bandwidth, it is not possible to satisfy the bandwidth requirement of FSK at higher speed. Therefore FSK is preferred only for the low speed modems.

12.17 Phase Shift Keying (PSK) :

Definition and waveforms :

- Phase Shift Keying (PSK) is the most efficient of the three modulation methods.
- Therefore it is used for high bit rates. In PSK, phase of the sinusoidal carrier is changed according to the data bit to be transmitted.
- Fig. 12.17.1(a) shows the simplest form of PSK called Binary PSK (BPSK). The carrier phase is changed between 0° and 180° by the bipolar digital signal. A bipolar NRZ signal is used to represent the digital data from the DTE.
- The BPSK signal can be represented mathematically as :

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

when binary "0" is to be represented

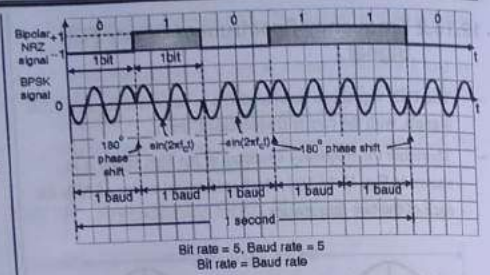
$$\text{and } V_{BPSK}(t) = -\sin(2\pi f_c t) = \sin(2\pi f_c t + \pi)$$

when binary "1" is to be represented.

- Combining the two conditions we can write

$$V_{BPSK}(t) = d \sin(2\pi f_c t) \quad \text{...(12.17.1)}$$

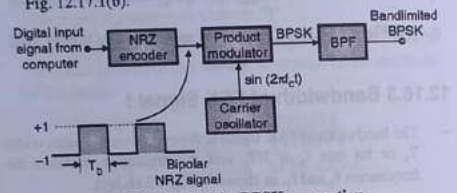
where $d = \pm 1$



(L-80) **Fig. 12.17.1(a) : Binary phase shift keying (BPSK)**

12.17.1 BPSK Generation :

- The BPSK generation takes place as shown in Fig. 12.17.1(b).



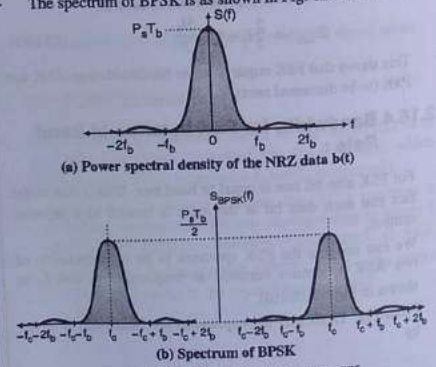
(L-81) **Fig. 12.17.1(b) : BPSK generation**

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

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

12.17.2 Spectrum of BPSK :

- The spectrum of BPSK is as shown in Fig. 12.17.2.



(a) Power spectral density of the NRZ data b(t)

(b) Spectrum of BPSK

(L-88) **Fig. 12.17.2 : Spectrum of BPSK**

12.17.3 Bandwidth of BPSK :

- From the frequency spectrum of BPSK signal, shown in Fig. 12.17.2(b), we can come to a conclusion that the bandwidth of a BPSK signal is given by,

$$BW = \text{Highest frequency} - \text{Lowest frequency in main lobe}$$

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

$$\therefore \quad BW = 2 f_b \quad \text{...(12.17.2)}$$

where $f_b = 1/T_b$

- Thus the minimum bandwidth of BPSK signal is equal to twice the highest frequency contained in the baseband signal.

Baud rate :

In BPSK also each digit (0 or 1) of the input digital data represents a symbol. Hence symbol rate is equal to bit rate.

$$\therefore \quad \text{Baud rate } N_b = \text{Bit rate } f_b$$

$$\therefore \quad BW = 2 N_b$$

12.17.4 Advantages of BPSK :

1. BPSK has a bandwidth which is lower than that of a BPSK signal.
2. BPSK has the best performance of all the systems in presence of noise. It gives the minimum possibility of error.
3. BPSK has a very good noise immunity.

12.17.5 Disadvantage of BPSK :

The only disadvantage of BPSK is that generation and detection of BPSK is not easy. It is quite complicated.

12.17.6 Applications :

- Phase shift keying is the most efficient of the three modulation methods and it is used for high bit rates even higher than 1800 bits/sec.
- Due to low bandwidth requirement the BPSK modems are preferred over the FSK modems, at higher operating speeds.

12.17.7 Comparison of Binary Modulation Systems :

Sr. No.	Parameter	Binary ASK	Binary FSK	Binary PSK
1.	Variable characteristic.	Amplitude	Frequency	Phase
2.	Bandwidth (Hz)	2R	$\lvert f_1 - f_0 \rvert + (1+r) R$	$(1+r) R$
3.	Noise immunity.	low	high	high
4.	Error probability	high	low	low
5.	Performance in presence of noise.	Poor	Better than ASK	Better than FSK
6.	Complexity	Simple	Moderately complex	Very complex
7.	Bit rate	Suitable upto 100 bits/sec.	Suitable upto about 1200 bits/sec.	Suitable for high bit rates.
8.	Detection method.	Envelope	Envelope	Coherent

Scanned by CamScanner

Ex. 12.17.1 : If the data bit sequence consists of the following string of bits, what will be the nature of waveform transmitted by BPSK transmitter ?

The data bit sequence is 1 0 1 1 1 0 1 0.

Soln. :

The BPSK signal can also be expressed in terms of cosine wave as :

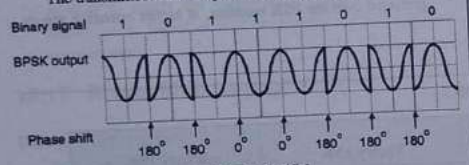
$$V_{BPSK}(t) = \sqrt{2P_s}\, b(t) \cos \omega_c t$$

where b (t) = ± 1 depending on the digital input signal. Table P. 12.17.1 lists the values of b (t) and the transmitted signal V_{BPSK} for different bit intervals.

Table P. 12.17.1

Binary signal	1	0	1	1	1	0	1	0
b (t)	+1	−1	+1	+1	+1	−1	+1	−1
$V_{BPSK}(t)$	cos $\omega_c t$	− cos $\omega_c t$	cos $\omega_c t$	− cos $\omega_c t$	cos $\omega_c t$	− cos $\omega_c t$	cos $\omega_c t$	− cos $\omega_c t$

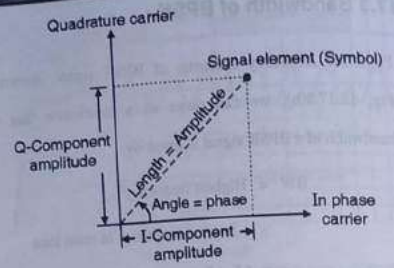
The transmitted BPSK signal is as shown in Fig. P. 12.17.1.



(L-89) **Fig. P. 12.17.1**

12.18 Constellation Diagram :

- A constellation diagram is a diagram which can help us to define the amplitude and phase of each symbol or signal element in a given system (ASK, FSK, PSK, ... etc.). This is particularly helpful when we are using two carriers (one in phase and the other in quadrature) or when we are studying the multilevel ASK, PSK or QAM.
- In this diagram each signal element (i.e. symbol) is represented by a dot as shown in Fig. 12.18.1. This diagram has two axes i.e. it is a two dimensional graphical representation of a symbol.
- On the X-axis we plot the in phase carrier while on the Y-axis we plot the quadrature (90° phase shifted) carrier. The concept of constellation diagram has been illustrated in Fig. 12.18.1.

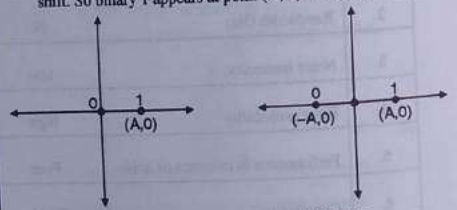


(L-786) **Fig. 12.18.1 : Concept of constellation diagram**

- Each point on the constellation diagram gives us the following information :
  1. Projection of the symbol point on X-axis gives amplitude of I (in phase) component.
  2. Projection of the symbol point on Y-axis gives amplitude of Q (Quadrature) component.
  3. The line that joins the origin and the signal element is called as signal vector.
  4. The length of the signal vector represents its peak amplitude.
  5. The angle made the signal vector with X-axis represents the phase angle of the signal element.

12.18.1 Constellation Diagram of ASK :

- Fig. 12.18.2(a) shows the constellation diagram of ASK. For ASK only one in-phase carrier is used. Hence both the signal points appear on the X-axis.
- There are two symbols (signal elements) in ASK namely 0 and 1.
- The amplitude of binary 0 is zero so it is located at the origin. The amplitude of binary 1 is say A volts and has zero phase shift. So binary 1 appears at point (A, 0) in Fig. 12.18.2(a).



(a) ASK (b) BPSK

(L-787) **Fig. 12.18.2 : Constellation diagrams of ASK and BPSK**

12.18.2 Constellation Diagram of BPSK :

- Fig. 12.18.2(b) shows the constellation diagram of Binary PSK (BPSK).
- BPSK also uses only one in phase carrier. The two symbols in the BPSK system are represented as follows :

Binary 1 : Amplitude A, phase 0

Binary 0 : Amplitude A, phase 180°

- Hence these two signal points are located at points (A, 0) and (– A, 0) respectively as shown in Fig. 12.18.2(b).
- Thus BPSK created two signal elements. One with amplitude A and in phase and the other with amplitude A and out of phase.

12.19 Quadrature Amplitude Shift Keying (QASK) or QAM :

- In all the PSK methods discussed till now, one symbol is distinguished from the other in phase, but all the symbols transmitted using BPSK, QPSK or M-ary PSK are of "same amplitude".
- The ability of a receiver to distinguish between one signal vector from another in presence of noise, depends on the distance between the vector end points.
- This suggests that the noise immunity will improve if the signal vectors differ not only in phase, but also in amplitude.
- Such a system is called as amplitude and phase shift keying system.
- In this system the direct modulation of carriers in quadrature (i.e. cos $\omega_c t$ and sin $\omega_c t$) is involved, therefore this system is called as the quadrature amplitude phase shift keying i.e. QAPSK or simply QASK.
- It is also known as Quadrature Amplitude Modulation (QAM).

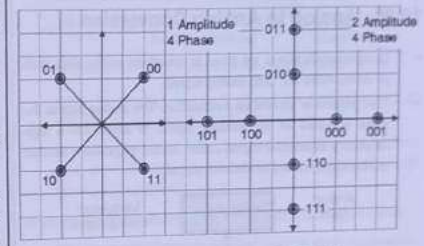
12.19.1 Types of QAM :

Depending on the number of bits per message the QAM signals are classified as follows :

Name	Bits per symbol	Number of symbols
4 QAM	2	$2^2 = 4$
8 QAM	3	$2^3 = 8$
16 QAM	4	$2^4 = 16$
32 QAM	5	$2^5 = 32$
64 QAM	6	$2^6 = 64$

12.19.2 4 QAM and 8 QAM Systems :

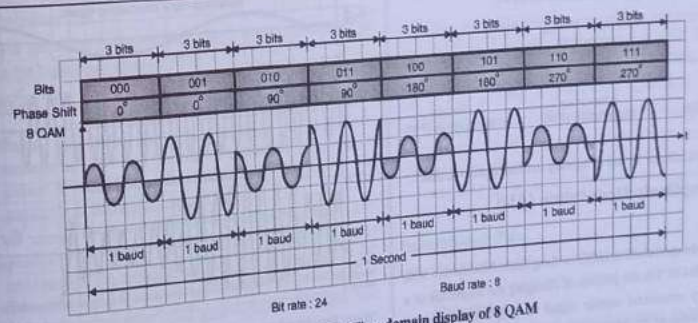
- The constellation of 4 QAM system is shown in Fig. 12.19.1(a). All the symbols have same amplitude but different phases.



(a) 4 QAM (b) 8 QAM

(L-103) **Fig. 12.19.1 : Constellation diagrams**

- Fig. 12.19.1(b) shows the constellation diagram of 8-QAM. Note that there are two amplitude levels and four phases involved.
- The time domain display of 8 QAM is shown in Fig. 12.19.2.



(L-104) **Fig. 12.19.2 : Time domain display of 8 QAM**

Scanned by CamScanner

12.19.3 Comparison of QASK and QPSK :

Table 12.19.1

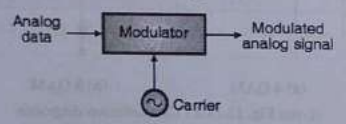
Sr. No.	Parameter	QPSK	QAM
1.	Type of modulation	Quadrature phase modulation	Quadrature amplitude and phase modulation
2.	Location of signal points	On the circumference of a circle	Equally spaced and placed symmetrically about origin
3.	Distance between the signal points	$d = 2\sqrt{E_b}$ for N = 2	$d = 2\sqrt{0.4\,E_b}$ for N = 4 or M = 16
4.	Noise immunity	Better than QASK	Poorer than QPSK
5.	Probability of error	Less than QASK	More than QPSK
6.	Type of demodulation	Synchronous	Synchronous
7.	System complexity	Less complex than QASK	More complex than QPSK

12.19.4 Bandwidth of QAM :

The minimum bandwidth required for QAM transmission is same as that for ASK or PSK.

12.20 Analog to Analog Conversion :

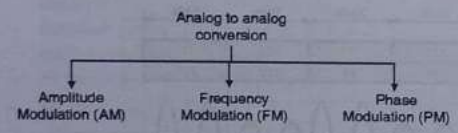
- In some applications we have to transform analog data such as voice, video etc. into analog signal.
- This process is known as modulation. The analog data at the input is called as modulating signal. It modulates a high frequency sinusoidal signal called carrier to produce another analog signal called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



(L-31) **Fig. 12.20.1 : Transformation from analog data to analog signals**

12.20.1 Types of Analog to Analog Conversion :

The three basic types of analog to analog conversion are shown in Fig. 12.20.2. They are AM, FM and PM.



(L-780) **Fig. 12.20.2 : Types of analog to analog conversion**

12.20.2 Amplitude Modulation (AM) :

Definition :

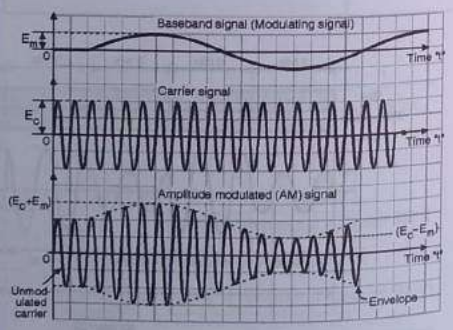
Amplitude modulation (AM) or Amplitude Modulation with Full Carrier (AM-FC) is the process of changing the amplitude of a high frequency sinusoidal carrier signal in proportion with the instantaneous value of modulating signal.

Fig. 12.20.3 shows the amplitude modulated wave when the modulating signal is a sinusoidal signal.

Observations :

1. The frequency of the sinusoidal carrier is much higher than that of the modulating signal.
2. In AM the instantaneous amplitude of the sinusoidal high frequency carrier is changed in proportion to the instantaneous amplitude of the modulating signal. This is the principle of AM.
3. The time domain display of AM signal is as shown in Fig. 12.20.3. This AM signal is transmitted by a transmitter. The information in the AM signal is contained in the amplitude variations of the carrier of the envelope shown by dotted lines in Fig. 12.20.3.
4. Note that the frequency and phase of the carrier remain constant.
5. AM is used in the applications such as radio transmission, TV transmission etc.

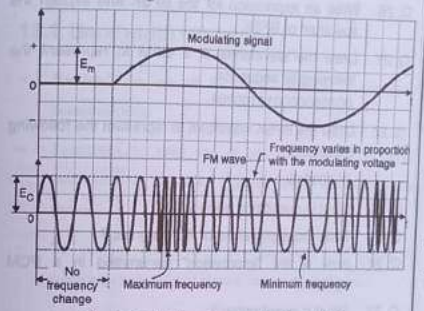
Note : The modulating signal in practice may or may not be purely sinusoidal. Most of the times it will have a complex shape.



(D-12) **Fig. 12.20.3 : AM waveform for sinusoidal modulating signal**

12.20.3 Frequency Modulation (FM) :

- In sinusoidal Frequency Modulation (FM), the modulating signal $x(t) = E_m \cos(2\pi f_m t)$ is a pure sinusoidal signal. The carrier signal c (t) is also a sinewave at much higher frequency.
- FM is a system of modulation in which the instantaneous frequency of the carrier is varied in proportion with the amplitude of the modulating signal. The amplitude of the carrier signal remain constant. Thus the information is conveyed via frequency changes.
- FM was first practically tried in 1936 as an alternative to AM. As will be shown later on, FM transmission is more resistant to noise than A.M. The time domain display of FM wave is as shown in the Fig. 12.20.4.

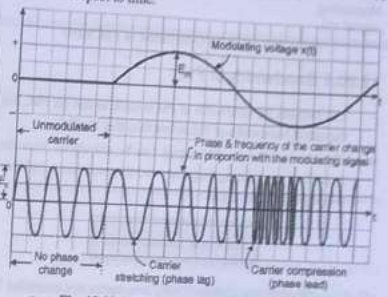


(B-709) **Fig. 12.20.4 : Time domain display of FM wave**

- The amount by which the carrier frequency deviates from its unmodulated value is called as "**deviation**". The deviation (δ) is made proportional to the instantaneous value of modulating voltage.
- The rate at which these frequency variations or oscillations takes place in the FM wave is equal to the modulating frequency (f_m).
- The amplitude of the FM wave always remains constant. This is the biggest advantage of FM.

12.20.4 Phase Modulation (PM) :

- Phase modulation is very similar to the frequency modulation. The only difference is that the phase of the carrier is varied instead of varying the frequency. The amplitude of the carrier remains constant.
- As shown in Fig. 12.20.5, as the modulating signal goes positive, the amount of phase lag increases with the amplitude of the modulating signal. The effect of this is that the carrier signal is stretched or its frequency is reduced.
- When the modulating signal goes negative, the phase shift becomes leading. This causes the carrier wave to be effectively compressed. The effect of this is as if the carrier frequency is increased.
- Thus phase modulation is always associated with frequency modulation and vice versa.
- Note that the P.M. wave of Fig. 12.20.5 is the same as the F.M. wave produced by dx(t) / dt i.e. the derivative of x (t) with respect to time.



(L-45) **Fig. 12.20.5 : Time domain display of PM wave**

- So in Fig. 12.20.5 we have plotted the derivative of x (t) which is original x (t) shifted by 90°.
- From the discussion it is clear that the difference between F.M. and P.M. waves can be made only by comparing with the original modulating wave.

Mathematical representation of Phase Modulation (PM) :

- The phase modulation is another type of angle modulation. PM and FM are closely related. It is possible to obtain FM from PM, using the method called "Armstrong method".
- The PM wave is obtained by varying the phase angle ϕ of a carrier in proportion with the amplitude of the modulating voltage.

  If the carrier voltage is expressed as,

$$e_c = A \sin(\omega_c t + \phi) \quad \text{...(12.20.1)}$$

- Then the PM wave can be expressed as,

$$e_{PM} = A \sin(\omega_c t + \phi_m \sin \omega_m t) \quad \text{...(12.20.2)}$$

- Here ϕ_m = Maximum phase change corresponding to the maximum amplitude of the modulating signal. For the sake of uniformity let us modify the Equation (12.20.2) as,

$$e_{PM} = A \sin[\omega_c t + m_p \sin \omega_m t] \quad \text{...(12.20.3)}$$

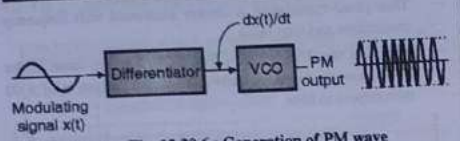
  Where $m_p = \phi_m$ = Modulation index of PM.

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

Generation of PM :

- Fig. 12.20.6 shows the scheme for the generation of PM wave. The modulating signal x (t) is applied to a differentiator.
- Then the differentiated modulating signal dx (t)/dt is applied to the VCO to produce the PM wave.

Scanned by CamScanner



(L-784) **Fig. 12.20.6 : Generation of PM wave**

12.20.5 Bandwidth of PM :

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

Review Questions

Q. 1 What is line coding ? Why line codes are essential ?

Q. 2 What are the disadvantages of RZ codes ?

Q. 3 State the various requirements of a line code.

Q. 4 Write a short note on : Manchester coding.

Q. 5 Represent ASK mathematically.

Q. 6 State the bandwidth requirement of ASK system.

Q. 7 What is the maximum B.W. of BPSK system ?

Q. 8 Draw the BPSK signal for the following binary signal.
10111010

Q. 9 Express QPSK mathematically.

Q. 10 How many phases are transmitted in QPSK ?

Q. 11 What are the advantages of QPSK system ?

Q. 12 What is the type of demodulation used for QPSK ?

Q. 13 State the expression for BFSK.

Q. 14 How is a message transmitted in BFSK ?

Q. 15 What is the BW of BFSK ?

Q. 16 What is QAM ?

Q. 17 What is the BW requirement of QAM ?

Q. 18 Why is QPSK superior to BPSK ?

Q. 19 State merits and demerits of BASK.

Q. 20 What type of receiver is used for the BPSK detection ?

Q. 21 Compare ASK and FSK.

Q. 22 Draw the waveforms for FSK and PSK modulation.

Q. 23 Explain the QPSK modulation scheme with constellation diagram.

Q. 24 What is ASK ? Draw its waveform ?

Q. 25 Draw the block diagram of binary PSK system and explain with signal space diagram.

Q. 26 Write an expression for the BFSK and explain the spectrum of BFSK.

Q. 27 Draw the waveforms of 8 QAM to represent the following bit sequence
001010000011100101

Q. 28 Draw the BFSK waveform to represent the following bit stream.
00101110.

Q. 29 What is quantizing noise ?

Q. 30 State the applications of PCM signals ?

Q. 31 How is the "information" transmitted in a PCM system ?

Q. 32 What is quantization ?

Q. 33 What is quantization error ? What is its maximum value ?

Q. 34 How to reduce the quantization error ?

Q. 35 Draw and explain the block diagram for generation of PCM signal.

Q. 36 Explain the delta modulation system.

Q. 37 What are the advantages of DM ?

Q. 38 What are the disadvantages of DM ?

□□□

CHAPTER 13

Module VI

Bandwidth Utilization

Syllabus :
Bandwidth utilization, Multiplexing, Spread spectrum.

