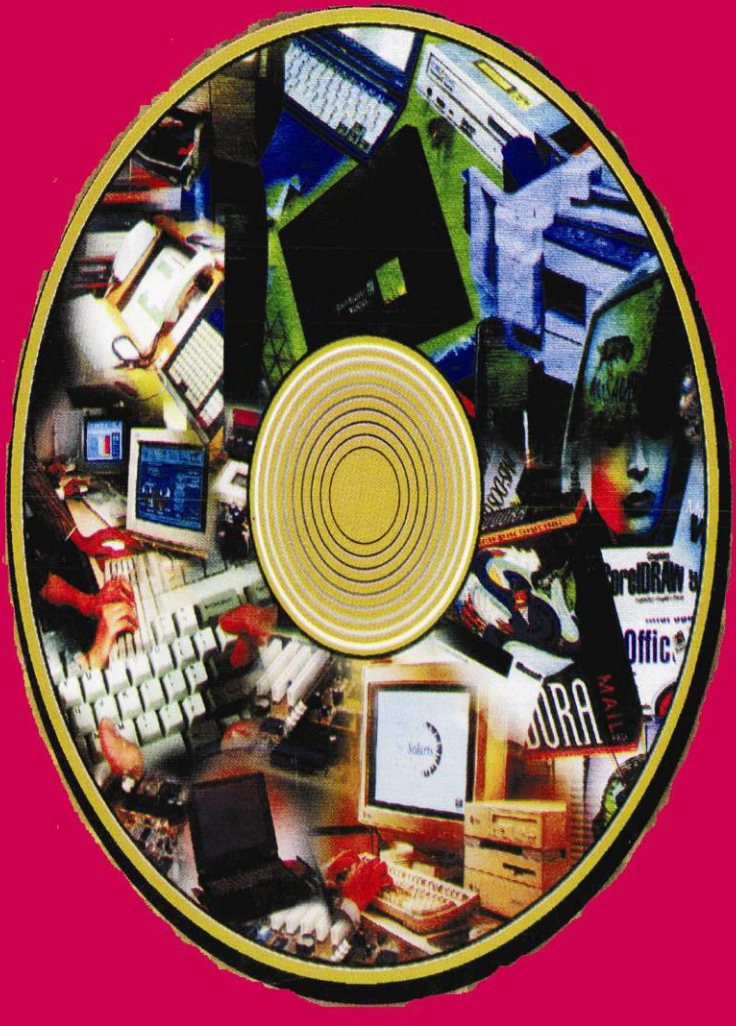
DATA COMMUNICATION AND NETWORKING



Copyright © 2009. Global Media. All rights reserved.

HIMALAYA PUBLISHING HOUSE

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:03:15.

DATA COMMUNICATION AND NETWORKING

C.S.V. MURTHY

B.Sc., B.E., MIE, Chartered Engineer,
Industrial Consultant,
Visiting Faculty at Various Management Colleges,
Bangalore, India.

Himalaya Publishing House

MUMBAI ● DELHI ● NAGPUR ● BANGALORE ● HYDERABAD

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:03:15.

© AUTHOR
No part of this book shall be reproduced, reprinted or translated for any purpose whatsoever without prior permission of the author and the publisher in writing.

ISBN : 978-93-5024-307-7
REVISED EDITION : 2010

Published by : Mrs. Meena Pandey
for **HIMALAYA PUBLISHING HOUSE,**
"Ramdoot", Dr. Bhalerao Marg, Girgaon,
Mumbai - 400 004.
Phones : 386 01 70 / 386 38 63
Fax : 022 - 387 71 78
E-mail : himpub@bom5.vsnl.net.in

Branch Offices :

Delhi : "Pooja Apartments", 4-B, Murari Lal Street, Ansari Road, Darya Ganj,
New Delhi - 110 002.
Phone : 327 03 92
Fax : 011 - 325 62 86

Nagpur : Kundanlal Chandak Industrial Estate, Ghat Road,
Nagpur - 440 018.
Phones: 72 12 15 / 72 12 16

Bangalore : No. 12, 6th Cross, Opp. Hotel Annapurna, Gandhi Nagar,
Bangalore - 560 009.
Phone : 22 86 611
Fax: 080 - 228 66 11

Hyderabad : No. 2-2-1 167/2H, 1st Floor, Near Railway Bridge, Tilak Nagar,
Main Road, Hyderabad - 500 044.