13.1 Bandwidth Utilization :

- Bandwidth is one of the main challenge of electronic communication.
- Sometimes to make use of one channel with a larger bandwidth we need to combine many low bandwidth channels
- To achieve goals such as antijamming and privacy, sometimes expansion of channel bandwidth is needed.
- In this chapter we will discuss following broad categories of bandwidth utilization :
  1. Multiplexing.
  2. Spread spectrum.
- The main goal of multiplexing is **efficiency**. In multiplexing many channels are combined into one.
- Frequency division multiplexing (FDM) allows to combine several analog signals into a single analog signal.
- Wavelength division multiplexing (WDM) allows to combine many optical signals into single optical signal.
- To share a channel in time time-division multiplexing allows several digital signals.
- **Privacy and antijamming** is main goal of spread spectrum. To achieve these goals we expand the channel bandwidth to add redundancy.
- In spread spectrum, before combining various channels we have to first spread signal bandwidth to add redundancy for more secure transmission.
- In FHSS (Frequency hopping spread spectrum), in different period of time, different modulation frequencies are used.
- In DSSS (Direct sequence spread spectrum), before transmission a signal bit in the original signal is changed to a sequence.

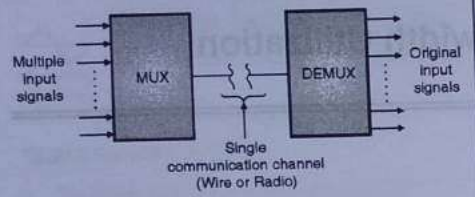
13.2 Introduction to Multiplexing :

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

13.3 Concept of Multiplexing and Demultiplexing :

- The concept of a simple multiplexer is illustrated in Fig. 13.3.1.
- The multiplexer receives a large number of different input signals.
- Multiplexer has only one output which is connected to the single communication channel.
- The multiplexer combines all input signals into a single composite signal and transmits it over the communication medium.

Scanned by CamScanner



(L-105) **Fig. 13.3.1 : Concept of multiplexing**

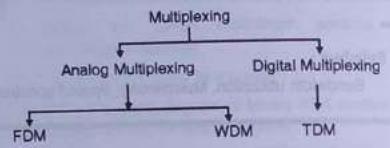
- Sometimes the composite signal is used for modulating a carrier before transmission.
- At the receiving end, of communication link, a demultiplexer is used to separate out the signals into their original form.
- The operation of demultiplexer is exactly opposite to that of a multiplexer. Demultiplexing is the process which is exactly opposite to that of multiplexing.

13.3.1 Types of Multiplexing :

- There are three basic types of multiplexing. They are :

1. Frequency Division Multiplexing (FDM).
2. Time Division Multiplexing (TDM).
3. Wavelength Division Multiplexing (WDM).

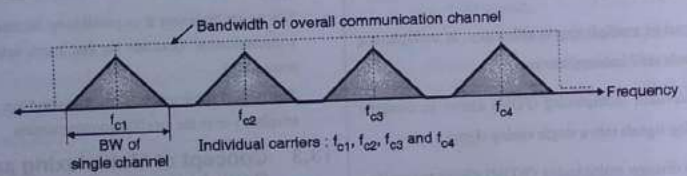
- The multiplexing techniques can be broadly classified into two categories namely analog and digital.
- Analog multiplexing can be either FDM or WDM and digital multiplexing is TDM.
- Fig. 13.3.2 shows the classification of multiplexing techniques.
- Generally the FDM and WDM systems are used to deal with the analog information whereas the TDM systems are used to handle the digital information.
- In FDM many signals are transmitted simultaneously where each signal occupies a different frequency slot within a common bandwidth.
- In TDM the signals are not transmitted at a time, instead they are transmitted in different time slots.



(L-106) **Fig. 13.3.2 : Classification of multiplexing techniques**

13.4 Frequency Division Multiplexing (FDM) :

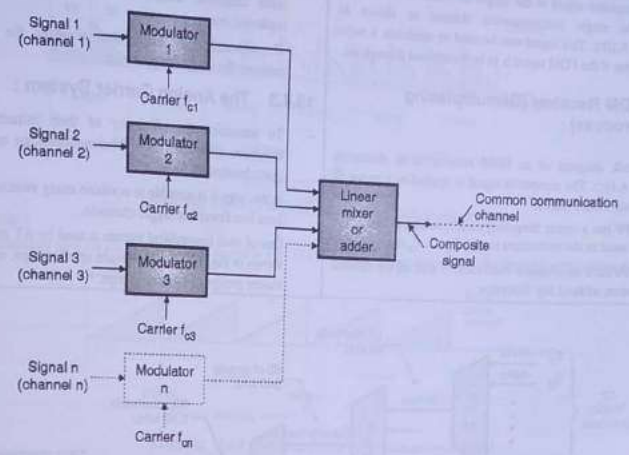
- The operation of FDM is based on sharing the available bandwidth of a communication channel among the signals to be transmitted.
- That means many signals are transmitted simultaneously with each signal occupying a different frequency slot within the total available bandwidth.
- Each signal to be transmitted modulates a different carrier. The modulation can be AM, SSB, FM or PM.
- The modulated signals are then added together to form a composite signal which is transmitted over a single channel.
- The spectrum of composite FDM signal is shown in Fig. 13.4.1(a).
- Generally the FDM systems are used for multiplexing the analog signals.



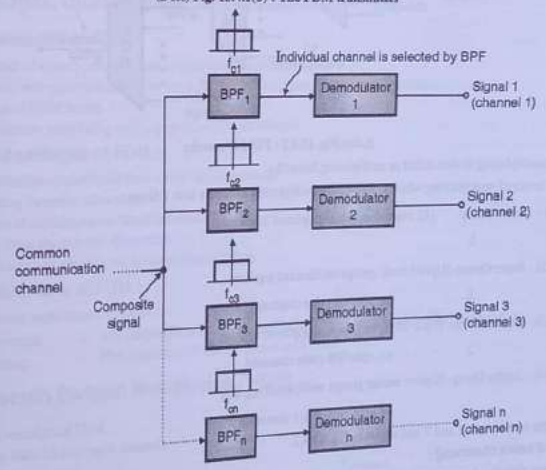
(L-107) **Fig. 13.4.1(a) : Spectrum of FDM signal**

13.4.1 FDM Transmitter (Multiplexing Process) :

- Fig. 13.4.1(b) shows the block diagram of an FDM transmitter. The signals which are to be multiplexed will each modulate a separate carrier.
- The type of modulation can be AM, SSB, FM or PM.
- The modulated signals are then added together to form a complex signal which is transmitted over a single channel.



(L-108) **Fig. 13.4.1(b) : The FDM transmitter**



(L-109) **Fig. 13.4.1(c) : FDM receiver**

Operation of the FDM transmitter :

- Each signal modulates a separate carrier. The modulator outputs will contain the sidebands of the corresponding signals.
- The modulator outputs are added together in a linear mixer or adder.
- The linear mixer is different from the normal mixers. Here the sum and difference frequency components are not produced. But only the algebraic addition of the modulated outputs will take place.
- Different signals are thus added together in the time domain but they have their own separate identity in the frequency domain. This is as shown in the Fig. 13.4.1(a).

Scanned by CamScanner

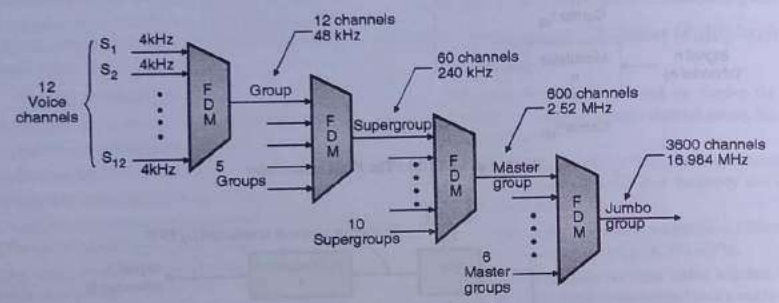
- The composite signal at the output of mixer is transmitted over the single communication channel as shown in Fig. 13.4.1(b). This signal can be used to modulate a radio transmitter if the FDM signal is to be transmitted through air.

13.4.2 FDM Receiver (Demultiplexing Process) :

- The block diagram of an FDM receiver is as shown in Fig. 13.4.1(c). The composite signal is applied to a group of Band Pass Filters (BPF).
- Each BPF has a center frequency corresponding to one of the carriers used in the transmitter i.e. f_{c1}, f_{c2}, ... f_{cn} etc.
- The BPFs have an adequate bandwidth to pass all the channel information without any distortion.
- Each filter will pass through only its channel and reject all the other channels. Thus all the multiplexed channels are separated out.
- The channel demodulator then removes the carrier and recovers the original signal back.

13.4.3 The Analog Carrier System :

- To maximize the efficiency of their infrastructure, the telephone companies have used multiplexing technique for lower bandwidth lines.
- In this way it is possible to combine many switched or leased lines into fewer but bigger channels.
- One of such hierarchical system is used by AT and T. It is as shown in Fig. 13.4.2 and is made up of groups, super groups, master groups and jumbo groups.



(L-110) **Fig. 13.4.2 : FDM hierarchy**

- The levels of multiplexing is also called as multiplexing hierarchy.
- The different levels of multiplexing which is also called multiplexing hierarchy is as follows :

Level (1) : Basic Group. [12 voice channels multiplexed together].

↓

Level (2) : Super Group. [Upto 5 basic groups multiplexed together

↓ i.e. upto 60 voice channels].

Level (3) : Master Group. [Upto 10 super groups multiplexed together

↓ i.e. upto 600 voice channels].

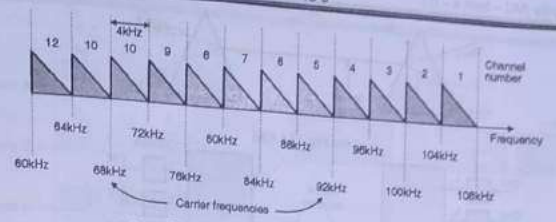
Level (4) : Jumbo Group. [Upto 6 master groups multiplexed together

i.e upto 3600 voice channels].

- This hierarchy is used by AT and T and shown in Fig. 13.4.2.

Basic Group [12 voice channels] :

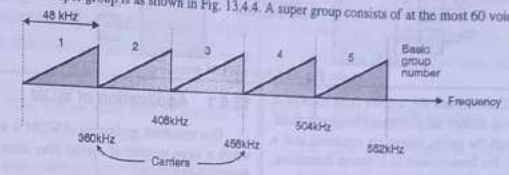
- The frequency plan for the typical basic group is as shown in Fig. 13.4.3. Here the 12 voice channels such as telephone channels modulate the carrier frequencies in the range of 60 to 108 kHz range. The carrier frequencies are spaced at 4 kHz from each other.
- SSB modulation technique is used to save the bandwidth. Each voice channel is applied to a balanced modulator along with a carrier. The output of a balanced modulator consists of the upper and lower sidebands.
- Frequency plans of groups of FDM are nothing but the frequency spectrums.
- The frequency plan for the basic group of FDM is shown in Fig. 13.4.3.



(L-111) **Fig. 13.4.3 : Frequency plan for the basic group of FDM**

Super group :

The frequency plan for a super group is as shown in Fig. 13.4.4. A super group consists of at the most 60 voice channels.



(L-112) **Fig. 13.4.4 : Frequency plan for a super group of FDM**

13.5 Advantages, Disadvantages and Applications of FDM :

13.5.1 Advantages of FDM :

1. A large number of signals (channels) can be transmitted simultaneously.
2. FDM does not need synchronization between its transmitter and receiver for proper operation.
3. Demodulation of FDM is easy.
4. Due to slow narrow band fading only a single channel gets affected.

13.5.2 Disadvantages of FDM :

1. The communication channel must have a very large bandwidth.
2. Intermodulation distortion takes place.
3. Large number of modulators and filters are required.
4. FDM suffers from the problem of crosstalk.
5. All the FDM channels get affected due to wideband fading.

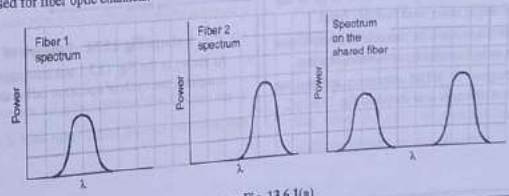
13.5.3 Applications of FDM :

Some of the important applications of FDM are :

1. Telephone systems.
2. AM (amplitude modulation) and FM (frequency modulation) radio broadcasting.
3. TV broadcasting.
4. First generation of cellular phones used FDM.

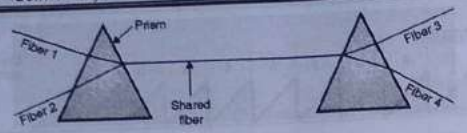
13.6 Wavelength Division Multiplexing (WDM) :

- WDM is the variation of FDM.
- It is specially used for fiber optic channels.

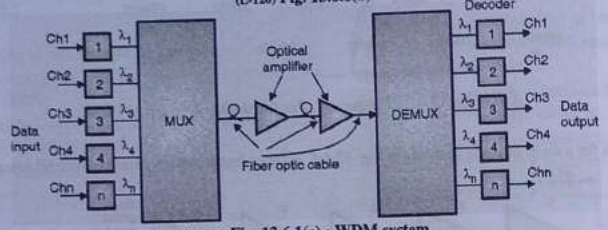


(L-119) Fig. 13.6.1(a)

Scanned by CamScanner



(L-120) Fig. 13.6.1(b)



(L-121) Fig. 13.6.1(c) : WDM system

- As shown in Figs. 13.6.1(a) and (b), 2 fibres come together at a prism, each having energy in a different frequency band. After passing through the prism, beams are combined onto a single shared fiber, for transmission to a distant destination, where they are split again.
- Channels having different frequency ranges can be multiplexed on a single long fiber.
- The only difference between WDM and electrical FDM is that an optical system is completely passive and thus highly reliable.
- Reason WDM is popular, is that the energy on a single fiber is a few gigahertz wide because it is impossible to convert between electrical and optical media any faster.
- Since BW of a single fiber band is about 25,000 GHz, there is great potential for multiplexing many optical channels together over long routes. Necessary condition is that incoming channels use different frequency bands.
- Potential application of WDM is in the FTTC (Fiber To The Curb) systems or in SONET networks.
- In the Fig. 13.6.1(b) we have a fixed wavelength system bits from fiber 1 go to fiber 3 and bits from fiber 2 go to fiber 4.
- It is not possible to have bits going from fiber 1 to fiber 4. It is also possible to build WDM systems that are switched, which contain many input and output fibers, switching data among themselves.
- Although spreading energy over n outputs dilutes it by a factor n, such systems are practical for hundred of channels.
- If light from one of the incoming fibers have to go to any output fiber, all the output fibers need tunnable filters.
- Alternatively, input fibers could be tunnable and output ones fixed. Having both to be tunnable is unnecessary expense.
- A simple block diagram of WDM transmitter and receiver system with different channels is as shown in Fig. 13.6.1(c).

13.6.1 Application of WDM :

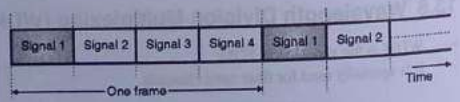
One important application of WDM is the SONET network in which a large number of optical fiber lines are multiplexed and demultiplexed.

13.6.2 DWDM (Dense WDM) :

- The long form of DWDM is dense WDM. It can multiplex a very large number of channels. The spacing between adjacent channels is small.
- Efficiency of DWDM is higher than that of WDM.

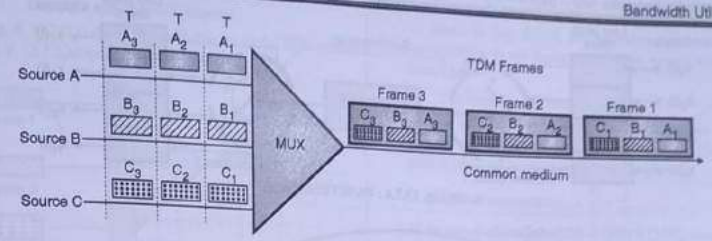
13.7 Synchronous Time Division Multiplexing :

- The process called multiplexing is used in order to utilize common transmission channel or medium to transmit more than one signals simultaneously.
- TDM is a digital multiplexing process.
- In TDM all the signals to be transmitted are not transmitted simultaneously. Instead, they are transmitted one-by-one.
- Thus each signal will be transmitted for a very short time. One cycle or frame is said to be complete when all the signals are transmitted once on the transmission channel. The TDM principle is illustrated in Fig. 13.7.1.



(L-122) Fig. 13.7.1 : Principle of TDM

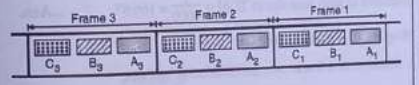
- As shown in the Fig. 13.7.1 one transmission of each channel completes one cycle of operation called as a "Frame".



(L-123) Fig. 13.7.2 : TDM system

- The TDM system can be used to multiplex analog or digital signals, however it is more suitable for the digital signal multiplexing.
- The concept of TDM will be more clear if you refer to Fig. 13.7.2.
- The data flow of each source (A, B or C) is divided into units (say A_1, A_2 or B_1, C_1 etc.)

  Then one unit from each source is taken and combined to form one frame. The size of each unit such as A_1, B_1 etc. can be 1 bit or several bits.
- Fig. 13.7.3 shows the frames of TDM signal. For 3 inputs being multiplexed, a frame of TDM will consist of 3 units i.e. one unit from each source.
- Similarly for n number of inputs, each TDM frame will consist of n units.



(L-124) Fig. 13.7.3 : TDM frames

- The TDM signal in the form of frames is transmitted on the common communication medium.

Data rate :

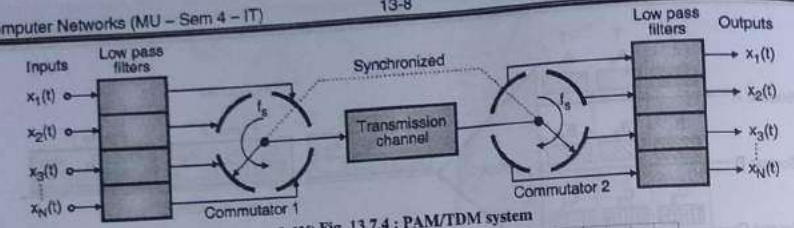
- For a TDM, the data rate of the multiplexed signal is always n times the data rate of individual sources, where n is the number of sources.
- So if three sources are being multiplexed, then the data rate of the TDM signal is three times higher than the individual data rate.
- Naturally the duration of every unit (A_1 or B_1 etc.) in TDM signal is n times shorter than the unit duration before multiplexing.

13.7.1 PAM - TDM System :

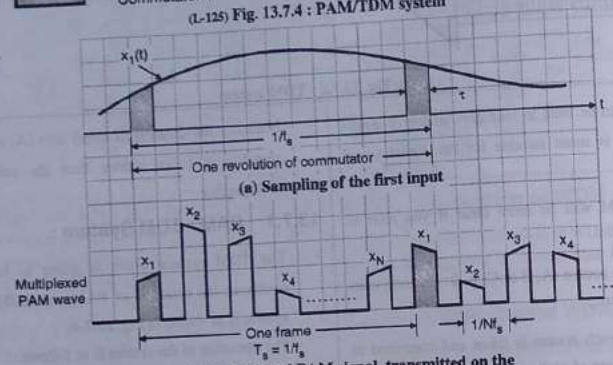
- The TDM system which is going to be discussed now, combines the concepts of PAM and TDM both. The TDM system is as shown in Fig. 13.7.4.

  The operation of the system is as follows :
- The multiplexer here is a single pole rotating switch or commutator. It can be a mechanical switch or an electronic switch. It rotates at f_s rotations per second.
- As the switch arm rotates, it is going to make contact with the position 1, 2, 3 or N for a short time. To these contacts are connected the N analog signals which are to be multiplexed.
- Thus the switch arm will connect these N input signals one by one to the communication channel.
- The waveform of a TDM signal which is being transmitted is as shown in Fig. 13.7.5. It shows that the rotary switch samples each channel during each of its rotations. Each rotation corresponds to one frame. Hence 1 frame is completed in T_s seconds where $T_s = 1/f_s$.
- At the receiver, there is one more rotating switch or commutator used for demultiplexing.
- It is important to note that this switch must rotate at the same speed as that of the commutator 1 at the transmitter and its position must be synchronized with commutator 1 in order to ensure proper demultiplexing.
- The same principle of multiplexing can be used for multiplexing more number of signals.