Printed at : Vicky Offset Press, New Delhi.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:03:15.

CONTENTS

UNIT - 1 1 - 116

1. **INTRODUCTION** 3 - 31

   Data Communication, Networks, Protocols and Standards, Standards Organisations

2. **BASIC CONCEPTS** 32 - 52

   Line Configurations, Topology, Transmission Mode, Categories of Networks, Internetworks

3. **THE OSI MODEL** 54 - 71

   Layered Architecture, Functions of the Layers

4. **SIGNALS** 72 - 89

   Analog and Digital, Analog to Digital, Digital to Analog

5. **ENCODING** 90 - 116

   Digital to Digital, Analog to Digital, Digital to Analog, Analog to Analog

UNIT - 2 117 - 206

6. **TRANSMISSION OF DIGITAL DATA : INTERFACES AND MODEMS** 118 - 148

   Interfaces and Transmission — Digital Data Transmission, DTE - DCE Interface, Standards

7. **TRANSMISSION MEDIA** 149 - 171

   Guided Media, Unguided Media, Performance

8. **MULTIPLEXING** 172 - 193

   Types, Telephone System

9. **ERROR DETECTION AND CORRECTION** 194 - 206

   Types of Errors, Detection, Correction

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 14:54:57.

UNIT - 3 207 - 296

10. DATA LINK CONTROL 208 - 222

Link Discipline, Flow Control, Error Control

11. DATA LINK PROTOCOLS 223 - 243

Asynchronous, Synchronous, Bit Oriented

12. LOCAL AREA NETWORKS 244 - 271

Project 802, Ethernet, Token Bus, Token Ring, FDDI

13. METROPOLITAN AREA NETWORKS (MAN) 272 - 280

IEEE 802.6, SMDS

14. SWITCHING 281 - 296

Circuit, Packet, Message, Network Layer

UNIT - 4 297 - 372

15. INTEGRATED SERVICES DIGITAL NETWORK (ISDN) 298 - 320

ISDN — Services, History, Subscriber Access, Layers, Broadband ISDN

16. X.25 321 - 331

Layers, Packet Layer Protocol

17. FRAME RELAY 332 - 339

Layers, Operation, Implementation

18. ASYNCHRONOUS TRANSFER MODE (ATM) 340 - 360

ATM — Design Goals, Topology, Protocol Architecture

19. SYNCHRONOUS OPTICAL NETWORK SONET/SDH 361 - 372

SONET/SDH — Physical Configuration, Layers, Sonet Frame, Multiplexing STS Frames

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 14:54:57.

UNIT - 5 373 - 489

20. NETWORKING AND INTERNETWORKING DEVICES 374 - 397

Repeaters, Bridges, Routers, Brouters, Gateways, Routing Algorithms

21. TRANSPORT LAYER 398 - 411

Duties, Connection, OSI Transport Protocol

22. UPPER OSI LAYER 412 - 432

Session Layer, Presentation Layer, Application Layer

23. TRANSMISSION CONTROL PROTOCOL (TCP)/INTERNET PROTOCOL 433 - 466

TCP/IP —Overview, Network Layer, Transport Layer, Application Layer

24. EMERGING TECHNOLOGIES COMPUTER TELEPHONY AND IP TELEPHONY 467 - 492

IP Telephony, Voice and Data, Computer Telephony, Unified Messaging, Call Centre Technology