Scanned by CamScanner



(L-125) Fig. 13.7.4 : PAM/TDM system



(a) Sampling of the first input

(b) Multiplexed PAM signal, transmitted on the transmission channel

(L-126) Fig. 13.7.5

Interleaving :

- On the multiplexer side the commutator-1 opens in front of a connection, that connection has the opportunity to send its bit on to the channel.
- This process is called as interleaving.

Ex. 13.7.1 : 3 signals having a data rate of 2 kbps are grouped together by means of time division multiplexing. Each unit consists of 1 bit. Calculate :

1. The bit duration before multiplexing.
2. The transmission rate of TDM.
3. The duration of each time slot in TDM.
4. The duration of one TDM frame.

Soln. :

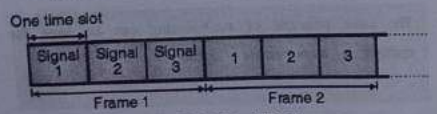
Step 1 : Duration of a bit before multiplexing :

- Each signal has a data rate of 2 kbps. That means 2000 bits per second.
- Hence the duration of each bit is,

$$T_b = \frac{1}{2000} = 0.5 \text{ mS} \quad \text{...Ans.}$$

Step 2 : Transmission rate of TDM :

The TDM frame is shown in Fig. P. 13.7.1.



(L-127) Fig. P. 13.7.1 : TDM frames

- As discussed earlier the transmission rate of TDM is n times higher than the bit rate of each source.

$$\text{Transmission rate of TDM} = n \times 2000 = 3 \times 2000$$
$$= 6000 \text{ bps or } 6 \text{ kbps} \quad \text{...Ans.}$$

Step 3 : Duration of time slot in TDM :

$$\text{Duration of each time slot in TDM} = \frac{1}{6000} = 166.67 \quad \text{...Ans.}$$

Step 4 : Frame duration :

$$\text{Duration of 1 frame} = n \times \text{duration of one slot}$$
$$= 3 \times 166.67\ \mu S = 0.5 \text{ mS} \quad \text{...Ans.}$$

Note : The duration of a TDM frame is always equal to the duration of one unit before multiplexing.

Ex. 13.7.2 : Three channels are to be multiplexed using TDM technique. The rate of each channel is 150 bytes per second. In TDM, one byte per channel is to be multiplexed.

Calculate :

1. Frame size
2. Frame duration
3. Frame rate and
4. Bit rate of the TDM signal.

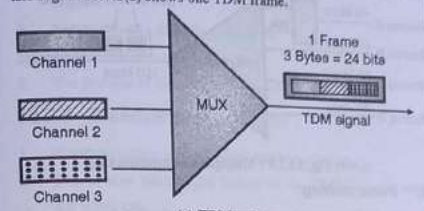
Soln. :

Given : Bit rate of each channel 150 bytes per sec, n = 3.

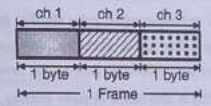
1 byte per channel to be multiplexed.

Step 1 : Draw the system block diagram :

Fig. P. 13.7.2(a) shows the block diagram of the TDM system and Fig. P. 13.7.2(b) shows one TDM frame.



(a) TDM system



(b) One frame of TDM

(L-128) Fig. P. 13.7.2

Step 2 : Frame size :

Each frame consists of one byte from each channel. So frame size is 3 bytes or 24 bits.

Step 3 : Frame duration and frame rate :

- The duration of a TDM frame is always equal to the duration of one unit before multiplexing.
- Here one unit before multiplexing is 1 byte i.e. 8 bits.

$$\therefore \text{ Frame duration} = 1 \text{ byte duration}$$

- But each channel transmits at 150 bytes/sec.

$$\therefore \text{ Frame duration} = \frac{1}{150} = 6.666 \text{ mS} \quad \text{...Ans.}$$

$$\text{Frame duration} = \frac{1}{\text{Frame duration}}$$

$$= \frac{1}{6.666 \times 10^{-3}} = 150 \text{ frames/sec.} \quad \text{...Ans.}$$

Step 4 : Bit rate of TDM signal :

$$\text{Bit rate of TDM} = \text{Number of bits per frame}$$
$$\times \text{Number of frames per second.}$$
$$= 24 \times 150 = 3600 \text{ bps} \quad \text{...Ans.}$$

13.7.2 Signaling Rate (r) :

- The signaling rate of a TDM system is defined as the number of pulses transmitted per second. It is denoted by "r". Let us now derive the expression for the signaling rate of the PAM-TDM system.
- Let W = Maximum frequency of all the input signals x_1 to x_N.
- Therefore as per Nyquist criteria, the sampling frequency $f_s \geq 2$ W. Therefore the speed of rotation of the commutators is f_s rotations per second with $f_s \geq 2W$.
- As shown in Fig. 13.7.6, one revolution of commutators corresponding to one frame contains one sample from each input signal.

$$\therefore \text{ 1 Revolution} \Rightarrow \text{1 frame} \Rightarrow \text{N pulses} \quad \text{...(13.7.1)}$$

- 1 frame period is $(1/f_s)$ i.e. T_s seconds. Therefore in "T_s" seconds "N" number of pulses are transmitted. Hence the pulse to pulse spacing within the frame is given by,

$$\text{Pulse to pulse spacing} = \frac{T_s}{N} = \frac{1}{Nf_s} \quad \text{...(13.7.2)}$$

- As the period of one pulse (ON + OFF) is $(1/Nf_s)$ seconds, the number of pulses per second is given by,

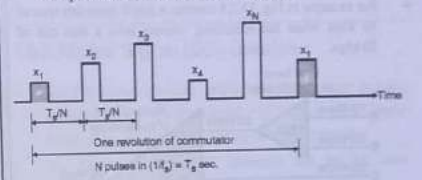
$$\text{Number of pulses per second} = Nf_s$$

- This is nothing but the signaling rate.

$\therefore$ Signaling rate of a TDM system = $r = Nf_s$ pulses/second. But as $f_s \geq 2W$.

$$\text{Signaling rate of a TDM system} = r \geq 2NW \text{ pulses/second} \quad \text{...(13.7.3)}$$

- A TDM system is supposed to have its signaling rate as high as possible. It is evident from the expressions above that the signaling rate can be increased by increasing the sampling rate f_s and/or the number of input signals N.



(L-129) Fig. 13.7.6 : Calculation of number of pulses per second for PAM-TDM system

13.7.3 Transmission Bandwidth of a TDM Channel :

- The minimum transmission bandwidth of a PAM-TDM channel is given by,

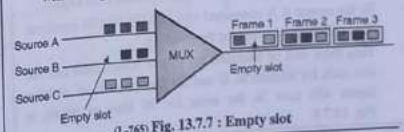
$$B_T = \frac{1}{2} \text{ signaling rate}$$

$$\therefore \text{ Minimum transmission bandwidth } B_T \geq \frac{1}{2} \times 2\,NW$$

$$\therefore \text{ Minimum transmission bandwidth } B_T = NW \quad \text{...(13.7.4)}$$

13.7.4 Empty Slots :

- The drawback of synchronous TDM is its low efficiency. This is because if a particular source does not have any data to send, then the time slot allotted to it in the output frame will be empty, as shown in Fig. 13.7.7.



(L-765) Fig. 13.7.7 : Empty slot

Scanned by CamScanner

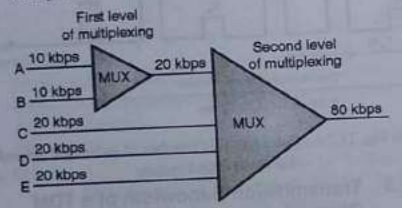
- In Fig. 13.7.7 the source B has one empty slot (due to discontinuous data).
- As shown in Fig. 13.7.7, the second and the third frame has three filled slots but the first frame has only two slots filled. Thus the first time slot is carrying less data than its maximum capacity.
- The statistical TDM system improves the efficiency by removing such empty slots.

13.7.5 Data Rate Management :

- The problem with synchronous TDM is it inability to handle the disparity in the input data rates. That means the data rates of different sources are not same but different.
- If the data rates of all the inputs are not same then three different strategies may be used. They are :
  1. Multilevel multiplexing.
  2. Multiple slot allocation.
  3. Pulse stuffing.
- We will discuss these strategies one by one.

1. Multilevel multiplexing :

- This technique is used when the data rate of an input line is exact multiple of data rates of other lines.
- For example in Fig. 13.7.8 sources A and B have data rates of 10 kbps while the remaining sources have a data rate of 20 kbps.

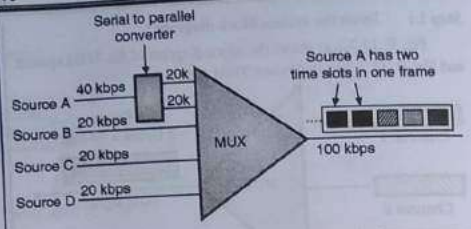


(L-766) **Fig. 13.7.8 : Multilevel multiplexing**

- As shown in Fig. 13.7.8, the input lines from sources A and B are multiplexed together to provide the data rate of 20 kbps (which is equal to the data rate of remaining three sources).
- These four inputs are given to second level of multiplexer which produces an output at 80 kbps.

2. Multiple slot allocation :

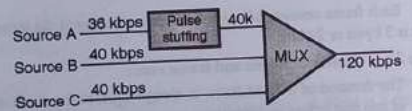
- Sometimes we can improve the efficiency by allotting more than one slot in a frame to a single source. This can be done for an input source which has a higher data rate as compared to the other input lines.
- For example refer Fig. 13.7.9 the source A has a data rate of 40 kbps and the data rate of the other sources is 20 kbps.
- So the source A is connected to a serial to parallel converter. This will give two slots for the source A.
- Thus there will be two slots for source A per frame and one slot each for sources B, C and D. The data rate of all these inputs will now be the same i.e. 20 kbps as shown in Fig. 13.7.9.



(L-767) **Fig. 13.7.9 : Multiple slot multiplexing**

3. Pulse stuffing :

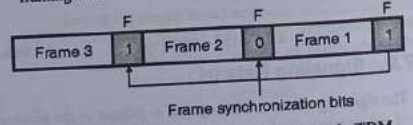
- If the bit rates of sources are not multiple integers of each other, then the two techniques discussed earlier are not useful.
- So another technique called pulse stuffing is used. Here the highest input data rate is made the dominant data rate and then dummy bits to the input lines having lower data rates.
- Pulse stuffing is also called as pulse stuffing, bit padding, or bit stuffing and it is demonstrated in Fig. 13.7.10.
- Note that the source A has a lower data rate of 36 kbps and so pulse stuffing is done to correct its rate to 40 kbps.



(L-768) **Fig. 13.7.10 : Pulse stuffing**

13.7.6 Frame Synchronization :

- The implementation of TDM is not as simple as that of FDM because in TDM, the synchronization of multiplxer and demultiplxer is essential.
- If the synchronization is not there then the bit that belongs to one channel may be received by some other channel.
- Therefore one or more synchronization bits are generally added to the beginning of each frame. They are known as the framing bits.



(L-131) **Fig. 13.7.11 : Frame synchronization in TDM**

- These bits are called frame synchronizing bits or simply framing bits.
- The framing bits will follow a pattern frame to frame. For example the pattern shown in Fig. 13.7.11 is 101.
- The framing bit pattern will allow the demux to synchronize itself to the mux.

13.7.7 Advantages of TDM :

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

13.7.8 Disadvantages of TDM :

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

13.7.9 Applications of TDM :

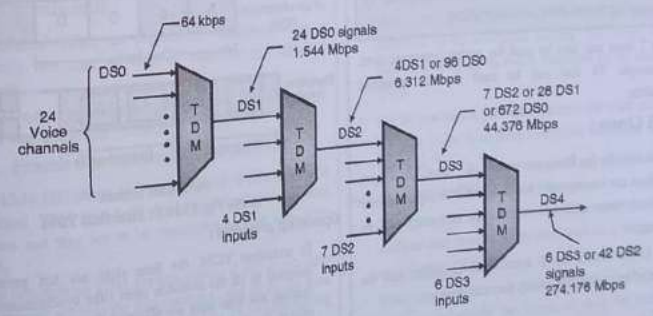
1. Multiplexing of digital signals.
2. Digital telephony.
3. Satellite communications.
4. Fiber optic communication.
5. Wireless communication applications.

13.8 Comparison of FDM and TDM Systems :

Sr. No.	FDM	TDM
1.	The signals which are to be multiplexed are added in the time domain. But they occupy different slots in the frequency domain.	The signals which are to be multiplexed can occupy the entire bandwidth but they are isolated in the time domain.
2.	FDM is usually preferred for the analog signals.	TDM is preferred for the digital signals.
3.	Synchronization is not required.	Synchronization is required.
4.	The FDM requires a complex circuitry at the transmitter and receiver.	TDM circuitry is not very complex.
5.	FDM suffers from the problem of crosstalk due to imperfect band pass filters.	In TDM the problem of crosstalk is not severe.
6.	Due to wideband fading in the transmission medium, all the FDM channels are affected.	Due to fading only a few TDM channels will be affected.
7.	Due to slow narrowband fading taking place in the transmission channel only a single channel may be affected in FDM.	Due to slow narrowband fading all the TDM channels may get wiped out.

13.9 Digital Signal (DS) Service :

- The telephone companies implement TDM (time division multiplexing) through the hierarchy of digital signals. This is called as digital signal (DS) service or digital hierarchy.
- Fig. 13.9.1 shows the DS hierarchy and the bit rates corresponding to various levels.



(G-1311) **Fig. 13.9.1 : D.S. hierarchy**

Scanned by CamScanner

Explanation :

- A DS0 signal is the basic input signal which is a single digital channel (usually 64 kbps PCM channel).
- 24 DS0 signals are multiplexed using TDM to produce a DS1 signal. The bit rate of DS1 is 24 × 64 kbps = 1.544 Mbps plus 8 kbps of overhead.
- 4 such DS1 signals are multiplexed at the second level of multiplexing to obtain the DS2 signal.
- One DS2 signal is equivalent to 4 DS1 or 96 DS0 signals and it has a bit rate of 6.312 Mbps.
- 7 DS2 signals are multiplexed to produce a DS3 signal. Its bit rate is 44.376 Mbps and it is equivalent to 7 DS2 or 28 DS1 or 672 DS0 signals.
- Finally 6 DS3 lines are multiplexed to obtain a DS4 signal. Its bit rate is 274.176 Mbps. It is obtained as a result of 6 DS3 or 42 DS2 channels, 168 DS1 channels and 4032 DS0 channels.

13.9.1 T Lines :

- DS0, DS1, DS2, ... etc. are the names of the services. The telephone companies use the T lines (T0, T1, T2, ... etc.) to implement these services.
- The T lines have capacities which precisely match with the bit rates of the corresponding services as shown in Table 13.9.1.

Table 13.9.1 : Relation between DS and T lines

Service	Line	Rate (Mbps)	Number of voice channels
DS – 1	T – 1	1.544	24
DS – 2	T – 2	6.312	96
DS – 3	T – 3	44.736	672
DS – 4	T – 4	274.176	4032

- Thus T – 1 line implements DS – 1 service, T – 2 implements DS – 2 service and so on.
- DS0 is defined as the basic service.

Note : T lines are digital lines which are designed to carrying digital data, audio or video.

- But the T lines can also be used for analog communication. For example T1 line can be used for the telephone applications.

13.9.2 E Lines :

- E-line is actually the European version of T lines. The T lines and E lines are conceptually identical but their capacities and number of voice channels which they can carry will be different.
- Table 13.9.2 shows the E lines, their capacities and the number of voice channels which they can carry.

Table 13.9.2 : E lines and their capacity

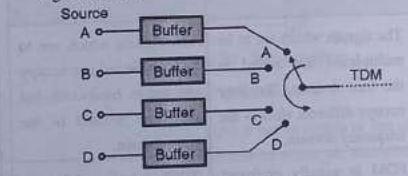
Line	Rate (Mbps)	Number of voice channels
E – 1	2.048	30
E – 2	8.448	120
E – 3	34.368	480
E – 4	139.264	1920

13.9.3 Applications of Synchronous TDM :

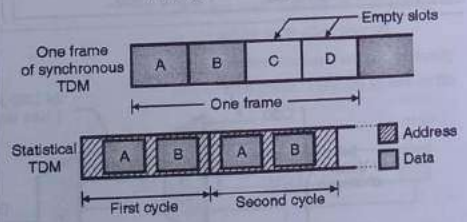
1. For analog telephone system (T – 1 system).
2. Some second generation cellular telephone companies use synchronous TDM.

13.10 Statistical TDM :

- The TDM system that we have discussed earlier is known as the synchronous TDM. This system has a major drawback. In synchronous TDM, many of the time slots in a frame are wasted due to absence of data on some of the time slots.
- Therefore an alternative system called as statistical TDM or asynchronous TDM or intelligent TDM is used.
- The block diagram of the statistical TDM system is as shown in Fig. 13.10.1(a) and its frame format is as shown in Fig. 13.10.1(b).



(L-138)(a) Block diagram



(b) Frame format

(L-139) Fig. 13.10.1 : Statistical TDM

Operating principle :

- In statistical TDM, the time slots are not permanently assigned to all the available users (like synchronous TDM). Instead, the time slots are allocated dynamically on demand only to those channels holding data for transfer.

- Each TDM channel is called as an I/O line. Thus the statistical TDM has many I/O lines and one high speed multiplexed line.
- Each I/O line has a buffer associated with it. As shown in Fig. 13.10.1, there are N number of I/O lines. Out of these only K channels are transmitted which hold data for transfer. The remaining (N – K) channels are not considered for transmission.
- In statistical TDM, the multiplexer will "scan" the input buffers of all the channels, sequentially. During the scan time, it collects the data until a frame is filled. As soon as a frame is filled, it is transmitted.
- The data is transferred on the transmission medium. The received frame is then distributed among the output buffers by the output multiplexer.

13.10.1 Data Rate of Statistical TDM :

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

13.10.2 Slot Size :

- The slot carries both data and address, the ratio of the data size to address size should be reasonable to ensure high efficiency.
- In statistical TDM, the data block contains many bits while address bits are very few.

13.10.3 No Synchronization Bit :

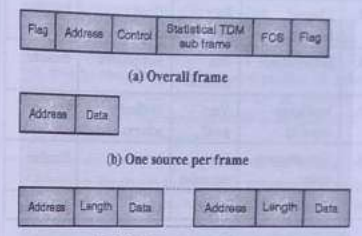
- The statistical TDM frames need not be synchronized. So it is not necessary to use the synchronizing bit.

13.10.4 Bandwidth :

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

13.10.5 Frame Format for Statistical TDM :

- Fig. 13.10.1(b) shows the comparison of synchronous and statistical TDM frames. It shows that there are four data sources and they are to be transmitted in four time slots t_0 to t_3.
- In the synchronous TDM, the data sources A and B only have data present whereas the data sources C and D do not have any data. Hence time slots $(t_1 - t_2)$ and $(t_2 - t_3)$ corresponding to these sources are empty.
- On the other hand, the statistical TDM system does not send the empty slots. Thus during the first cycle, data from the sources A and B only is transmitted.
- As the data from A and B only is being sent and the time slots of C and D are utilized for this purpose, the positional identity of slots is lost in statistical TDM. We cannot predict ahead of time about data from which source will be in which slot.
- Due to this unpredictability, the address information is required to be sent alongwith the data information. This address is then used for proper delivery of data.
- Thus each slot of statistical TDM carries an address as well as data. The detailed frame structure is as shown in Fig. 13.10.2.



(a) Overall frame

(b) One source per frame

(c) Multiple sources per frame

(L-140) Fig. 13.10.2 : Frame formats of statistical TDM

Now refer to Fig. 13.10.2.

- The frame structure for the statistical TDM should be such that it should minimize the overhead bits. This is important for improving the throughout efficiency.
- The statistical TDM system uses a synchronous protocol such as HDLC. Therefore within the HDLC frame, the data frame contains the control bits for the sake of multiplexing operation.
- Fig. 13.10.2 shows two such frame formats. Fig. 13.10.2(b) shows only one source of data per frame. This source is identified by the associated address. The length of the data field is variable and its end is identified by the end of overall frame.
- But the one source per frame scheme will work properly only for light loads. It is quite inefficient under the heavy load condition.

Improvement in efficiency :

1. The throughput efficiency can be improved by allowing the multiple data sources to be packaged in a single frame as shown in Fig. 13.10.2(c).
2. When many sources are packaged in a single frame, it is necessary to specify the length of data for each source. Therefore the statistical TDM subframe consists of a

Scanned by CamScanner

sequence of data fields. Each data field is labelled with an address and a length.

13.10.6 Comparison of FDM, Synchronous TDM and Statistical TDM :

Table 13.10.1 : Comparison of data multiplexer techniques

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

13.11 Introduction to Spread Spectrum :

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

1. How to utilize the channel bandwidth efficiently ?
2. How to minimize the amount of transmitted power ?

However the efficient utilization of bandwidth and minimizing the transmitted power are not the "only" problems faced by a communication system. Some other problems encountered by it are as follows :

Problems encountered by a communication system :

1. In the areas such as "military communication", the information has to be "secured". That means an unauthorized user is not expected to access the information. Also he should not be allowed to interfere the communication by any means.
2. Sometimes a hostile transmitter (say used by terrorists) can "jam" the desired or legitimate transmission. To avoid this the channel should be "immune" to any external interference.
3. Even in the non-military communications an unintentional interference is caused by a user who is transmitting its information through a channel which is already being used.

Remedy :

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

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

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

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

13.12 Applications of Spread Spectrum Modulation :

The spread spectrum signals are used in the following applications :

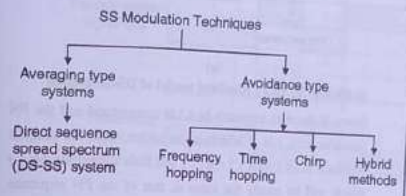
1. To avoid the intentional interference (called as jamming).
2. **To reject the unintentional interference from some other user :** This is possible to achieve by assigning a different code for the signals from various users. This type of communication which allows multiple users to share a common channel for transmission of information is called as Code Division Multiple Access (CDMA).
3. **To avoid the self interference due to multipath propagation :** A signal can take multiple paths while travelling over a communication channel from transmitter to receiver.

   The signal components following different path lengths will result in a dispersed signal at the receiver. This is known as the self-interference. This type of interference also can be suppressed by using the SS modulation.
4. **In low probability of intercept (LPI) signals :** A message can be hidden in the background noise by spreading its bandwidth using the code word and then transmitting the coded signal at a low power level. Due to these modifications, the probability that such a signal be intercepted (detected) is reduced to a great extent. Hence such a spread and coded signal is called as the low probability-of-intercept (LPI) signal.
5. **In obtaining the message privacy :** The message privacy can be obtained by superimposing a pseudorandom pattern on the transmitted message.

13.13 Classification of the Spread Spectrum Modulation Techniques :

The SS modulation techniques are broadly categorized into two categories namely the averaging type systems and the avoidance type systems as shown in Fig. 13.13.1.

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



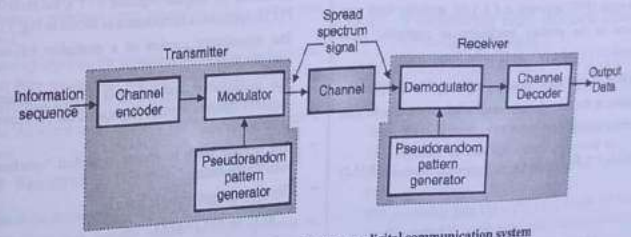
(E-470) Fig. 13.13.1 : Classification of spread spectrum technique

13.14 Model of Spread Spectrum Digital Communication System :

The block diagram shown in Fig. 13.14.1 illustrates the basic elements of a spread spectrum digital communication system.

Operation :

- The information sequence at the input of the system is a binary information sequence. The same signal is recovered at the output of the system as output data signal.
- We have already discussed the role of a channel encoder, channel decoder, modulator and demodulator.
- In addition to these basic building blocks of a digital communication system, two additional blocks called "pseudo-random pattern generator" are used as shown in Fig. 13.14.1. One of them is connected to the modulator on the transmitter side whereas the other is connected to the demodulator on the receiving side. Both these generators are identical to each other.
- These generators generate a pseudorandom or pseudonoise (PN) binary sequence.
- It is impressed on the transmitted signal at the modulator. Thus the modulated signal along with the pseudorandom sequence travels over the communication channel. This sequence spreads the signal randomly over a wide frequency band. Thus the output of the modulated is a spread spectrum signal.
- The pseudorandom sequence is removed from the received signal, by the other "pseudorandom generator" operating at the receiver. Thus the pseudorandom pattern generators operate in synchronization with each other.
- The synchronization between these pattern generators is achieved before the beginning of the signal transmission. This is done by transmitting a fixed pseudorandom bit pattern which a receiver can recognize even in presence of interference. Once this synchronization is established, it is possible to begin the transmission.
- Thus in the spread spectrum receiver, the receiver can demodulate the transmitted signal if and only if a known pseudo-noise sequence has been transmitted along with the information signal.
- Two types of interferences are present in the SS digital communication system namely the narrow band or broadband interference.
- The modulation techniques used are :
  1. Phase shift keying (PSK) and
  2. Frequency shift keying (FSK)
- If PSK is used, then the PN sequence generated at the modulator is used along with the PSK modulation to shift the phase of the PSK signal pseudorandomly. The resulting signal at the modulator output is called as a "Direct-Sequence" (DS) spread spectrum signal.
- If binary or M-ary FSK is being used, then the frequency of the FSK signal is shifted pseudorandomly. The resulting signal at the output of the modulator is called as "Frequency Hopped" (FH) spread spectrum signal.



(E-471) Fig. 13.14.1 : Model of spread spectrum digital communication system

Scanned by CamScanner

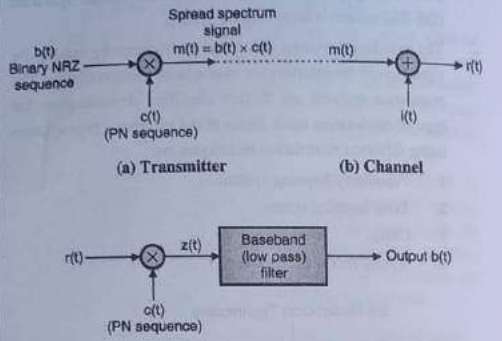
13.15 Direct Sequence Spread Spectrum (DS-SS) :

- The most important advantage of spread spectrum modulation is that it provides protection against externally generated interfering signals. Such signals are called as a jamming signals.
- The information bearing signal is made to occupy a bandwidth which is much larger than the minimum bandwidth required for its transmission.
- This will make the signal to appear like a noise and blends into the background.
- Thus the spread spectrum is a method of **camouflaging** the message signal.
- One of the methods used for widening the bandwidth of the data sequence is to use the modulation.
- Refer Fig. 13.15.1 which shows the transmitter, channel and receiver of an idealized model of baseband spread spectrum system. This is also known as direct sequence spread spectrum (DS-SS) modulation.

13.15.1 Operation of the Encoder (Transmitter) :

- The input data sequence is denoted by d(t). This data sequence is first converted into an NRZ sequence b (t) by the NRZ encoder.
- The NRZ signal b (t) and the pseudonoise signal c (t) are applied to the two inputs of a product modulator.
- At the output of the product modulator, we obtain the spread spectrum signal.
- The spectrum of this signal is quite spread out as compared to the spectrum of b (t) which is a narrow band signal.
- Thus a data sequence b (t) is used to modulate a wideband pseudo-noise (PN) sequence c (t) by applying these two sequences to the product modulator or multiplier. Both sequences b (t) and c (t) are in polar form.
- According to the fourier transform theory the multiplication of signals in the time domain results in convolution of their frequency domain i.e.

$$c(t)\times b(t) \overset{F}{\longleftrightarrow} C(f) * B(f) \qquad ...(13.15.1)$$



(E-478) **Fig. 13.15.1 : Idealized model of DS-SS system**

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

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

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

$$r(t) = m(t)+i(t) \qquad ...(13.15.2)$$

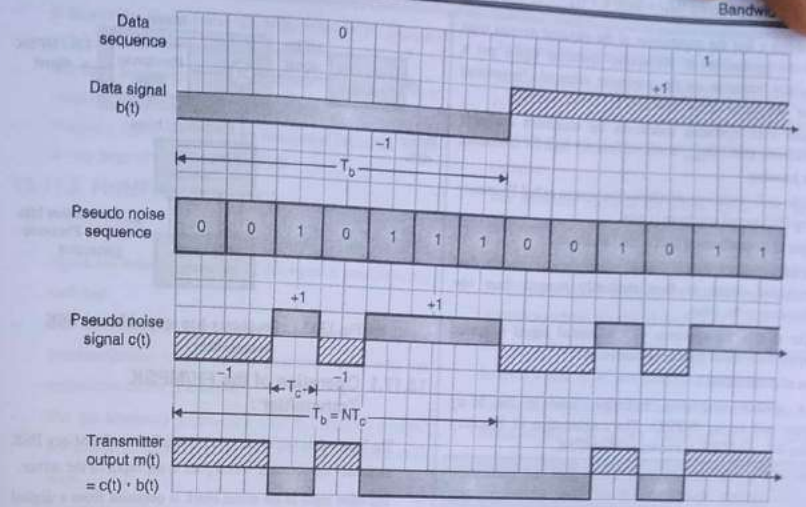
$$= c(t)b(t)+i(t) \qquad ...(13.15.3)$$

- The waveforms at different points in the transmitter are as shown in Fig. 13.15.2.

13.15.2 Receiver :

- To recover the original sequence b (t), the received signal r (t) is applied to a demodulator as shown in Fig. 13.15.1(c).
- The demodulator consists of a multiplier followed by a low-pass filter.
- The multiplier is supplied with a locally generated PN sequence which is an exact "replica" of the PN sequence used at the transmitter.
- The receiver needs to operate in perfect "synchronization" with the transmitter.
- The demodulated signal is given by,

$$z(t) = c(t)\times r(t) \qquad ...(13.15.4)$$



(E-479) **Fig. 13.15.2 : Waveforms of DS-SS transmitter**

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

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

We get,

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

$$\therefore\ z(t) = c^2(t)b(t)+c(t)i(t) \qquad ...(13.15.5)$$

- In Equation (13.15.5) note that the desired signal b(t) has been multiplied by $c^2(t)$. We know that,

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

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

Hence Equation (13.15.5) gets converted to,

$$z(t) = b(t)+c(t)i(t) \qquad ...(13.15.6)$$

- Thus the multiplier output in a receiver contains the desired signal b (t) and the product of the PN sequence c (t) and interference signal i (t).
- Due to the multiplication, the product signal c (t) · i (t) becomes a wideband signal whereas b (t) is a narrow band signal.
- Hence by applying the multiplier output to a baseband (low pass) filter we can pass only signal b (t) and attenuate the interference signal c (t) i (t) heavily.
- Thus the effect of interference signal is reduced to a great extent.

13.15.3 Features of DSSS :

- Some of the important features of DSSS are as follows :

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

13.15.4 Applications of DS-SS System :

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

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

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

- In the DS-SS system discussed in the previous section, the NRZ data sequence b (t) modulates the PN sequence.
- The product signal [m (t) = b (t) × c (t)] is spread instantaneously in the frequency domain due to this process.
- The capacity of DS-SS system to reject the intentional interference (jamming) is dependent on the "processing gain PG".
- The processing gain PG = (T_b / T_c). Hence PG increases if the chip period T_c is decreased which in turn permits a greater transmission bandwidth and more chips per bit.

Scanned by CamScanner

- **Problem :** But the capabilities of the physical devices used for the generation of PN spread spectrum signal put a practical limitation on the maximum value of "processing gain" and hence on the capability to combat jamming.
- Under some operating conditions the maximum attainable processing gain $PG_{(max)}$ is not sufficiently high for combating the jamming.
- Under such conditions an alternative system called Frequency Hop (FH) spread spectrum is used.

Principle of operation of (FH – SS) system :

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

Types of modulation :

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

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

13.16.1 Types of Frequency Hopping :

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

1. Slow frequency hopping.
2. Fast frequency hopping.

Slow frequency hopping :

- In slow frequency hopping the **symbol rate R_s** of the MFSK signal is an integer multiple of the hop rate R_h.
- That means several symbols are transmitted corresponding to each frequency hop.

  ∴ Each frequency hop ⇒ Several symbols.

  i.e. Frequency hopping takes place slowly.

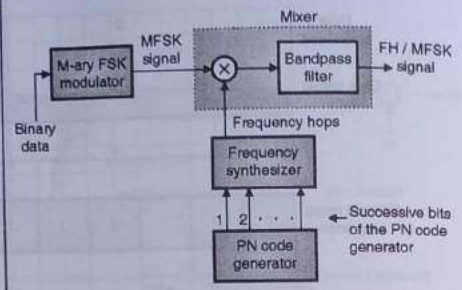
Fast frequency hopping :

- In the fast frequency hopping the hop rate R_h is an integer multiple of the MFSK **symbol rate R_s**.
- That means during the transmission of one symbol, the carrier frequency will hop several times.

  ∴ Each symbol transmission ⇒ Several frequency hops.
- Thus the frequency hopping takes place at a fast rate.

13.17 Slow Frequency Hopping :

- Fig. 13.17.1 shows the block diagram of a slow-frequency hopping FH/MFSK transmitter.



(L-609) **Fig. 13.17.1 : Frequency hop spread M-ary FSK transmitter**

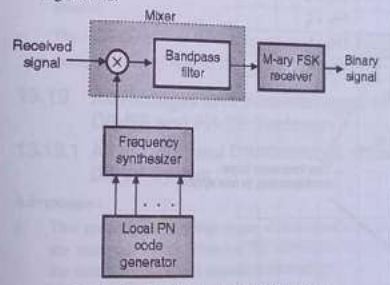
13.17.1 Operation of the FH/MFSK Transmitter :

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

- If the number of successive bits at the output of PN generator is "n", then the total number of frequency hops will be 2^n.
- The total bandwidth of the transmitted FH/MFSK signal is equal to the sum of all the frequency hops.
- Therefore the bandwidth of the transmitted FH/MFSK signal is very large of the order of few GHz.

13.17.2 FH/MFSK Receiver :

- Due to the large bandwidth occupied by the FH/MFSK signal, the coherent detection of this signal is possible within each hop.
- This is because for coherent detection, the phase synchronization of the locally generated carrier with the transmitted carrier is essential.
- But the frequency synthesizers used in FH/MFSK receiver are unable to maintain this phase coherence over successive hops.
- Therefore most frequency hop spread spectrum systems use the non-coherent M-ary modulation schemes.
- The block diagram of an FH-MFSK receiver is as shown in Fig. 13.17.2.



(L-610) **Fig. 13.17.2 : An FH-MFSK receiver**

Operation of FH/MFSK receiver :

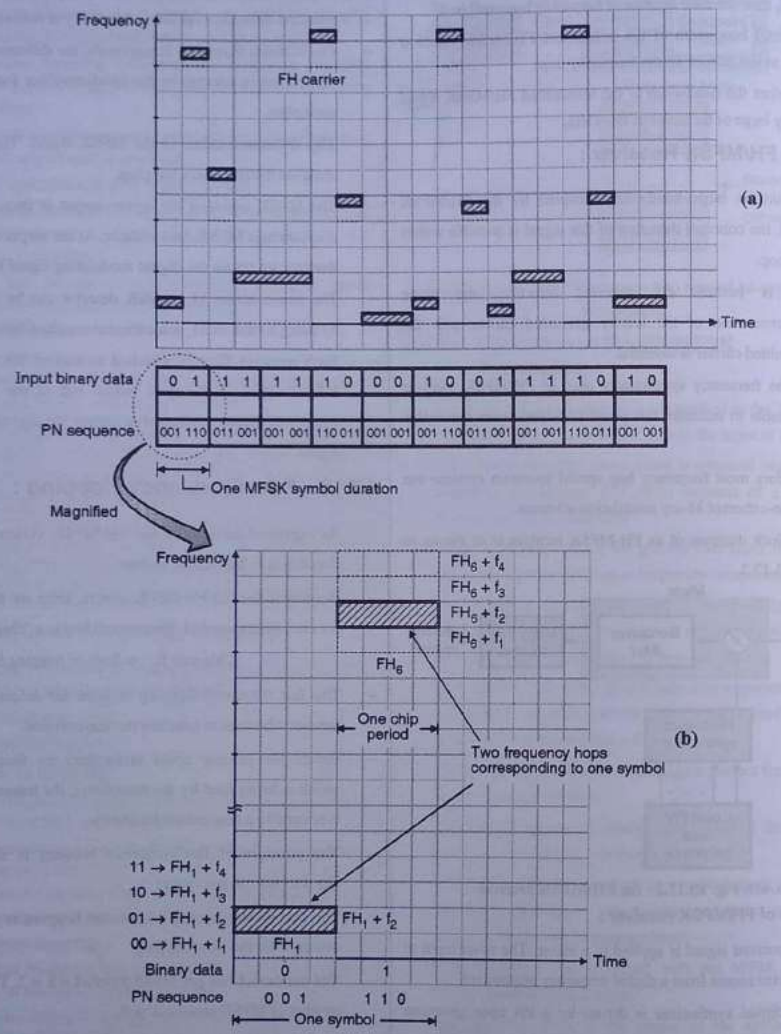
- The received signal is applied to a mixer. The other input to the mixer comes from a digital frequency synthesizer.
- This digital synthesizer is driven by a PN code generator which is synchronized with the PN code generator at the transmitter and generates the same code sequence.
- Therefore the frequency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

13.18 Fast Frequency Hopping :

- As explained earlier, the fast FH/MFSK system is different than the slow FH/MFSK system.
- Because in the fast FH/MFSK system, there are multiple hops for each M-ary symbol. Hence each hop is a "chip".

  ∴ Chip rate R_c = Rate of hopping R_h
- The fast frequency hopping is used for defeating a smart jammer who tries to interfere the transmission.
- Before the jammer could understand the frequency band which is being used by the transmitter, the transmitted signal is hopped to a new carrier frequency.
- The principle of fast frequency hopping is illustrated in Fig. 13.18.1 (on next page).
- The data sequence used for the fast hopping is same as the one used for the slow hopping.
- The number of bits per MFSK symbol = k = 2. Therefore the number of MFSK tones = $2^k = 4$.
- The length of PN segment per hop i.e. n = 3. Therefore the total number of frequency hops = $2^3 = 8$.
- The PN sequence decides the hopping frequency (shown by dotted lines in Fig. 13.18.1(a). Two successive input binary bits 0 1 form the first symbol.

Scanned by CamScanner



(E-487) **Fig. 13.18.1 : Waveforms of fast hopping system**

- During this symbol duration the PN sequence (3 digit) has two distinct values viz. : 001 and 110.
- Therefore one symbol duration corresponds to two frequency hops. As shown in Fig. 13.18.1(b) the frequency of the MFSK modulator for symbol 01 is f_2 and the outputs of the synthesizer corresponding to 001 and 110 outputs of the PN sequence generator are say FH_1 and FH_6.
- Therefore the transmitted frequencies are $(FH_1 + f_2)$ and $(FH_6 + f_2)$. The operation for the first symbol 01 is summarized below.

Summary of operation in the first symbol duration :

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

Receiver used for fast hopping :

- For the recovery of the data, at the receiver, noncoherent detection is used.
- But the detection procedure is very much different from that used for a slow FH/MFSK system.
- In practice the following two procedures are considered :

1. In this procedure, a separate decision is made on the k frequency-hop chips received. Then the estimation of the dehopped MFSK symbol is done based on the simple rule based on majority vote.
2. In the second procedure, for each FH/MFSK symbol likelihood functions are computed, as functions of the total signal received over k chips and the largest one of them is selected.

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

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

13.19.1 Advantages and Disadvantages of the DS-SS System :

Advantages :

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

Disadvantages :

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

13.19.2 Advantages and Disadvantages of FH-SS System :

Advantages :

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

Disadvantages :

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

13.20 Comparisons :

13.20.1 Comparison of Slow and Fast Frequency Hopping :

- Table 13.20.1 shows the comparison of FH-SS methods.

Table 13.20.1

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

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

Sr. No.	Parameter	Direct sequence spread spectrum	Frequency hopping spread spectrum
1.	Definition	PN sequence of large bandwidth is multiplied with narrow band data signal.	Data bits are transmitted in different frequency slots which are changed by PN sequence.
2.	Chip rate	It is fixed $R_c = \frac{1}{T_c}$	$R_c = \max(R_b, R_f)$
3.	Modulation technique	BPSK	M-ary FSK

Scanned by CamScanner

Sr. No.	Parameter	Direct sequence spread spectrum	Frequency hopping spread spectrum
4.	Acquisition time	Long	Short
5.	Effect of distance	This system is distance relative	Effect of distance is less

Review Questions

Q. 1 With the help of block schematic, explain the principle of FDM.

Q. 2 Compare FDM and TDM methods of multiplexing.

Q. 3 Illustrate working of FDM used for 96 channels of telephone.

Q. 4 With the help of block diagram explain the FDM system for telephone communication.

Q. 5 Explain the principles of Time Division Multiplexing.

Q. 6 What is statistical TDM ?

Q. 7 What is the difference between synchronous and statistical TDM ?

Q. 8 What are the advantages of statistical TDM ?

Q. 9 Why is it necessary to use time division multiplexing while transmitting PAM signals ?

Q. 10 Why is synchronization needed in TDM system ?

Q. 11 Describe how transmission distortion of a TDM signal can cause cross-talk between two adjacent channels ?

Q. 12 Describe the multiplexing hierarchy for an FDM system.

Q. 13 Describe the multiplexing hierarchy for digital multiplexing.

Q. 14 Explain the PCM-TDM system.

Q. 15 What do you understand by the channel associated signaling ?

Q. 16 State the applications of PCM-TDM.

Q. 17 How is synchronization achieved in PCM-TDM system ?

Q. 18 State advantages and disadvantages of TDM system.

Q. 19 State the problems encountered by a communication system.

Q. 20 How is SS signal different from the normal one ?

Q. 21 State true or false : The SS signal is pseudorandom in nature.

Q. 22 State some applications of SS modulation.

Q. 23 Name various types of SS systems.

Q. 24 Which modulation techniques are used in SS ?

Q. 25 Explain the DS-SS system with the help of suitable block diagram.

Q. 26 Explain the FH-SS system with the help of suitable block diagram.

Q. 27 Compare DS-SS and FH-SS systems.

Q. 28 Compare slow and fast FH-SS systems.

□□□

CHAPTER 14

Transmission Media

Module VI

Syllabus :

Guided madia, Unguided media, Wireless, Real time interactive protocols : Rationale for new protocols RTP, Session Initialization Protocol (SIP), H.323, SCTP.