REFERENCES 491 - 492

INDEX 493 - 499

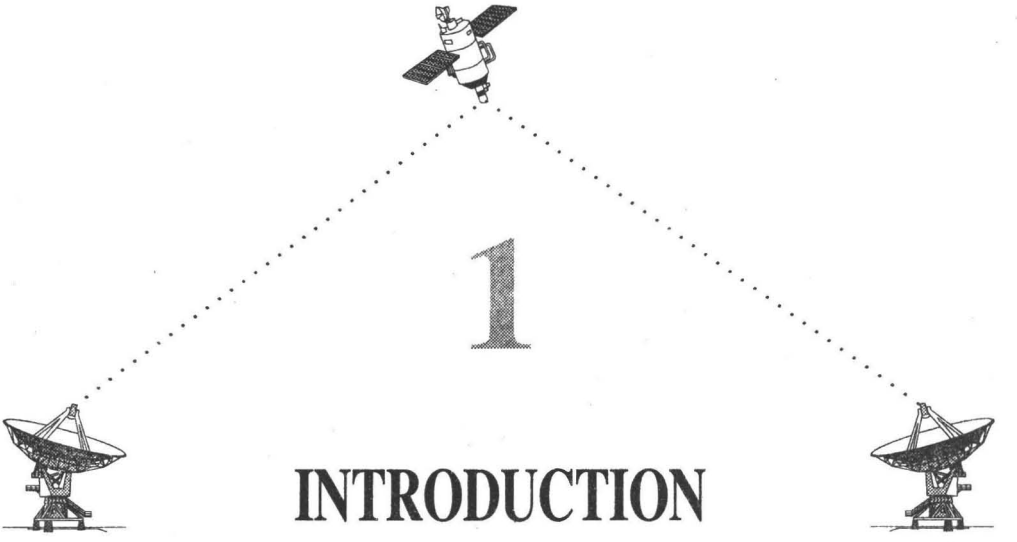
Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 14:54:57.

"This page is Intentionally Left Blank"

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 14:54:57.



1

INTRODUCTION

1.1 DATA COMMUNICATIONS

Data

Data is the raw material from which useful information is derived. The word Data is the plural of Datum. Data is commonly used in both singular and plural forms. It is defined as raw facts or observations, typically about physical phenomenon or business transactions. Example: A sale of a machine tool or an automobile would generate a lot of data describing those events. Data are objective measurements of attributes (the characteristics) of entities (such as people, place, things and events). These measurements are usually represented by symbols such as numbers, words, codes, composed of a mixture of numerical, alphabetical and other characters. It takes a variety of forms, including numeric data, text, voice and images.

Data is the collection of facts, which is unorganised but can be made organised into useful information. The term Data and Information come across in our daily life and are often interchanged. Example: Dates, weights, prices, costs, number of items sold, employees' names, product names etc.

Information

The data which has been converted into a useful and meaningful form is *information*. As already mentioned, the terms data and information are used interchangeably. *Data* are raw material resources that are processed into finished information products. *Information* can be defined as data that has been converted into a meaningful and useful context for specific end-users. Data is usually not useful until subjected to a *Value added* process where:

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

(i) Its form is aggregated, manipulated and organised.
(ii) Its content is analysed and evaluated.
(iii) It is placed in a proper context for a human user.

Information is processed data, placed in a context that gives it value for specific end-users.

Data processing

The conversion of facts into meaningful information is known as *data processing*. It is also called in general as *information processing*. It is the processing of data to make it more usable and meaningful, thus transforming it into information.

Data communications

It refers to the transmission of computerized data from one location to another. Computers transmit data for many reasons.

(i) One is the need to transfer information from one storage location to another within primary memory or primary memory to either the arithmetic logic unit or the supervisory control unit.
(ii) Another is the need to transfer data from the CPU to peripheral devices. E.g. floppy disks or printers.
(iii) Many businesses need to transfer data from one local computer to another or from local data terminals to distant main frame computers.

Microcomputers also employ data communications. Ex: Many businesses tie their microcomputers together in Local Area Networks (LANs) to facilitate electronic mail or to share printers or other computer resources. Private microcomputer users also rely on data communications, when they phone time-sharing, computer shopping, airline reservation, and financial information services. In the near future, these uses probably will expand as both individuals and large organisations send pictures, advertise services, and perform daily tasks using data communications.

Methods of data communications

Through computers, business often find it convenient to exchange data eg: To consolidate the data from several branch offices into a single financial statement. The problem faced by today's companies is how to transmit such data in a cost effective manner. Telephone lines are one possibility, but newer technologies, such as a microwave and satellite data transmission, can often accomplish the same thing without physical enabling.

Two types of transmissions are:

(i) *Internal* (refers to the transfer of data within a computer).
(ii) *External* (refers to the transfer of data to either local peripheral equipment say printers or remote computers).