14.1 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.

14.1.1 Classification of Transmission Media :

MU : May 15, Dec. 15, May 16, Dec. 16

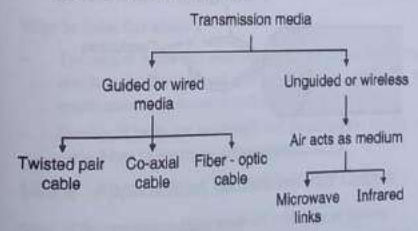
University Questions

Q. 1 Explain the different transmission media in networking. **(May 15, 10 Marks)**

Q. 2 Describe about the different guided transmission medias. **(Dec. 15, Dec. 16, 10 Marks)**

Q. 3 Explain guided transmission media in detail. **(May 16, 10 Marks)**

- We can classify the transmission media as shown in Fig. 14.1.1 into two categories.

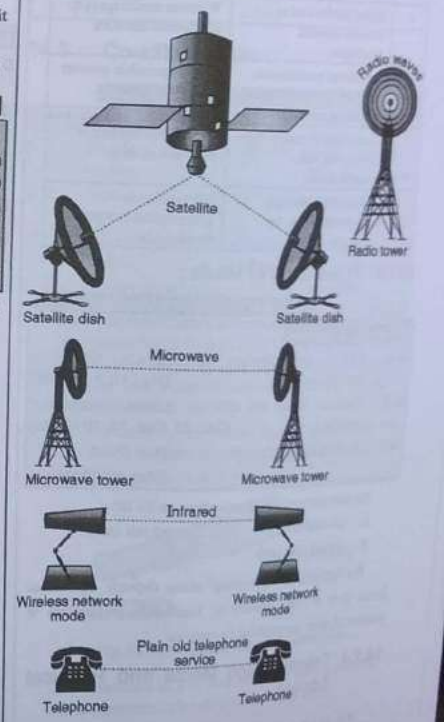


(L-571) Fig. 14.1.1 : Classification of transmission media

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

1. **Guided media :** Guided media is a communication medium which allows the data to get guided along it. For this the media need to have a point to point physical connection.
2. **Unguided media :** The wireless media is also called as an unguided media.

- The examples of guided media are copper wires and fiber-optics, whereas radio and lasers through the air are examples of unguided media as shown in Fig. 14.1.2.



(L-573) Fig. 14.1.2 : Transmission medias

Scanned by CamScanner

14.1.2 Comparison of Wired and Wireless Media :

Comparison of wired and wireless media is given in Table 14.1.1.

Table 14.1.1 : 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.

14.1.3 Types of Wired Media :

MU : May 15, Dec. 15, May 16, Dec. 16

University Questions

Q. 1 Explain the different transmission media in networking. **(May 15, 10 Marks)**

Q. 2 Describe about the different guided transmission medias. **(Dec. 15, Dec. 16, 10 Marks)**

Q. 3 Explain guided transmission media in detail. **(May 16, 10 Marks)**

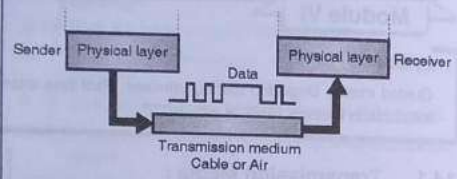
The most commonly used networking media are :

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.

14.1.4 Transmission Media and Physical Layer :

- Fig. 14.1.3 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. 14.1.3 and the physical layer controls the transmission media directly.
- Transmission medium is the cable or air over which data can travel from sender to receiver in the form of digital or analog signals.



(L-570) **Fig. 14.1.3 : Relation between transmission medium and physical layer**

14.2 Twisted Pair Cables :

MU : May 14, May 15, Dec. 15, May 16, Dec. 16

University Questions

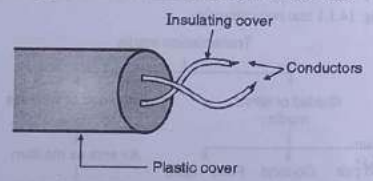
Q. 1 Describe about the different guided transmission medias. **(May 14, 10 Marks)**

Q. 2 Explain the different transmission media in networking. **(May 15, 10 Marks)**

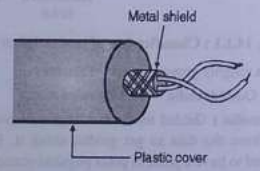
Q. 3 Describe about the different guided transmission medias. **(Dec. 15, Dec. 16, 10 Marks)**

Q. 4 Explain guided transmission media in detail. **(May 16, 10 Marks)**

- The construction of twisted pair cable is as shown in Fig. 14.2.1. 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. 14.2.1 : Construction of twisted pair cables**

14.2.1 Types of Twisted Pair Cables :

- The two commonly used types of twisted pair cables are as follows :
  1. Unshielded Twisted Pair (UTP).
  2. Shielded Twisted Pair (STP).
- The construction of UTP and STP cables is shown in Fig. 14.2.1.

UTP :

- A twisted pair consists of two insulated conductors twisted together in the shape of a spiral as shown in Fig. 14.2.1. It can be shielded or unshielded.
- The unshielded twisted pair cables are very cheap and easy to install. But they are badly affected by the electromagnetic noise interference.

STP :

- STP cable as shown in Fig. 14.2.1(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.

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.

14.2.2 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.

14.2.3 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

14.3 Co-axial Cables :

MU : May 14, May 15, Dec. 15, May 16, Dec. 16

University Questions

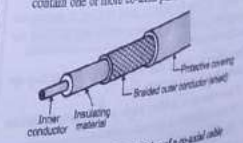
Q. 1 Describe about the different guided transmission medias. **(May 14, 10 Marks)**

Q. 2 Explain the different transmission media in networking. **(May 15, 10 Marks)**

Q. 3 Describe about the different guided transmission medias. **(Dec. 15, Dec. 16, 10 Marks)**

Q. 4 Explain guided transmission media in detail. **(May 16, 10 Marks)**

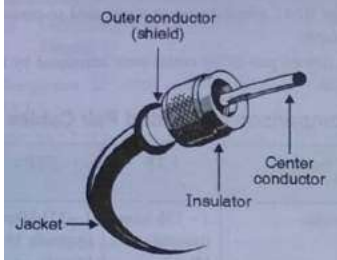
- The construction of co-axial cable is as shown in Fig. 14.3.1. It consists of two concentric conductors namely as inner conductor and a braided outer conductor separated by a dielectric material.
- The external conductor is in the form of metallic braid and used for the purpose of shielding. The co-axial cable may contain one or more co-axial pairs.



(L-577) **Fig. 14.3.1 : 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. 14.3.2.

Scanned by CamScanner



(L-577) **Fig. 14.3.2 : 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. 14.3.2 providing insulation and protection.

The co-axial cable was initially developed for analog telephone networks. A single co-axial cable would be used to carry more than 10,000 voice channels at a time.

The digital transmission systems using the co-axial cable were developed in 1970s. These systems operated in the range of 8.5 Mb/s to 565 Mb/s.

The most popular application of a co-axial cable is in the cable TV system. The existing co-axial cable system has a range from 54 MHz to 500 MHz.

Other important application is cable modem, with the cable modem termination system (CMTS).

One more application is Ethernet LAN using the co-axial cable. The co-axial cable is used for its large bandwidth and high noise immunity.

.1 Characteristics of a Co-Axial Cable :

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.

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).

14.3.2 Co-axial Cable Standards :

Table 14.3.1 shows the co-axial cable standards. The co-axial cables are categorised by their RG ratings where RG stands for Radio Government.

Table 14.3.1 : Categories of co-axial cables

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

14.3.3 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.

14.4 Optical Fiber Cables :

MU : May 14, May 15, Dec. 15, May 16, Dec. 16

University Questions

Q. 1 Describe about the different guided transmission medias. **(May 14, 10 Marks)**

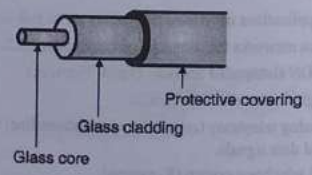
Q. 2 Explain the different transmission media in networking. **(May 15, 10 Marks)**

Q. 3 Describe about the different guided transmission medias. **(Dec. 15, Dec. 16, 10 Marks)**

Q. 4 Explain guided transmission media in detail. **(May 16, 10 Marks)**

Construction :

- The construction of an optical fiber cable is as shown in Fig. 14.4.1.
- 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.

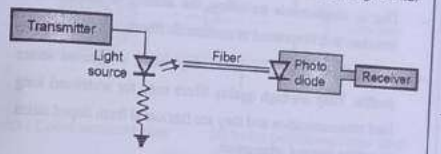


(G-103) **Fig. 14.4.1 : Construction of optical fiber cable**

- 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.

14.4.1 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. 14.4.2.

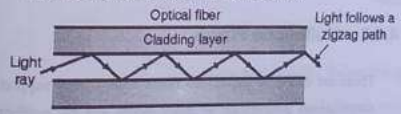


(G-104) **Fig. 14.4.2**

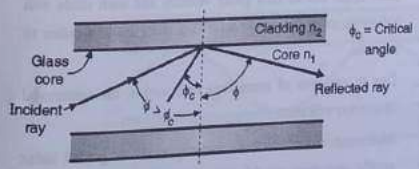
- The two light sources which are used popularly are :
  1. LED (Light Emitting Diode).
  2. Injection Laser Diode (ILD).
- The LED is cheaper but has a disadvantage that it provides an unfocussed light which hits the core boundaries and gets diffused.
- So LED is preferred only for short distances.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

14.4.2 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. 14.4.3(a).



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



(b) Reflection at the interface of core and cladding

(G-105) **Fig. 14.4.3**

- Fig. 14.4.3(b) illustrates the principle of light travel through the optical fiber.
- When the light enters into a glass fiber from one end, most of it propagates along the length of the fiber and comes out from the far end.
- A small portion of the incident light escapes through the side walls of the fiber.
- The light which travels from one end to the other end of the glass fiber is said to have "guided" through the fiber.
- The light stays inside the fiber and does not escape through the walls because of the "total internal reflection" taking place inside the fiber.
- This total internal reflection can take place only if the following two conditions are satisfied :
  1. The glass fiber core must have a refractive index which is higher than the refractive index of the cladding around the core ($n_1 > n_2$).
  2. The angle of incidence of the light entering the fiber must be greater than the critical angle "ϕ_c".

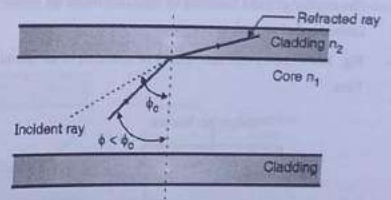
$$\sin \phi_c = \frac{n_2}{n_1}$$

This is as shown in Fig. 14.4.3.

Observations from Fig. 14.4.3(b) :

Some of the important observations from Fig. 14.4.3(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. 14.4.4. The refracted ray enters into the cladding and gets lost.



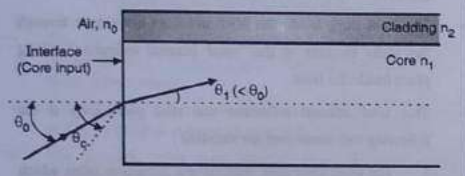
(G-106) **Fig. 14.4.4 : Refraction takes place at the core cladding interface if $\phi < \phi_c$**

Scanned by CamScanner

14.4.3 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. 14.4.5.

- 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. 14.4.5 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. 14.4.5 : 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. 14.4.5. 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,

$$n_0 \sin \theta_0 = n_1 \sin \theta_1 \quad ...(14.4.1)$$

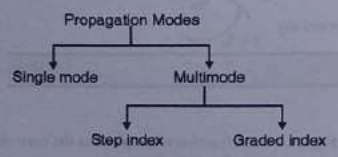
- Therefore the emerging angle θ_1 is given by,

$$\sin \theta_1 = \frac{n_0}{n_1} \sin \theta_0 \quad ...(14.4.2)$$

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.

14.4.4 Modes of Propagation :

- The number of paths followed by light rays inside the optical cable is called as modes.
- Fig. 14.4.6 shows different modes of operation of an optical fiber.

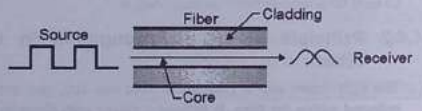


(G-108) **Fig. 14.4.6 : Propagation modes in optical fibers**

- There are two types namely single mode and multimodes 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.

14.4.5 Single Mode Fibers :

- These are called as single mode fibers because they support on one mode of propagation (TE, TM or TEM).
- The optical signal travelling inside this fiber has only one group velocity.
- Due to single mode travelling, the amount of dispersion is less than that introduced in multimode fibers.
- These fibers can have either step index or graded index profile. They are high quality fibers used for wideband long haul communication and they are fabricated from doped silica to reduce internal attenuation.
- The light travel in a single mode fiber is shown in Fig. 14.4.7. This beam travel's almost horizontally and follows only one path from source to destination, as shown in Fig. 14.4.7. 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.

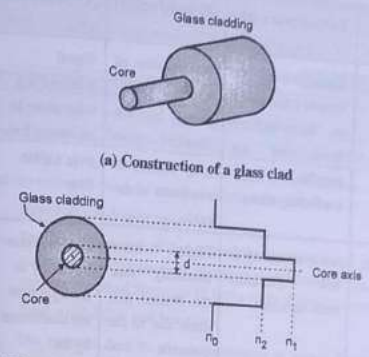


(G-109) **Fig. 14.4.7 : Single mode fiber**

14.4.6 Multimode Fibers :

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

Step index fibers :

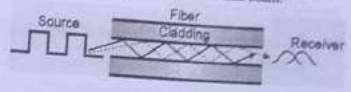


(a) Construction of a glass clad

(b) Cross sectional view (c) Index profile core type fiber

(G-110) **Fig. 14.4.8**

- The construction of an optical fiber with a core and glass cladding is as shown in Fig. 14.4.8(a).
- The refractive index of the core is n_1 and that of the glass cladding is n_2, with $n_1 > n_2$. Therefore the index profile of glass clad core fiber is as shown in Fig. 14.4.8(c).
- Due to the sudden change in refractive index at the boundary of core and cladding, this fiber is called **step index** fiber.
- Fig. 14.4.9 illustrates the propagation of light over a step index fiber.
- Multiple beams will follow different zigzag paths as shown in Fig. 14.4.9. The number of reflections that a beam undergoes, depends on the angle of incidence of that beam.

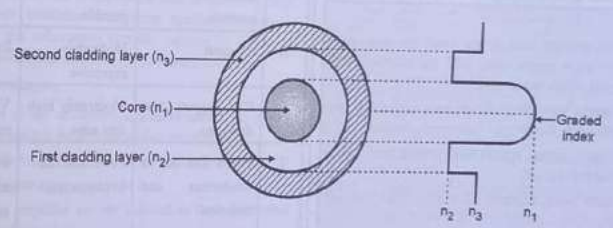


(G-111) **Fig. 14.4.9 : Multimode step index fiber**

- 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.

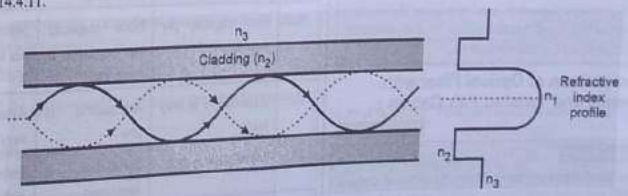
Graded index fibers :

- As shown in Fig. 14.4.10, 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. 14.4.10 : 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. 14.4.11.



(G-113) **Fig. 14.4.11 : Propagation of light in a graded index fiber**

Scanned by CamScanner

- 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.

14.4.7 Characteristics of Optical Fiber Cables :

Fiber optic cables have the following characteristics :

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

Note :

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

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

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.

14.5 Advantages and Disadvantages of Fiber Optical Fibers :

14.5.1 Advantages of Optical Fibers :

MU : May 09

University Questions

Q. 1 What are the advantages of fiber optics as communication medium ? **(May 09, 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.

14.5.2 Disadvantages of Optical Fibers :

Some of the disadvantages of optical communication system are :

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

14.5.3 Applications :

1. Optical fiber transmission systems are widely used in the backbone of networks.
2. Optical fibers are now used in the telephone systems.
3. In the Local Area Networks (LANs).

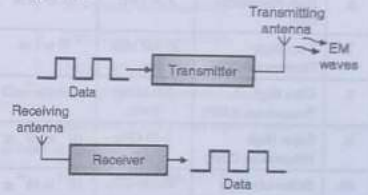
14.6 Unguided (Wireless) Media :

MU : May 15

University Questions

Q. 1 Explain the different transmission media in networking. **(May 15, 10 Marks)**

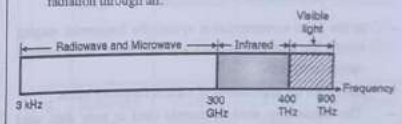
- As already defined, an unguided media (also called as wireless media) does not use a conductor or wire as a communication channel.
- Instead it uses the air or vacuum as medium to carry the information from transmitter to receiver.
- The transmitter first converts the data signal into electromagnetic 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. 14.6.1.



(G-117) **Fig. 14.6.1 : Concept of unguided media**

14.6.1 Unguided Media : Wireless :

- The electromagnetic spectrum used for wireless communication is shown in Fig. 14.6.2. The signal from sender to receiver travels in the form of electromagnetic radiation through air.



(L-597)**Fig. 14.6.2 : Electromagnetic spectrum for the wireless communication**

Propagation methods :

- The unguided signals can travel from the transmitter to receiver in many different ways : The three most important methods are :

Scanned by CamScanner

1. Ground wave propagation 2. Sky propagation.
3. Space propagation or line of sight propagation.

14.6.2 Bands :

The electromagnetic spectrum is divided into several subbands. Table 14.6.1 gives various frequency bands, corresponding type of propagation and application.

Table 14.6.1 : 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

14.6.3 EM Spectrum and Communication Applications :

- In the radio communication system the frequencies ranging from a few kilohertz to many gigahertz all are being used for various purposes.
- Let us see the applications of various frequency bands.
- The frequencies most commonly used in early days were from about 300 kHz to 3 MHz and were called as **Medium Frequencies (MF).** The frequencies in the range 30 kHz to 300 kHz are known as the **Low Frequencies (LF).**
- The frequencies in the range 3 kHz to 30 kHz are called as **Very Low Frequencies (VLF).** On the higher frequency side **High Frequencies (HF)** will cover the frequency range from 3 MHz to 30 MHz. Then **Very High Frequency (VHF)** from 30 MHz to 300 MHz and so on.
- Table 14.6.2 gives you the details of entire usable frequency spectrum and its applications.

Table 14.6.2 : 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.

14.6.4 Infrared Signals :

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

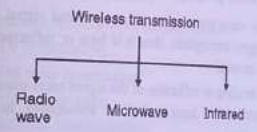
3. TV remote control.
4. Wireless keyboards and mouse.

14.6.5 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.

14.7 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.

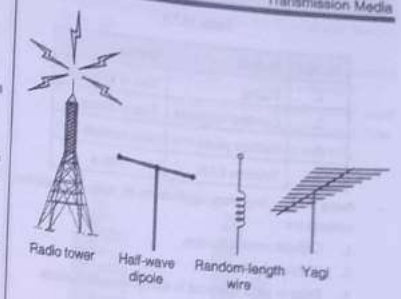


(L-598)**Fig. 14.7.1 : Classification of wireless media**

14.7.1 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. 14.7.2.



(L-599) **Fig. 14.7.2 : 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 14.7.1.

Table 14.7.1

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 14.7.2.

Scanned by CamScanner

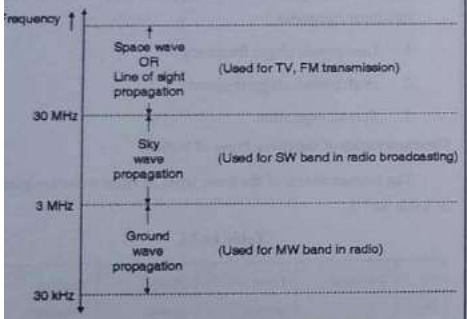
Table 14.7.2

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.

14.7.2 Modes of Propagation of EM Waves :

- Once the signal leaves the antenna, (i.e. radiated) it can take any of the following three routes (paths).
- The type of propagation is decided by the route taken by the signal to reach the receiver from the transmitter.



(D-718)Fig. 14.7.3 : Relation between the type of propagation and frequency

The three basic paths that a radio signal can take are :

1. Along the surface of the earth (ground wave propagation).
2. Upto the layer called "ionosphere" and back (sky wave propagation).
3. From transmitter to receiver in a straight line. (space wave propagation)

The path taken by a radio signal depends on many factors including the frequency of the signal, atmospheric conditions and the time of day.