Tele-communication system

The following figure 1.1 shows a simple tele-communication system networks. Let us take a small mail order catalog firm situated at Bangalore linking the firms head office at Bangalore with its branch office at Delhi, having a small mini computer and a printer.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

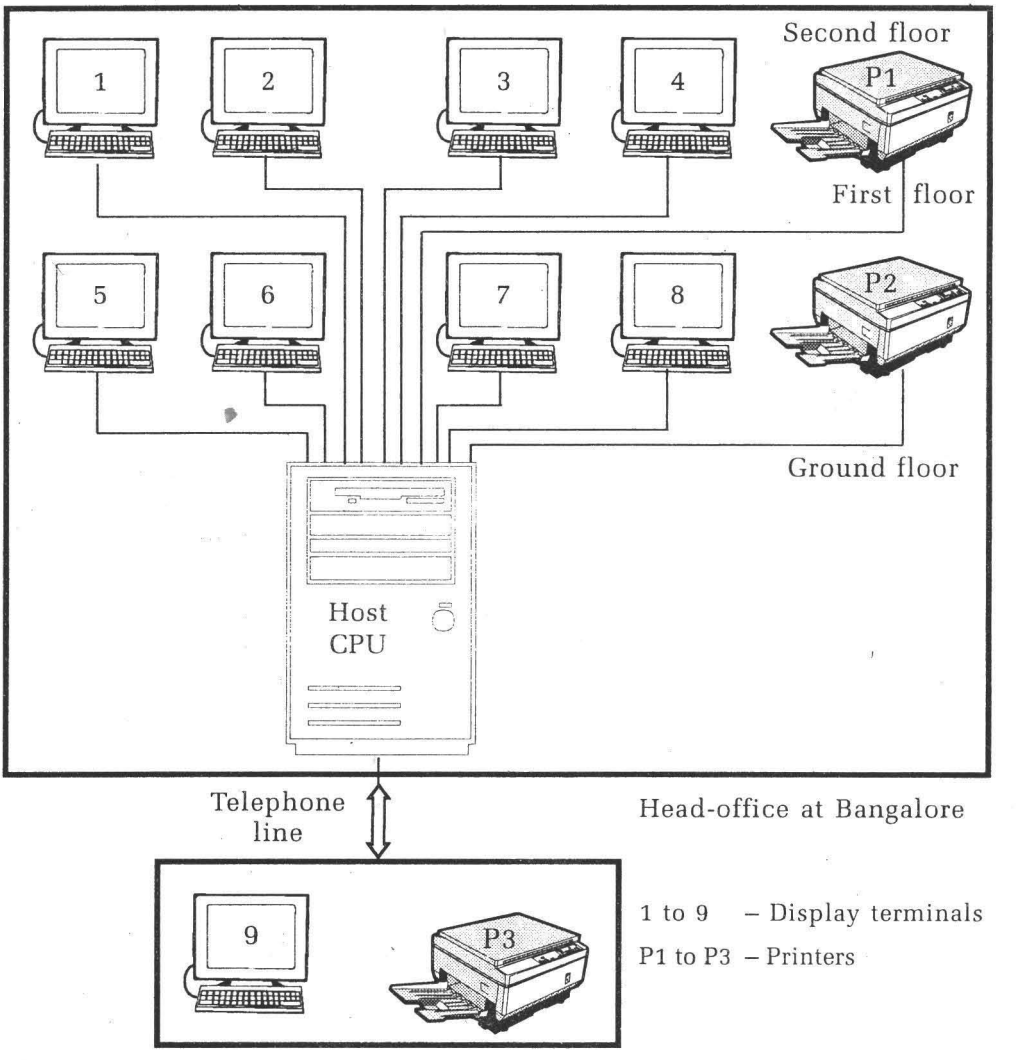


Fig. 1.1 Tele-communication system for a mail order catalog firm

Each day, the firm processes nearly 1000 phone and mail orders from its customers. At Bangalore head-office, eight display terminals and two printers are configured to the mini. The computers storage device contains, among other normal things up-to-date data on product prices, quantity of items in stock and the firm's customers. Authorised personnel may draw *on* any of these data in the course of processing an order.