The relation between frequency and the type of propagation is as shown in the Fig. 14.7.3.

Ground wave propagation :

Refer to the Fig. 14.7.4 showing the path followed by the radiated EM waves in ground wave propagation.

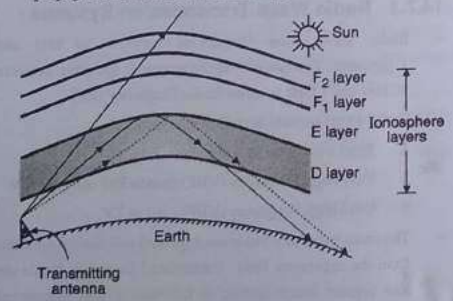
(D-719)Fig. 14.7.4 : Ground wave propagation

The important points about the ground wave propagation are as follows :

1. The ground or surface wave leaves the antenna and remains closed to the earth. The ground wave will actually follow the curvature of the earth and therefore can travel a distance beyond the horizon.
2. The ground wave propagation is the strongest at the low and medium frequency ranges. The ground waves is the path chosen by the signal when the frequency is between 30 kHz and 3 MHz.
3. The ground waves must be vertically polarized to prevent short circuiting of the electric field component. The EM waves are said to be vertically polarized if all its electric intensity vectors are vertical. The EM wave shown in Fig. 14.7.4 is vertically polarized.

2. Sky wave propagation - The ionosphere :

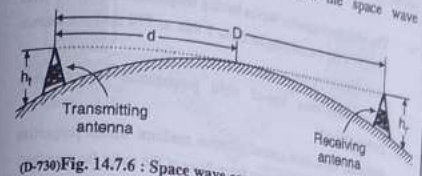
- In sky wave propagation, the transmitted signal travels into the upper atmosphere, then it is bent or reflected back from there to earth.
- This bending or reflection of the signal takes place due to the presence of a layer called as ionosphere in the upper atmosphere.
- The layers of ionosphere and the principle of sky wave propagation is as illustrated in the Fig. 14.7.5.



(D-721) Fig. 14.7.5 : Principle of sky wave propagation

3. Space wave propagation (Line of sight propagation) :

- The sky wave propagation cannot take place above the frequencies of 30 MHz because the ionosphere cannot reflect back such high frequencies and the ground wave dies out near the transmitting antenna itself, due to the wavefront tilting.
- Hence at frequencies above 30 MHz the space wave propagation is used.



(D-730)Fig. 14.7.6 : Space wave communication by space waves

- The space wave propagation takes place by the space waves or direct waves as shown in Fig. 14.7.6.
- These waves travel in a straight line directly from the transmitting antenna to the receiving antenna.
- The direct or space waves are not refracted like sky waves nor do they follow the curvature of the earth like the ground waves.
- Due to the straight line nature of the space waves they will at some point be blocked due to curvature of earth.
- If the signal is to be received beyond the horizon then the receiving antenna must be tall enough as shown in Fig. 14.7.6. The sky wave propagation is also called known as the line of sight propagation.

Applications of space waves :

Applications of space wave propagation are :

1. TV broadcasting.
2. FM radio broadcasting.
3. Microwave links.
4. Satellite communication.

14.7.3 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 :

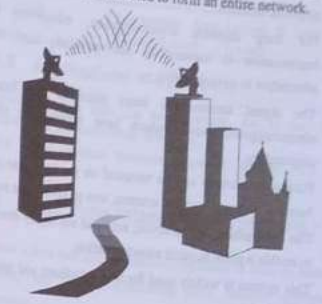
1. Terrestrial.
2. Satellite.

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. 14.7.7.
- 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.



(L-600) Fig. 14.7.7 : Terrestrial microwave system

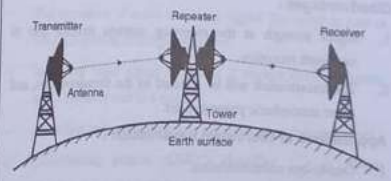
Characteristics of Terrestrial Microwave Systems :

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. 14.7.8 : 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. 14.7.8.

Scanned by CamScanner

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.

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.

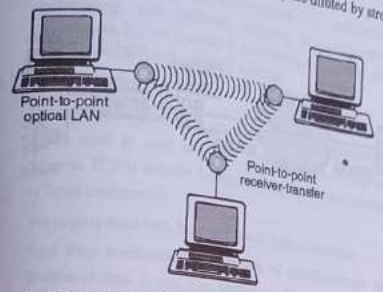
14.8 Infrared Light Used for Transmission :

- 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.

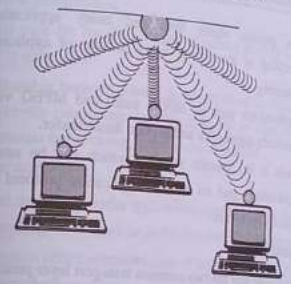
14.8.1 Applications and Standards :

- 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. 14.8.1**

14.8.2 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.

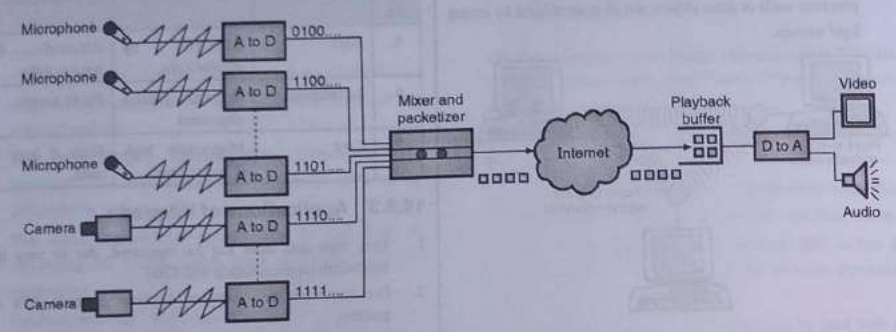
14.8.3 Applications of Infrared :

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.

14.9 Real Time Interactive Protocols :

- Now a days real time interactive applications such as internet phone and video conferencing have become extremely popular.
- So the standard bodies such as IRTE and ITU have been busy in laying out standards for the class of applications.
- Fig. 14.9.1 shows a real-time multimedia system.
- Now a days, interactive real time application is normally formed with many number of microphones and cameras.
- Digital data is formed by converting the audio and video information with the help of analog to digital converter.
- From different sources the digital data is generated which is mixed and packetized. These packets are sent to packet switched internet.
- At the destination the packets are received with different delays or some packets may also be lost or corrupted.
- Based on the timestamp on each packet, a **playback buffer** replays the packets.
- For recreation of audio and video signal this result is sent to DAC (Digital to Analog Converter).
- Recreated video signal is sent to a display device whereas audio signal is sent to a speaker.
- **Contributor** is each camera or microphone at the source site.
- **Contributing source (CSRC) identifier** : It is 32-bit identifier given to a contributor.
- The mixer is also known as **synchronizer** and synchronizing **source identifier (SSRC)** is another identifier given to synchronizer.

Scanned by CamScanner



(G-2218) **Fig. 14.9.1 : Real time multimedia system**

- The protocols used for real time interactive applications are :
1. RTP (Real time protocol).
2. RTCP (Real time transport control protocol).
3. SIP (Session initiation protocol).
4. H.323.
5. SCTP (Stream control transmission protocol).

14.9.1 Rationale for New Protocols :

- In this section we will discuss why we need new protocols for handling real time multimedia applications such as audio and video conferencing.
- First three layers of TCP/IP protocol suite i.e. physical, datalink and network layer need not be changed. Because for carrying any type of data these three layers are designed.
- Functions of first three layers of the TCP.IP protocol suite
- **Functions of first three layers of the TCP/IP protocol suite :**
  1. Physical layer : Provides service to datalink layer.
  2. Datalink layer : Responsible for node-to-node delivery of the network layer.
  3. Network layer : Responsible for host-to-host delivery of a datagram.
- It is necessary to encode and compress the multimedia data which considers the trade-off between the bandwidth requirement, quality and complexity of mathematical operations. For this reason some application layer protocols is needed.
- For handling multimedia application layer protocol can not be handled individually and have some requirements which can be handled by the transport layer.

Application layer :

- The nature of audio and video conferencing is different from some applications such as E-mail, file transfer etc.
- Due to this reason for interactive real time multimedia we need develop some application layer protocols.
- The private sector developed many applications and everyday in the market many number of applications are appearing.
- Applications such as MPEG audio and MPEG video uses standards defined for audio/video data transfer.
- There is no specific standard which can be used by all applications and no specific application protocol which is used by everyone.

Transport layer :

- We know that the two common transport layer protocols used are TCP and UDP.
- Now question is that for real time multimedia applications whether to use TCP or UDP ?
- First we discuss the transport layer protocol requirements for interactive real time multimedia. Then we will see either UDP or TCP can fulfill and respond to these requirements.

14.9.2 Requirements of Transport Layer for Interactive Real Time Multimedia :

Following are the transport layer requirements for interactive real time multimedia

1. Sender receiver negotiation.
2. Packet stream creation.
3. Error control.
4. Source synchronization.
5. Congestion control.
6. Identifying sender.
7. Jitter removal.

1. Sender-receiver negotiation :

- Before encoded and compressed data transfer the application program should negotiate the standards used.

- The lack of a single standard for audio or video is the first requirement.
- We have many number of standards for audio/video conferencing with different encoding or compression mechanisms. It is not possible to communicate if a sender and receiver uses different encoding methods.

2. Packet stream creation :

- User datagram protocol is appropriate for such applications which need to send messages with clear cut boundaries whereas TCP is suitable for applications which send stream of bytes continuously.
- We require these both features for real time multimedia.
- Real time multimedia is a **stream of chunks/stream of frames** of data. In real time multimedia frame or chunk has specific boundary or size, but between frames / chunks there are some relationships.
- In this case for handling stream of chunks neither TCP nor UDP is suitable.
- Relationship between frames is not provided by UDP. TCP can provide relationship between bytes but as compared to a multimedia frame/chunk, a byte is much smaller.

3. Error control :

- In real time multimedia applications special care is required for handling errors such as packet loss and packet corruption.
- We cannot afford retransmission of lost or corrupted packets. For reproduction of lost or corrupted packet we need to insert extra redundancy in data. That means TCP protocol is not suitable for real time applications.

4. Source synchronization :

- Synchronization of sources is required if an applications uses more than one source i.e. Both audio and video.
- With the help of mixers, source synchronization can be done.

5. Congestion control :

- It is necessary to provide some congestion control in multimedia like other applications. Because of retransmission problem if we decide not to use TCP for multimedia then somehow we should implement congestion control mechanism in the system.

6. Identifying sender :

- Like other applications, an issue with multimedia applications is that identification of sender at the application layer.
- When we are using the internet, with the help of IP addresses the parties are identified.
- In multimedia, it is required to map the IP address more friendly, as we did in the applications such as E-mail or HTTP.

7. Jitter removal :

- Jitter created at the receiver side is one of the problem with multimedia applications. Packet switched service provided by the internet can generate delays for different packets in the stream, due to this reason jitter is created at the receiver side.
- In the past years audio conferencing was provided by telephone network. Telephone network was designed as circuit switched network which was jitter free.
- With the help of playback buffers and time-stamping, the problem of jitter can be improved.
- At the receiver side the playback buffer is implemented at the applications layer. But with time-stamping and sequencing the transport layer must able to provide the application layer.

14.9.3 Whether to use TCP or UDP to Handle Real – Time Multimedia :

- In this section we will discuss the ability of UDP or TCP to handle real-time multimedia. Let us see either TCP and UDP is able to handle requirements of real time multimedia.
- Table 14.9.1 shows comparison between TCP and UDP with respect to requirements discussed above.

Table 14.9.1 : Comparison between TCP and UDP

Sr. No.	Requirement	TCP	UDP
1.	Sender-receiver negotiation	No	No
2.	Packet stream creation	No	No
3.	Error control	Yes	No
4.	Source synchronization	No	No
5.	Congestion control	Yes	No
6.	Identifying sender	No	No
7.	Jitter removal	No	No

- From Table 14.9.1 it is evident that neither TCP nor UDP can fulfill these all requirements.
- One important point we must remember that for implementation of client-server socket we require a transport layer protocol. Application layer cannot do the job of the transport layer.

These means we possibly have following three choices :

1. New transport layer protocol :

- A new transport layer protocol can be used e.g. SCTP which combines characteristics of both TCP and UDP.
- The choice of SCTP is probably the best choice because SCTP has its own additional features with features of TCP and UDP.
- When there were several multimedia applications SCTP was introduced.
- In the future SCTP can become the de-facto transport layer.

Scanned by CamScanner

2. Combination of TCP with another transport facility :

- For compensation of requirements which cannot be provided by TCP we can combine TCP with another transport facility.
- As TCP uses a retransmission mechanism which is not acceptable for real time multimedia applications, this choice is somewhat difficult.
- TCP cannot do multicasting is another problem with TCP.
- For real time interactive communication multi-party connection is required but TCP connection is only two parity connection.

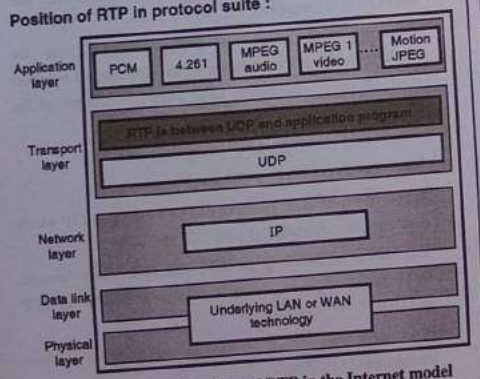
3. Combination of UDP with another transport facility :

- The requirements which UDP cannot provide, in this choice we can use combination of UDP with another transport facility.
- To provide client server socket interface we use UDP, but another protocol which runs at the top of UDP is used.
- For real time multimedia applications this is the present choice.
- The transport facility which we can use with UDP is Real Time Transport Protocol (RTP) which we will discuss in the next section.

14.10 RTP [Real Time Transport Protocol] :

- The protocol which is designed to handle real time traffic on the Internet is the Real Time Protocol or RTP. Since it has no delivery mechanism like multicasting, port numbers and so on, it must be used with UDP.
- RTP has been placed between UDP and the application program as in the Internet model shown in Fig. 14.10.1.
- RTP is mainly used for carrying out following functions :
  1. Time stamping. 2. Sequencing.
  3. Mixing facilities.

Position of RTP in protocol suite :



(G-742) **Fig. 14.10.1 : Position of RTP in the Internet model**

14.10.1 RTP Packet Format :

- The format of the RTP packet header has been shown in Fig. 14.10.2. The format is very simple and general in nature. It is capable of covering all real time applications.
- The function of each field is as described below :

1. Version field (Ver) :

This is a two bit long field which helps us define the version number. The current version of RTP is 2. So the contents of Ver field will be 2.

2. Padding (P) field :

This is a 1 bit field.

If padding is present at the end of the packet, then it is indicated by P = 1.

If P is set to 0, then there is no padding.

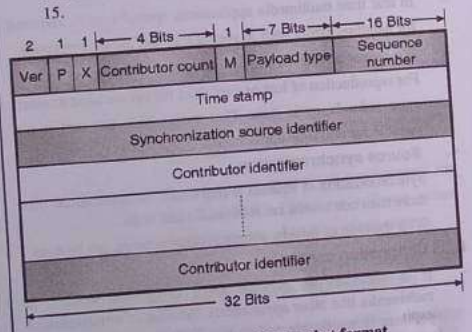
3. X : This is also a 1 bit field.

It indicates the presence of an extra extension header between the basic header and the data, if X = 1.

If it is set to 0, then there is no extra extension header.

4. Contributor count :

This is a 4-bit field. It is used for indicating the number of contributors. We can have at the most 15 contributors because a 4-bit field can have combinations between 0 and 15.



(G-743) **Fig. 14.10.2 : RTP packet format**

5. Marker (M) Field :

This is a 1-bit field called as marker which is used by the application to indicate, the end of its data.

6. Payload type :

This is a 7-bit field which is used for specifying the type of the payload. Different types of payload types have been defined so far.

Some common applications have been listed in Table 14.10.1.

Table 14.10.1 : Payload types

Type	Application	Type	Application
0	PCMM audio	7	LPC audio
1	1016	8	PCMA audio
2	G721 audio	9	G722 audio
3	GSM audio	14	MPEG audio

7. Sequence number :

This is a 16 bit long field which is used for numbering the RTP packets. The sequence number is chosen in a random manner for the first packet. It is incremented by 1 for each subsequent packet. The receiver uses the sequence number for detection of lost or out of order packet.

8. Time stamp :

This is a 32-bit field and it is used for indicating the time relationship between packets. A random number is used as the time stamp for the first packet. For each succeeding packets, the value of this field is equal to the sum of the preceding time stamp plus the time the first byte is produced (sampled). The value of the time tick is dependent on the application. For example the value of time tick is equal to 160 for the audio applications.

9. Synchronization source identifier :

This 32-bit field defines the source if there is only source. But in the event of presence of several sources, the mixer acts as the synchronization source and the other sources act as contributors. The protocol provides a strategy to resolve the conflict arising in situations like two sources start with the same sequence number.

10. Contributor identifier :

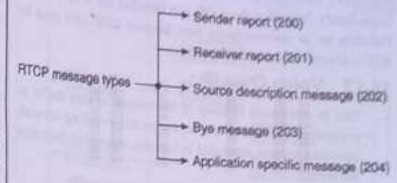
This is a 32-bit field. Thus each identifier is 32 bit long and each one defines a source. In the event of multiple sources present in a session, the mixer acts as the synchronization source and the remaining sources act as the contributors.

14.10.2 UDP Port :

- As stated earlier, RTP does not have any delivery mechanism despite being a transport protocol. Therefore practically RTP is treated like an application program and the RTP packets are encapsulated in a UDP user datagram. However there is no-well-known port is assigned to RTP, the way it is for other application programs.
- The UDP port can be selected as and when required but there is only one restriction. The **port number assigned to RTP must be an even number** because the next odd numbered port is used by Real time Transport Control Protocol (RTCP).
- Thus an even numbered UDP port is used temporarily by RTP.

14.11 RTCP [RTP Control Protocol] :

- RTP allows to usage of only one type of message. This message carries data from source to the destination. Many a times this single message type is sufficient but sometimes other messages also are required to be used.



(G-744) **Fig. 14.11.1 : RTCP message types**

- The function of these additional messages is flow control and quality control of data. Using these messages the recipient can send feedback to the source or sources.
- The protocol designed for this purpose is Real time Transport Control Protocol (RTCP). RTCP has five types of messages as shown in Fig. 14.11.1. The number written next to each box in the brackets specifies the type of the message.

1. Sender report :

All the active senders in a conference send the sender report periodically in order to report transmission and reception statistics for all RTP packets sent during the interval. The sender report consists of an absolute time stamp, which helps the receiver to synchronize different RTP message. The sender report is of particular importance when both audio and video are transmitted simultaneously. However note here that separate relative time stamps are being used by the audio and video transmissions.

2. Receiver report :

The receiver report is used for informing the sender and other receivers about the quality of service. This report is meant for passive participants i.e. those participants who do not send RTP packets.

3. Source description message :

The source description message gives additional information about the source which periodically sends it. This information can be in the form of e-mail address, telephone number or postal address of the owner or controller of the source.

4. Bye message :

In order to shut down a stream of data bits a bye message will be sent by the source. By sending the bye message the source to announce that it is leaving the conference. The other sources can detect the absence of a source but that would be an indirect announcement. This message is a direct announcement of a source leaving the conference. It is also very useful to a mixer.

5. Application specific message :

The application specific message is a packet for an application that wants to use new applications which are not defined in the standard. We can also use it to define a new message type.

Scanned by CamScanner

6. UDP port :

RTCP uses a temporary port and not a well known UDP port like RTP. The UDP port chosen for RTCP is always the one immediately following the UDP port selected for RTP. It must therefore be an odd-numbered port (because UDP port used by RTP is always an even numbered port).

14.12 Voice Over IP :

- Due to continuous increase in the volume of data traffic as compared to the voice traffic, the packet switching network operators became interested in carrying voice over their data networks.
- This is called as Internet telephony or voice over IP.
- The voice over IP is a real time interactive audio / video application. Voice over IP is also known as Internet telephony.
- In voice over IP, the Internet is used as a telephone network and some additional capabilities are included.
- Thus now a packet switched network is being used for the telephony application.
- We need to use the following specially designed protocols to handle this communication :

  1. SIP 2. H. 323

14.13 SIP (Session Initiation Protocol) :

- The session initiation protocol (SIP) was designed by IETF. It is an application layer protocol. SIP has been designed to establish, manage and terminate a multimedia session i.e. call. SIP can use either UDP, TCP or SCTP, for its operation.

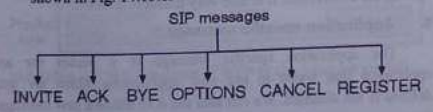
What does a SIP do ?

The SIP carries out the following tasks :

1. It provides the mechanism to establish a call between the caller and called party over an IP network.
2. It allows the caller to tell the called party that it wants to start the call. It also allows the participants to decide on media coding and end calls.
3. SIP provides a mechanism so that caller can determine the current IP address of the called party.
4. SIP also provides the required mechanism for call management.
5. SIP can create a two party, multiparty or multicast sessions.