When head office receives an order, an order clerk keys data into a display terminal. The clerk checks such things as the requested items are in stock, the item's latest prices and customer's credit status. Once all these details are in order, an electronic order is prepared and sent to the branch office at Delhi where a small *warehouse* is available to cater to the customers of north. Two printers are available at the head office site for billing, preparing out of stock notices to customers and various other purposes.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

At the Delhi office, personnel use a display terminal to check the order log and update stock counts as soon as products are received from vendors or shipped out to customers. All data keyed at the Delhi office display terminal are transmitted over ordinary phone lines and are processed by the Bangalore head quarters computer. A printer is also available at Delhi branch office to prepare packing lists or invoices in hard copy form. Such documents are placed in a shipping envelopes to the customer that is attached to the top of the carton containing the order.

Communication system elements

A tele-communication network shown above as an example in figure 8.1 consists of the following elements.

(i) A certain computer called the host computer (or host) handles the processing.

(ii) Peripheral devices (Display terminals) send data to or receive data from the host computer.

(iii) Communication media transmit the data. In this example, it is the ordinary telephone that carry the data between the remote Delhi branch office and the host CPU at Bangalore and special cables link the peripherals of the head office at Bangalore to the host.

(iv) Devices called modems convert computer signals into a form compatible with the phone lines and vice versa.

(v) Communications management devices optimise the flow of messages and from the CPU.

In some of the networks we do not find a host computer. There may be devices that are capable of providing input, output, processing or storage can serve as a terminal on a network. Besides the traditional display terminal among the most widely used type of terminals found today in communication networks are personal computer work stations, direct access storage devices, touch-tone phones, FAX machines, high speed printers and copiers.

A simple communication system will be as follows:

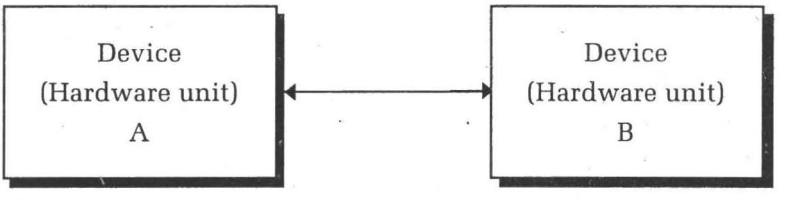


Fig. 1.2 Communication system

Two devices which are located at a distance from each other transfer messages over some types of communication media like

- *Physical lines :* Twisted wire pairs, coaxial cable and fiber optic cable.
- *Microwaves :* Terrestrial microwave stations, communications satellites.

The first one can be called as *bounded* media. The second one can be called as *unbounded* media.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

Communications model

Communication is essentially a *perceptual* process. The sender must encode intended meaning to create messages. The receiver then decodes messages to obtain perceived meaning. Effective communication depends on the sender and receiver sharing an understanding of the rules used to encode meaning into message. Feedback can be used to help sender and receiver find time that shared understanding.