14.13.1 SIP Messages :

- SIP is a text based protocol like HTTP. That means SIP uses messages just like HTTP. Six messages are defined for SIP as shown in Fig. 14.13.1.

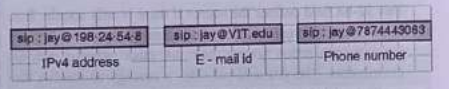


(G-1815) **Fig. 14.13.1 : SIP messages**

- Each message has got two parts namely a header and a body. A header would describe the following aspects :
  1. Structure of the message.
  2. Media type.
  3. Caller's capability.
- The caller uses INVITE message to initialises a session. After the called party responds to the call, the caller sends an ACK message as a confirmation of the call.
- A session can be terminated using the BYE message. The OPTIONS message is used to ask queries to a machine about its capabilities. The CANCEL message cancels an initialisation process which has already been started.
- The REGISTER message makes a connection when the called party is unavailable.

14.13.2 SIP Addresses :

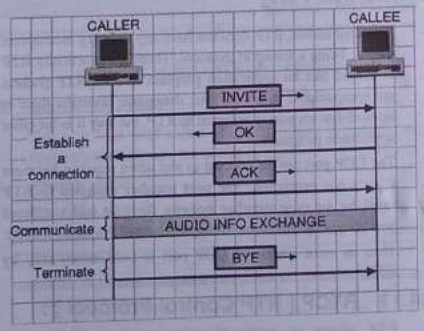
- In the conventional telephone system, the caller and receiver are identified only by their telephone numbers but in case of SIP we can use, an e-mail address, an IP address, a telephone number and 8 other types of addresses to identify the sender and receiver. However, these address needs to be in SIP formats.
- Various commonly used SIP formats are as shown in Fig. 14.13.2.



(G-1816) **Fig. 14.13.2 : SIP format**

14.13.3 Simple SIP Session :

- Fig. 14.13.2 demonstrates a simple SIP session which takes place in three steps :
  1. Establish a connection. 2. Communicate.
  3. Terminate the connection.



(G-1818) **Fig. 14.13.3 : Simple session of SIP**

1. Establish a connection :

To establish a session in SIP, a three-way handshake needs to take place. The caller sends an INVITE message, using UDP, TCP or SCTP to initiate the communication with the callee. If the called party wants to communicate then, she sends a reply message. The caller than sends back an ACK message, in order to confirm that he has received the reply code.

2. Communication :

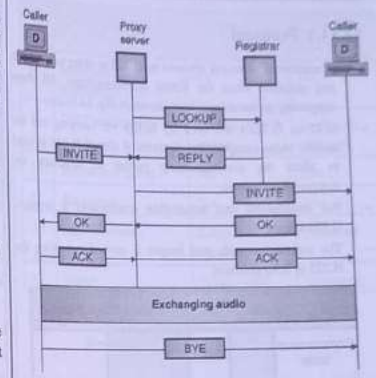
After establishing the session the caller and the called person can exchange audio using two temporary ports.

3. Terminating :

The session can be terminated by sending a BYE message by either the caller or the callee.

14.13.4 Tracking the Callee :

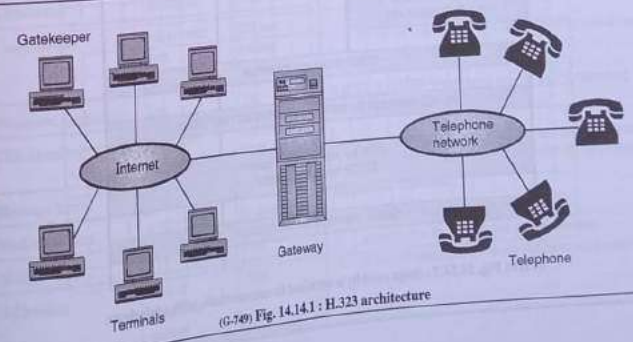
- What happens if the caller is not present at his terminal ? He may be away or at another terminal. His IP address is also not fixed if DHCP is being used.
- SIP can find the IP address of the other terminal at which the caller is sitting. The SIP make use of the concept of registration in order to track the callee.
- Some servers are defined by SIP as registrars. At any moment every user is registered with at least one registrar server and this server knows the IP address of the callee.
- Refer Fig. 14.13.4 to understand the tracking process of the callee. The caller can use the e-mail to contact the caller instead of the IP address in the INVITE message when he wants to start communicating with the callee.
- The message goes to the proxy server. The proxy server then sends a lookup message which is not a part of SIP to that registrar server which has the callee registered with it.
- As soon as a reply message from the registrar server reaches the proxy server it will take the caller's INVITE message and inserts the newly discovered IP address of the callee. This message is then sent to the callee. This is how the tracking process of callee is complete.



(G-748) **Fig. 14.13.4 : Tracking the callee**

14.14 H.323 :

- The general architecture of H. 323 is as shown in Fig. 14.14.1.
- H.323 is a standard designed by ITU in order to make the voice communication between the telephones on the public telephone network with the computers connected to the Internet, practically possible.
- Internet is connected to the telephone network via a gateway as shown. A gateway is a five layer device which makes the communication between one protocol stack to another, possible by translating the messages.
- The gateway used in Fig. 14.14.1 transforms the message from the telephone network to a message suitable for the Internet.
- The **gatekeeper** server connected in local area network as shown in Fig. 14.14.1 work as the registrar server.

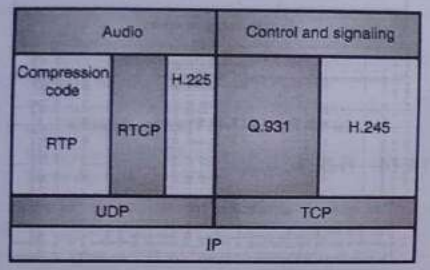


(G-749) **Fig. 14.14.1 : H.323 architecture**

Scanned by CamScanner

14.14.1 Protocol :

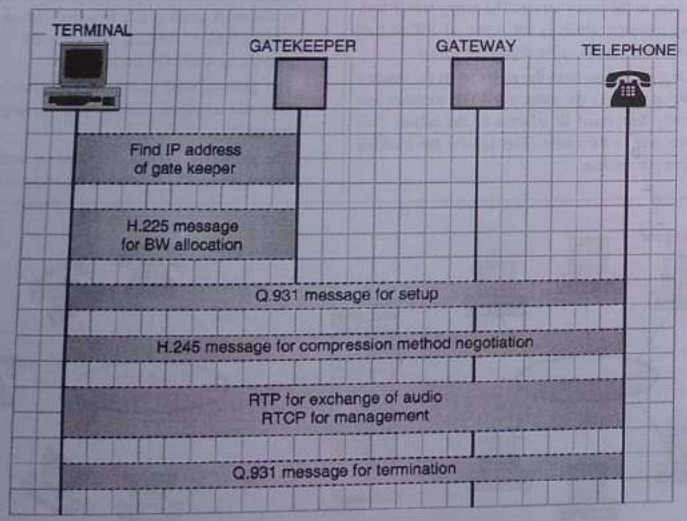
- A number of protocols are used by H.323 in order to establish and maintain voice (or video) communication. All these supporting protocol have been shown in Fig. 14.14.2.
- G.71 or G.723.1 are used by H.323 for carrying out the audio / video compression. A protocol named H.245 is used to allow the communicating parties to negotiate the compression method.
- For establishing and terminating connections a protocol Q.931 is used.
- The registration with gate keeper is carried out using the H.225 or RAS protocol.



(G-750) **Fig. 14.14.2 : H.323 protocol**

Operations :

- With a simple example we will demonstrate the operation of a telephone communications using H.323.
- Fig. 14.14.3 shows the stepwise procedure followed by a terminal to communicate with a telephone. So the terminal acts as the sender while the telephone works as a receiver in this example.
  1. The terminal, sends a broadcast message to the gatekeeper. The gatekeeper in response sends its IP address.
  2. The terminal communicates with the gatekeeper communicate. They negotiate bandwidth with the help of H.225 protocol
  3. The terminal, the gatekeeper, gateway and the telephone communicate with each other with the help of H.245 and negotiate the compression method to be used.
  4. The terminal, the gatekeeper, the telephone exchange the audio information with the help of RTP under the management of RTCP.
  5. The termination of connection can be exercised by the terminal, the gatekeeper, gateway and the telephone communicating with each other using Q.931 protocol.



(G-1817) **Fig. 14.14.3 : Steps used by a terminal to communicate with a telephone**

14.14.2 Comparison of H.323 and SIP :

- H.323 and SIP have many similarities but also some difference.
- Both of them allow the two party and multiparty calls using computers as well as telephones as the end points.
- Both support parameter negotiation, encryption and the RTP/RTCP protocols.
- Eventhough the features are similar, these two protocols differ basically in their philosophy.
- H.323 is a typical telephone industry standard. It specifies the complete protocol stack, defining specifically what is allowed and what is not.
- This is beneficial because it eases out the task of interoperability. But these advantages are at the cost of increased price, complexity and rigidity which cannot be accepted for future applications.
- SIP is a typical Internet protocol. It works by exchange of short ASCII text. It interworks well with other Internet protocols, but it does not work well with the existing telephone system protocols.
- Table 14.14.1 summarizes the similarities and differences between H.323 and SIP.

Table 14.14.1

Sr. No.	Parameter	H.323	SIP
1.	Designed by	ITU	IETF
2.	Compatibility with telephone networks	Yes	Largely
3.	Compatibility with Internet	No	Yes
4.	Architecture	Monolithic	Modular
5.	Completeness	Full protocol stack	SIP just handles setup
6.	Parameter negotiation	Yes	Yes
7.	Call signalling	Q.931 over TCP	SIP over TCP or UDP
8.	Message format	Binary	ASCII
9.	Media transport	RTP/RTCP	RTP/RTCP
10.	Multiple calls	Yes	Yes
11.	Addressing	Host of telephone number	URL
12.	Multimedia conferences	Yes	No
13.	Call Termination	Explicit or TCP release	Explicit or time out
14.	Instant messaging	No	Yes
15.	Encryption	Yes	Yes
16.	Implementation	Large and complex	Moderate
17.	Status	Widely used	Upcoming

14.15 Stream Control Transmission Protocol (SCTP) :

- SCTP is a new transport layer protocol. The multimedia and steam traffic is increasing day by day on the Internet.
- SCTP is a general purpose transport layer protocol which is designed to handle the multimedia and stream traffic.
- SCTP is a new reliable, message oriented transport layer protocol. The position of SCTP is between the application layer and network layer. It provides the interface between the application programs and the network operations.
- SCTP is designed mostly for the newly designed and recently introduced Internet applications. These new applications are as follows :
  1. H. 323 (IP telephony).
  2. SIP (IP telephony).
  3. H. 248 (Media gateway control).
  4. IUA (ISDN over IP).
- It is not possible to use TCP for these applications because they need more sophisticated service than that provided by TCP.
- SCTP is capable of providing the required services with better performance and reliability.

14.15.1 UDP Performance for Internet Applications :

- The following features of UDP are desirable when it is to be used for the Internet application like IP telephony.

Desirable features :

1. It is a message oriented protocol.
2. It conserves the boundaries of the message.
3. All UDP messages are independent of each other.

Scanned by CamScanner

- However UDP is not suitable for the applications such as IP telephony or real time data transmission due its following undesirable features.

Undesirable features :

1. UDP is unreliable. So the sender does not know anything if the datagram is lost or duplicated or discarded or received out of order.
2. No congestion control.
3. No flow control.

14.15.2 TCP Performance for Internet Applications :

Some of important desirable features of TCP are as follows :

Desirable features :

1. TCP is a byte oriented protocol.
2. TCP is a reliable protocol.
3. TCP can detect the duplicate segments.
4. In TCP the lost segments are resent.
5. Bytes are delivered in order.
6. TCP has flow control.
7. TCP has congestion control.

Undesirable features :

1. TCP does not preserve the message boundaries.

14.15.3 SCTP Performance for Internet Applications :

The important features of SCTP are as follows :

1. SCTP combines all the desirable features of UDP and TCP.
2. It is a message oriented protocol (like UDP).
3. It is a reliable protocol (like TCP).
4. It preserves the message boundaries (like UDP).
5. It can detect lost, duplicate or out of order data (like TCP).
6. It provides flow control and congestion control (like TCP).
7. SCTP has new features that are not available in UDP and TCP.

14.16 SCTP Services :

Following are some of the most important services provided by the SCTP to the application layer processes.

1. Process to process communication.
2. Multiple streams.
3. Multihoming.
4. Full duplex communication.
5. Connection oriented service.
6. Reliable service.

14.16.1 Process to Process Communication :

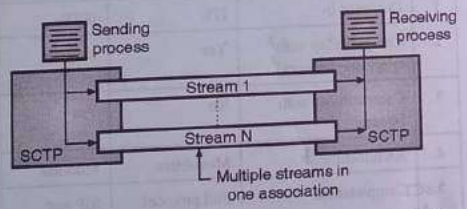
- All the well known ports in the TCP space are used by SCTP. But it uses some extra ports as well which have been listed in Table 14.16.1.

Table 14.16.1

Sr. No.	Protocol	Port number	Description
1.	IVA	9990	ISDN on IP
2.	M2UA	2904	SS7 Telephone signaling
3.	M3UA	2905	SS7 Telephone signaling
4.	H. 248	2945	Media gateway control
5.	H. 323	1718, 1719, 1720, 11720	IP Telephony
6.	SIP	5060	IP Telephony

14.16.2 Multiple Streams :

- TCP being a stream oriented protocol, each connection between a TCP client and a TCP server is a stream.
- If there is a loss at any point in the steam, the data will be blocked there and there will be no delivery of the remaining data.
- This problem is acceptable when the data is in the text form. But it is not acceptable when the data is real time video or real time audio data.
- This problem in TCP is overcome in SCTP by providing multiple steams in a single connection between a client and a server. This concept is similar to a multilane highway.
- Due to such multiple stream service in SCTP, the delivery of data does not get blocked. If one stream is blocked, the other streams can continue delivering the data.
- The concept of SCTP multiple stream service has been illustrated in Fig. 14.16.1.



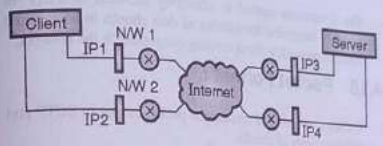
(G-2046) **Fig. 14.16.1 : SCTP multiple stream is one association**

- In SCTP, each connection is called as an association. Thus each **association** consists of multiple streams.

14.16.3 Multihoming :

- Assume that the sender and receiver hosts are **multihome** hosts. That means they are connected to multiple physical addresses with multiple IP addresses.
- In such a situation, if we use TCP, then the TCP connection involves only one source IP address and one destination address. Thus TCP does not support the multihoming services.

- However SCTP has been designed for providing multihome services. In an SCTP association the sending and receiving hosts can define more that one IP addresses at each end for an association.
- Thus multiple interfaces are established between the sending and receiving hosts in the same association.
- Multihoming is a **fault free** approach which ensures the data delivery without interruption.
- The concept of multihoming has been illustrated in Fig. 14.16.2 and it is very useful in the real time applications such as **Internet Telephony.**



(G-2047) **Fig. 14.16.2 : Concept of multihoming in SCTP**

- As shown in Fig. 14.16.2, the client has been connected to two different local networks with two different IP addresses.
- SCTP can allow an association between the client and the server using four different pairs of IP addresses.
- However the current SCTP version, it is possible to choose only one pair of IP addresses for data communication.
- The other pairs of IP addresses are used as alternatives only if the main choice fails. That means the current version of SCTP does not allow load sharing among different paths.

14.16.4 Full Duplex Communication :

- In SCTP also a full duplex service is offered, similar to TCP. That means the data can flow in both the directions simultaneously.
- SCTP at each end has a sending buffer and a receiving buffer and the packets are sent in both the directions.

14.16.5 Connection Oriented Service :

- SCTP provides a connection oriented service similar to TCP. An SCTP connection is called as an **association.**
- When a process at the site A wants to communicate with a process at the other site B, the sequence of operations in SCTP take place as follows :
  1. The SCTPs at sites A and B establish an association between them.
  2. A bidirection data transfer takes place.
  3. Terminate the association.

14.16.6 Reliable Service :

- SCTP also is a reliable transport protocol like TCP. It ensures the safe delivery of data with the help of acknowledgement mechanism.

14.17 SCTP Features :

- Let us understand the general features of SCTP and then compare them with the features of TCP.
- Some of the general features of SCTP are as follows :
  1. Transmission sequence number.
  2. Stream identifier.
  3. Stream sequence number.
  4. Packets.
  5. Acknowledgement number.
  6. Flow control.
  7. Error control.
  8. Congestion control.

14.17.1 Transmission Sequence Number (TSN) :

- In TCP the unit of data is **a byte** because it is a byte oriented protocol.
- Therefore TCP controls the data transfer by numbering bytes with the sequence numbers.
- However the data unit in SCTP is a **Data chunk** and it may or may not have a one to one relationship with the messages produced by the sending process. (This happens due to the fragmentation).
- Therefore in SCTP the **data chunks** are numbered with **transmission sequence number** (TSN) in order to control the data transfer.
- Each TSN is a unique 32 bit number which is stored in the header of the data chunk. TSN has a value between $(2^{32} - 1)$.

14.17.2 Stream Identifier (SI) :

- As stated earlier, in SCTP there are more than one stream in each association, and each such stream should be identified using a **Stream Identifier (SI).**
- The SI is a 16 bit number which starts from 0, and it is stored in header of the corresponding data chunk.
- This will help in placing the data chunk in its stream after receiving it at the destination.
- Thus SCTP uses SI to distinguish between different streams.

14.17.3 Stream Sequence Number (SSN) :

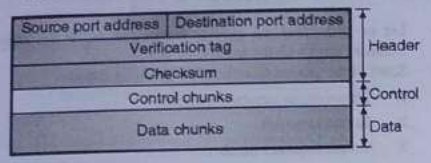
- SCTP uses the stream sequence number (SSN) to distinguish between different data chunks which belong to the same stream.
- The received data chunk at the destination is delivered to the appropriate stream in proper order by the destination SCTP.
- This becomes possible as SCTP defines each data chunk in each stream with stream sequence number (SSN) in addition to an SI.

14.17.4 Packets :

- The SCTP packet design is completely different than that of TCP. In SCTP, the data is carried in the form of data chunks while control information is carried as control chunks. Fig. 14.17.1 shows the SCTP packet.

Scanned by CamScanner

- The role of an SCTP packet is same as that of a TCP packet.



(G-2048) **Fig. 14.17.1 : An SCTP packet**

- In SCTP the control information is not a part of the header, but it is included in the control chunks. The control chunks are of different types.
- In SCTP the data is not treated as one entity. Instead it is in the form of several data chunks, and each chunk can belong to a different stream.
- There is no option section is SCTP like TCP. We have to define new chunk types to handle options in SCTP.
- The length of general header in SCTP is 12 bytes as compared to 20 bytes in TCP.
- The checksum length in SCTP is 32 bit as compared to 16 bits in TCP.
- The verification tag field in SCTP packet is used as an association identifier. Each association is defined by a unique verification tag. We can have multihoming in SCTP by using different IP addresses.
- In an SCTP packet several different data chunks will be present and each one is defined by TSN, IS and SSN.
- In SCTP, control information and data information are carried in separate chunks. In SCTP the TSN, IS and SSN numbers (identifiers) are used only to identify the data chunks. The control chunks never use these three identifier. In SCTP the data is contained in data chunks, streams and packets. The relationship between these three is as follows :
  1. An association may send many **packets.**
  2. Each **packet** may contain many **chunks.**
  3. These **chunks** may belong to different **streams.**

14.17.5 Acknowledgement Number :

- In TCP the acknowledgement numbers are byte oriented and they refer to the sequence numbers.
- But the acknowledgement numbers in SCTP are chunk-oriented, and they refer to the TSN.
- In SCTP, the control chunks carry the control information. The control chunks do not need the TSN.
- These control chunks are acknowledged by an other appropriate type of control chunk. The sequence number or acknowledgement number is not necessary for the control chunks in SCTP.

14.17.6 Flow Control :

- In SCTP, the receiver is prevented from overwhelming by implementing flow control.

14.17.7 Error Control :

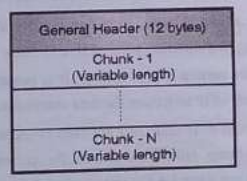
- SCTP provides reliability to data transfer by implementing the **error control** with the help of TSN numbers and acknowledgement numbers.

14.17.8 Congestion Control :

- The congestion control is inherently included in SCTP in order to determine the number of data chunks to be injected into the network without creating congestion in the network.

14.18 Packet Format :

- We are now going to discuss the packet format in SCTP and different types of chunks.
- Fig. 14.18.1 shows the SCTP packet format, which shows that an SCTP packet consists of two parts namely :
  1. A mandatory header and
  2. A set of blocks called chunks.

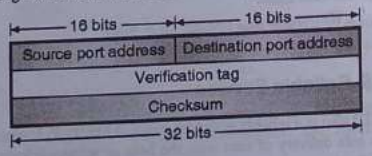


(G-2049) **Fig. 14.18.1 : SCTP packet format**

- In SCTP, there are two types of chunks :
  1. Data chunks and
  2. Control chunks
- An association in SCTP is controlled and maintained by the control chunks whereas the user data is carried by the data chunks.

14.18.1 General Header :

- The general header or packet header in SCTP is used for defining the end points of each association to which that packet belongs to.
- It also guarantees that the packet belongs to a particular association. It ensures that the integrity of the contents of the packet including the header itself is preserved.
- Fig. 14.18.2 shows the format of the general header.

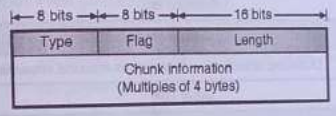


(G-2050) **Fig. 14.18.2 : General header**

- Following are the four fields in the general header.
  1. **Source port header :** This 16 bit field is used for defining the port number of the packet sending process.
  2. **Destination port number :** This 16 bit field is used for defining the port number of the packet receiving process.
  3. **Verification tag :** The contents of this 32 bit field will match a packet to an association. Due to this number a packet from a previous association is not mistaken as the packet in this association.
- In short, verification tag is used as an identifier for the association. In every packet during the association, the verification tag is repeated.
- For data transfer in forward and reverse direction, a separate verification is used.
  4. **Checksum :** This is a 32 bit field which contains a CRC-32 checksum. In the UDP, TCP and IP the checksum is 16 bit long. In SCTP it has been increased to 32 bits, in order to allow the use of CRC-32 checksum.

14.18.2 Chunks :

- As discussed earlier chunks carry either the control information or user data. The common layout of a chunk is as shown in Fig. 14.18.3.



(G-2051) **Fig. 14.18.3 : Common layout of a chunk**

- The first three fields i.e. type, flag and length are common to all types of chunks.
- But the chunk information field should be a multiple of 4 bytes. If it is not then additional zeros are padded up to make it a multiple of four bytes.

1. Type :

- This is an 8 bit field which is used for defining upto $2^8 = 256$ chunk types. Table 14.18.1 gives a list for chunks and their description.
- Note that all only a few types are actually defined till date. The remaining types have been reserved for future.

Table 14.18.1 : Chunks

Type	Chunk	Description
0	DATA	User data
1	INIT	An association is set up
2	INIT ACK	Acknowledgement for INIT chunk
3	SACK	Selective acknowledgement
4	HEART BEAT	Checks the peer for its liveness
5	HEAR BEAT ACK	Acknowledgement to HEART BEAT chunk
6	ABORT	Association is aborted
7	SHUTDOWN	Association is terminated
8	SHUTDOWN ACK	Acknowledgement to SHUTDOWN chunk
9	ERROR	Error is reported without shutdown
10	COOKIE ECHO	Third packet in association establishment
11	COOKIE ACK	Acknowledgement for COOKIE ECHO chunk
14	SHUTDOWN COMPLETE	Third packet in association termination
192	FORWARD TSN	For adjusting cumulative TSN

2. Flag :

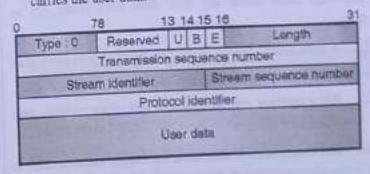
- This is an 8-bit field which is used for defining special flags needed by a particular chunk. The meaning of each bit is different for different types of chunks.

3. Length :

- The size of the information section depends on the type of chunk. Therefore it is necessary to define the chunk boundaries.
- **Length** is a 16 bit field which is used for defining the total size of the chunk, in bytes which includes the type, flag and length fields.
- If a given chunk does not carry any information then the value of length field will be 4 i.e. 4 bytes.
- Note that the length of padding, if any, is not included in the calculations of the length field. From this the receiver can find out the number of useful bytes carried by a chunk.
- If this value is not multiple of 4, the receiver will understand that padding (of 0s) has been done.

14.18.3 DATA :

- Fig. 14.18.4 shows the format of the DATA chunk which carries the user data.



(G-2052) **Fig. 14.18.4 : DATA chunk**

- A packet may contain zero or more data chunks. The type, length are the common field which we have already discussed.
- The contents of type field is 0. The flag field has 5 reserved bits and the remaining three defined bits U, B and E.

Scanned by CamScanner

- U stands for unordered field. If U = 1 it indicates the unordered data, and the value of the stream sequence number will be ignored.
- B stands for beginning and E for end. B and E bits together define the position of a chunk in the message which is fragmented.
- For B = E = 1 the message is not fragmented and one chunk will carry the whole message.
- The operation corresponding to the remaining combinations of B and E bits is as follows :

B	E	Operation
1	0	Carry the first fragment
0	1	Carry the last fragment
0	0	Carry the middle fragment

- The other fields with their description are as follows :

1. Transmission Sequence Number (TSN) :

- As shown in Fig. 14.18.4, this is a 32 bit field which is used to define the transmission sequence number.
- The INIT chunk will initialize this sequence number for one direction whereas the INIT ACK chunk will initialize it for the opposite direction.

2. Stream Identifier (SI) :

- This is a 16 bit field which is used to define each stream in an association.
- All the chunks that correspond to the same stream in the same direction would carry the same stream identifier (SI).

3. Stream Sequence Number (SSN) :

This 16 bit field is used for defining a chunk in a particular stream in one direction.

4. Protocol Identifier :

This is a 32-bit field which can be used by the application program for defining the type of data.

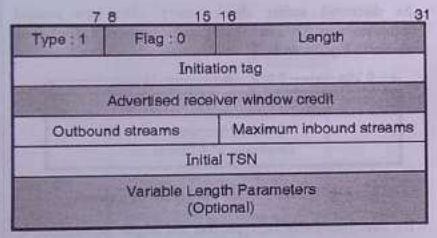
5. User Data :

- The user data is carried in this field. SCTP specifies very important rules about the user data field. They are as follows :
  1. A data chunk cannot carry data belonging to more than one message.
  2. But a message can be split and sent using multiple data chunks.
  3. The user data field can never be empty. It has to carry a minimum user data of one byte.
  4. Padding bits should be added if the data cannot end at a 32 bit boundary. These padding bits are not included while calculating the value of length field.
  5. As the data chunk has to carry a minimum data of 1-byte, the value of length field cannot be less than 17.

14.18.4 INIT :

- INIT chunk is an **initiation chunk.** The end point sends the INIT chunk as the first chunk to establish an association.
- The packet carrying the INIT chunk can carry only the INIT chunk. No data or control chunk can be carried by the packet carrying the INIT chunk.
- The value of verification tag is 0. The format of INIT chunk has been shown in Fig. 14.18.5.
- The values of the three common fields are as follows :

Field	Value
Type	1
Flag	0
Length	Minimum 20



(G-2053) **Fig. 14.18.5 : Format of INIT chunk**

- The format of INIT chunk is as shown in Fig. 14.18.5. The description of the fields other than the common fields is as follows :

1. Initiation tag :

- This is a 32 bit field which is used to define the value of the verification tag for the packets travelling in opposite direction.
- As stated earlier, the general header contains the verification tag for all the packets. For all the packets travelling in one direction, the value of verification tag will be the same.
- When the association is being established, the value of verification tag is determined.
- The value of this tag is defined in the initiation tag field by the end point which initiates the association.

2. Advertised receiver window credit :

- This is a 32 bit field which is used in flow control for defining the amount of initial data in byte that the sender of INIT chunk can allow to send.
- The **rwnd** value is used by the receiver to understand how much data is to be sent. Remember that the sequence numbers in SCTP are in the form of chunks.

3. Outbound stream :

- This is a 16 bit field which is used for defining the number of streams as suggested by the initiator of the association.

4. Maximum inbound stream :

- This is also a 16 bit field which is used for defining the maximum number of streams that the initiator of association is capable of supporting in the inbound direction.
- This number is the maximum possible value which cannot be increased by the other end point.

5. Initial TSN :

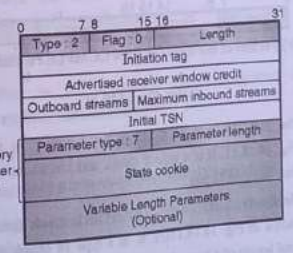
- This is a 32-bit field which is used for initialization of the transmission sequence number (TSN) in the outbound direction.
- Remember that every data chunk in an association must have only one TSN. The contents of this field is a random number less than 2^{32}.

6. Variable - length parameters :

- These are the optional parameters that may be added to the INIT chunk for defining the following :
  1. The IP address of sending end point.
  2. The number of IP addresses supported by the end point.
  3. The preservation of cookie state.
  4. The support of explicit congestion notification. (ECN).

14.18.5 INIT ACK :

- This is called as the initiation acknowledgement chunk and it is the second chunk sent during the establishment of association.
- The packet carrying this chunk can carry only this chunk and no other chunk such as the data chunk or control chunk.
- The value of verification tag for this packet which is located in the general header is actually the value of initiation tag defined in the received INIT chunk.
- Fig. 14.18.6 shows the format of INIT ACK chunk.

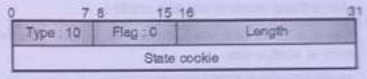


(G-2054) **Fig. 14.18.6 : INIT ACK chunk**

- Referring Fig. 14.18.6 you will notice that the fields corresponding to the main part of the chunk are same as those defined in the INIT chunk.
- However a point of difference between the two is that for this chunk a mandatory parameter is required.
- The mandatory parameter here is type 7 which defines the state cookie sent by the sender to this chunk.
- It is also possible to have some optional parameters in this chunk.
- The job of the **initiation tag** field in this chunk is to initiate the value of the verification tag for the packets travelling from opposite direction in future.

14.18.6 COOKIE ECHO :

- This chunk is the third chunk sent when an association is being established.
- This chunk is sent by the end point which receives an INIT ACK chunk. This end point is generally the sender of the INIT chunk.
- Fig. 14.18.7 shows the format of the COOKIE ECHO chunk. It is also possible to include the user data into the packet carrying the COOKIE ECHO chunk.

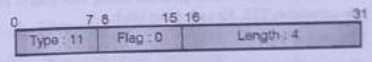


(G-2055) **Fig. 14.18.7 : Format of COOKIE ECHO chunk**

- From Fig. 14.18.7 it is evident that this chunk of type 10 is a very simple chunk.
- The state cookie that it has received in the INIT ACK chunk is as it echoed in the information field. The receiver of the INIT ACK cannot open the cookie.

14.18.7 COOKIE ACK :

- The fourth and last chunk sent during the establishment of an association is the COOKIE ACK chunk.
- The end point that receives a COOKIE ECHO chunk will send this chunk. We can include the user data in the packet that carries this chunk. It format has been shown in Fig. 14.18.8.



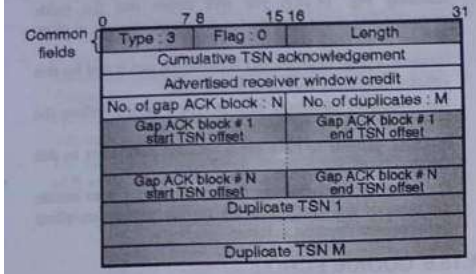
(G-2056) **Fig. 14.18.8 : Format of COOKIE ACK chunk**

- Remember that COOKIE ACK is a type 11 very simple chunk. The length of this chunk is always exactly equal to 32 bits i.e. 4 bytes.

14.18.8 SACK :

- The long form of SACK is selective ACK chunk, and it is used for acknowledging the receipt of data packets.
- The format of SACK chunk in Fig. 14.18.9.

Scanned by CamScanner



(G-2057) **Fig. 14.18.9 : The format of SACK chunk**

- We have already discussed about the three common fields i.e. type, flag and length earlier. This is the type 3 chunk. All the flag bits have been reset to 0. The other fields are as given below.

1. **Cumulative TSN acknowledgement :**

   As shown in Fig. 14.18.9, this is a 32 bit field which is used to define the TSN of the last data chunk received in sequence.

2. **Advertised receiver window credit :**

   This is a 32 bit field which contains the updated value for receiver window size.

3. **Number of gap ACK blocks :**

   - This is a 16 bit field which is used to define the number of gaps in the data chunk which is received after the cumulative TSN.
   - Note that **gap** does not mean the missing chunks however **gap** defines the sequence of received chunks.

4. **Number of duplicates :**

   This is a 16 bit field which is used for defining the number of duplicate chunks following the cumulative TSN.

5. **Gap ACK block start offset :**

   This is a 16 bit field which is used to give the starting TSN relative to the cumulative TSN for each group block.

6. **Gap ACK block end offset :**

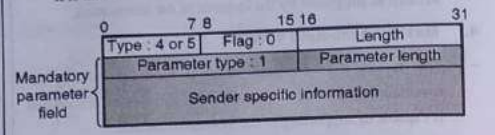
   This is a 16 bit field which gives the ending TSN relative to the cumulative TSN, for each group block.

7. **Duplicate TSN :**

   This is a 32 bit field, which gives TSN of the duplicate chunk of each duplicate chunk.

14.18.9 HEARTBEAT and HEARTBEAT ACK :

- These two chunks are similar except for one change i.e. the type field. The type of field is 4 for the HEART BEAT chunk while it is 5 for the HEARTBEAT ACK chunk.
- The format for both these chunks is as shown in Fig. 14.18.10. The function of both these chunks is to periodically probe the condition of an association.
- In order to do so, an end point sends the HEARTBEAT chunk. The peer sends back the HEARTBEAT ACK chunk if it is alive.

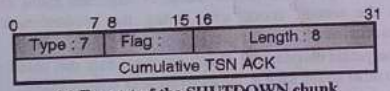


(G-2058) **Fig. 14.18.10 : Formats of HEARTBEAT and HEARTBEAT ACK chunks**

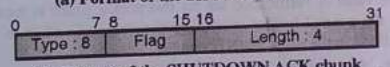
- The format of Fig. 14.18.10 can be divided into two parts namely : the three common fields and the mandatory parameter field which carries the sender specific information.
- For the HEART BEAT chunk this field contains the local time and the address of the sender. All this information is copied without any change into the HEARTBEAT ACK chunk.

14.18.10 SHUTDOWN, SHUTDOWN ACK and SHUTDOWN COMPLETE :

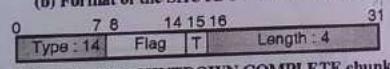
- SCTP uses these three chunks for closing an already established association, They are very similar to each other.
- The format of the SHUTDOWN chunk is as shown in Fig. 14.18.11(a). Its type is 7 and its length is 8 bytes.
- Out of these, the first four byes define the three common fields while the remaining four bytes define the cumulative TSN.



(a) Format of the SHUTDOWN chunk



(b) Format of the SHUTDOWN ACK chunk



(c) Format of the SHUTDOWN COMPLETE chunk

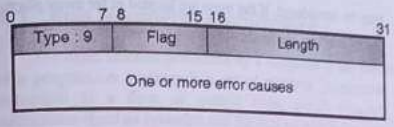
(G-2059) **Fig. 14.18.11**

- The SHUTDOWN ACK chunk has a format as shown in Fig. 14.18.11. It is a type 8 chunk and has a total length of four bytes or 32 bits.
- Finally, the SHUTDOWN COMPLETE chunk format is as shown in Fig. 14.18.11(c). It is a type 14 chunk and has a total length of 4 bytes. It also has a one bit flag i.e. the T flag.

- The T flag indicates that the sender does not have a TCB table.

14.18.11 ERROR :

- Fig. 14.18.12 shows the format of the ERROR chunk. On finding some error in a received packet the end point will immediately send the ERROR chunk.
- However even if an ERROR chunk is sent, it does not mean that the association is to be aborted. For doing so an ABORT chunk is required.

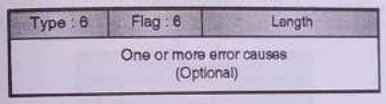


(G-2060) **Fig. 14.18.12 : Format of ERROR chunk**

- As shown in Fig. 3.28.12, ERROR is a type 9 flag.

14.18.12 ABORT :

- The format of the ABORT chunk is as shown in Fig. 14.18.13. It is a type 6 chunk.
- If an end point find a fatal error and needs to abort the association, then it will send the ABORT chunk.



(G-2061) **Fig. 14.18.13 : Format of the ABORT chunk**

14.18.13 FORWARD TSN :

- This chunk has been added very recently to the standard (RFC 3758). It will inform the receiver to adjust its cumulative TSN.
- A partial reliable service is provided by the FORWARD TSN.

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 ?

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

Q. 22 State and discuss various types of connectors.

Q. 23 Write a note on RTP and RTCP.

Q. 24 Which protocols are used for voice on IP ? Explain any one of them.

Q. 25 Write a short note on : Voice on IP.

Q. 26 Write short note on : Real time interactive protocols.

Q. 27 Write short note on : Rationale for new protocols.

Q. 28 State the requirement of transport layer for interactive real time multimedia.

Q. 29 To handle real time multimedia which protocol is used ?

Q. 30 Write short note on : Session initiation protocol.

Q. 31 Give types of SIP messages.

Q. 32 Explain SIP connection establishment.

Q. 33 Write short note on : H.323.

Q. 34 Give comparison between H.323 and SIP protocol.

Q. 35 Write short note on stream control transmission protocol.

Q. 36 Explain SCTP services.

Scanned by CamScanner

Q. 37 Explain process to process communication in SCTP.

Q. 38 State the features of SCTP.

Q. 39 With neat diagram explain SCTP packet format.

Q. 40 Write short note on : SCTP header.

14.19 University Questions and Answers :

Q. 1 Is there any relationship between transmission media and topology ? **(May 2014, 5 Marks)**

Ans. :

- The choice of transmission media and network topology are not independent of each other.
- A bus topology can use twisted pair, Broadband/baseband co-axial cable, optical fiber or wireless media. The choice of a particular transmission media depends on many factors such as; number of computers, the physical separation between them, need of expansion, bandwidth requirement, installation cost etc.
- If the number of users is large then use of optical fiber cable may be considered. If the users are located at far away places, use of wireless media should be considered.

□□□

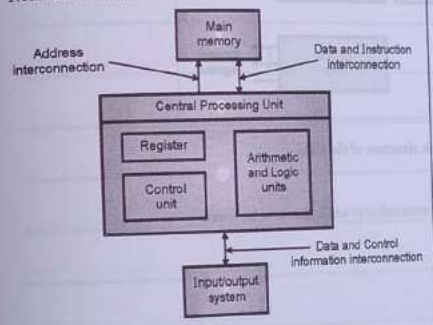
APPENDIX A Von Neumann Model

A.1 Von Neumann Architecture :

The basic function performed by a computer is the execution of a program. A program is a set of machine instructions. An instruction is a form of control code, which supplies the information about an operation and the data on which the operation is to be performed. A typical Von Neumann machine consists of five functionally independent units :

1. Input unit
2. Output unit
3. Arithmetic and logic units
4. Control unit
5. Memory unit

Fig. A.1.1 shows the basic structure of a conventional Von Neumann machine.



(CO-1.1)**Fig. A.1.1 : Structure of a computer**

A.1.1 Input Unit :

Computers accept coded information through input units, which read the data. The most common input device is the keyboard. Whenever a key is pressed, the corresponding letter or digit is translated into its corresponding code and sent to the processor. There are many other kinds of input devices like :

1. Mouse
2. Joysticks
3. Floppy drive
4. CD-drive
5. Modem

A.1.2 Output Unit :

Output unit sends processed result to outside world. The familiar example of such device is a printer. There are many other kinds of output devices like :

1. Video terminal
2. Floppy drive
3. CD-drive
4. Modem

A.1.3 Arithmetic and Logic Unit (ALU) :

Arithmetic or logic operations like multiplication, addition, division are performed by ALU. Operands are brought into the ALU, where the necessary operation is performed.

A.1.4 Control Unit :

Operations of ALU, memory and input and output units are coordinated and controlled by the control unit. Control unit sends control signals to other units. Data transfer between processor and memory are controlled by the control unit through timing signals.

A.1.5 Memory Unit :

Main memory is needed in a computer to store instructions and the data at the time of program execution. It was pointed out by Von Neumann that the same memory can be used for storing data and instruction. The memory unit stores all information in a group of memory cells as binary digits. Each memory location has a unique address and can be addressed independently. The contents of the desired memory locations are provided to the central processing unit by referring to the address of the memory location. The amount of information, which can be transferred between CPU and memory, depends on the size of the BUS connecting the two.

A.1.6 Key Features of a Von Neumann Machine :

- The Von Neumann machine uses stored program concept. The program and data are stored in the same memory unit. The computers prior to this idea used to store programs and data in separate memories. Entering and modifying these programs were very difficult as they were entered manually.
- Each location of the memory can be addressed independently.
- Execution of instruction in Von Neumann machine is carried out in a sequential fashion (unless explicitly altered by the program itself) from one instruction to the next.

A.1.7 Basic Structure of the CPU :

The design of CPU in modern form was proposed by John Von Neumann and his colleagues for the IAS computer. The IAS computer had a minimal number of registers along with the essential circuits. This computer had a small set of instruction and an instruction was allowed to contain only one operand address. Fig. A.1.2 gives the structure of IAS computer. The structure shown in Fig. A.1.2 consists of the following registers.

Accumulator (AC) :

It interacts with ALU and stores the input or output result.

Data Register (DR) :

It acts as buffer storage between the main memory and the CPU.

Scanned by CamScanner