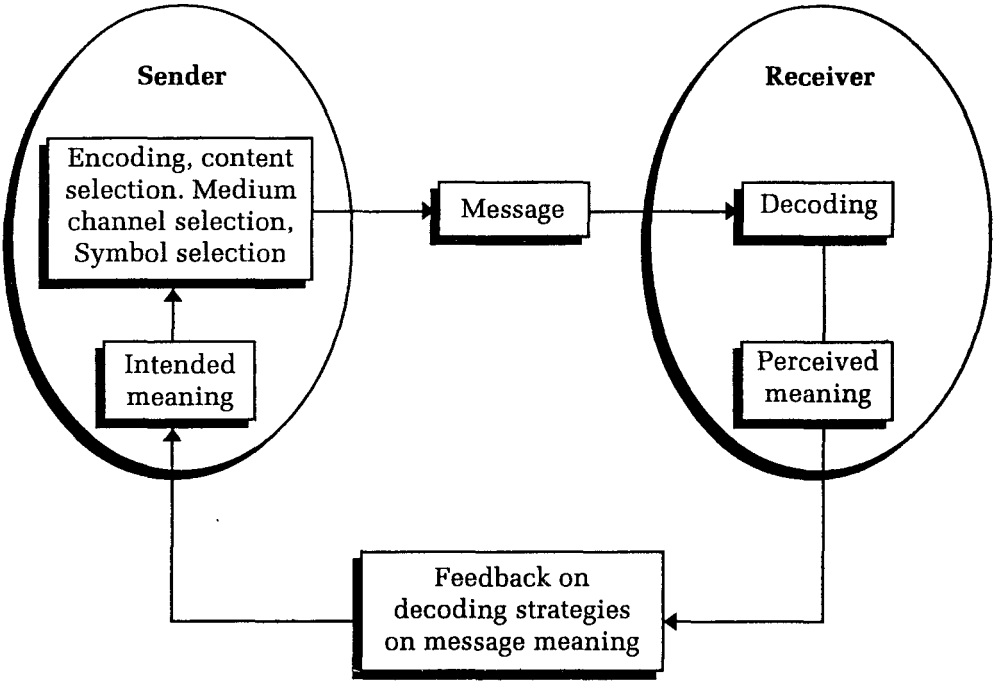


Fig. 1.3 Communication model

The basic communication media

People engage in electronic transmissions. If person A is sending a message to person B, A does not talk directly to.B. The process is complex involving multiple layers of intermediary hardware, software and transmission services. This process is called *mediated* because of no direct interaction, but only through the mediation of:

- Software
- Computers
- Transmission technologies

The key to mediated communication is 'standards' expectations of how people (and technology) are to behave when they communicate. In data communications, technical layer standards have to be multivendor standards so that products from different vendors can work together.

(i) Person A sends a message to B through mediated communication (standard in English)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

(ii) Person A uses electronic mail program 1, while person B uses e-mail program 2 from a different vendor,

(iii) Program 1 works on computer S. Program 2 works on a different computer T.

(iv) Computer S has transmission process x, which attaches the computer to network Alpha. Computer T attaches to network Beta via transmission process y.

There must be standard for communication at all four layers.

- The user Layer - English is the standard

Standards are also needed in the other 3 levels.

Data communication system components :

- *Message* — pictures, numbers, text, sound, video or a combination of such items.
- *Sender*] computer, workstation, telephone, handset
- *Receiver*] videocamera etc.
- *Medium* — twisted pairwire, coaxial cable, flat or ribbon cable, files, optic cable, laser, radio waves, microwaves etc.
- *Protocol* — A set of rules that govern data communication.

Data communication is the exchange of data with binary digits in the form of 0s and 1s between two devices through a transmission medium.

Data communications are grouped as :

- *Local* (if the communicating devices are close by - in the same building or in a restricted area).
- *Remote* (if the communicating devices are situated apart).

The data communication will be effective if the following three fundamental characteristics are achieved by the system :

- *Delivery* – To the correct destination.
- *Accuracy* – To deliver data accurately.
- *Timeliness* – To deliver data at the appropriate time (immediately when it is produced, in the same order that they are produced and without much delay). This is also termed as real-time transmission.

Definition

As per Jerry Fitzgerald, *data communications* is the movement of computer information from one point to another by means of electrical or optical transmission systems. Such systems often are called data communication networks. This is in contrast to the broader term tele-communications, which includes the transmission of voice, video (images and graphics) as well as data.

Data communications is principle enabler of the rapid information exchange and will become more important than the use of computers themselves in the future.

Eg. : Wal-mart uses data communications extensively, can gain significant competitive advantage in the market place.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

Data communication networks are established :

- to collect data from remote points (terminals or microcomputers).
- to transmit that data to a central point with a more powerful microcomputer or a main frame or minicomputer.
- to perform the reverse process alternatively.
- to combine some of the two.
- to facilitate more efficient use of central computers (mainframe, micro or mini).
- to improve the day-to-day control of a business by providing faster information flow.
- to provide message transfer services to allow computer users to talk to one another via electric mail.
- to offer better and more timely interchange of data among their users.
- to bring the power of computers closer to more users.

Objectives of data communication networks

The objectives are :

- to reduce the time, effort and cost required to perform various business tasks.
- to capture business data at its source and rapidly disseminate it.
- to support improved management control of the organisation.

Types of data communication systems

There are 8 types of data communication systems :

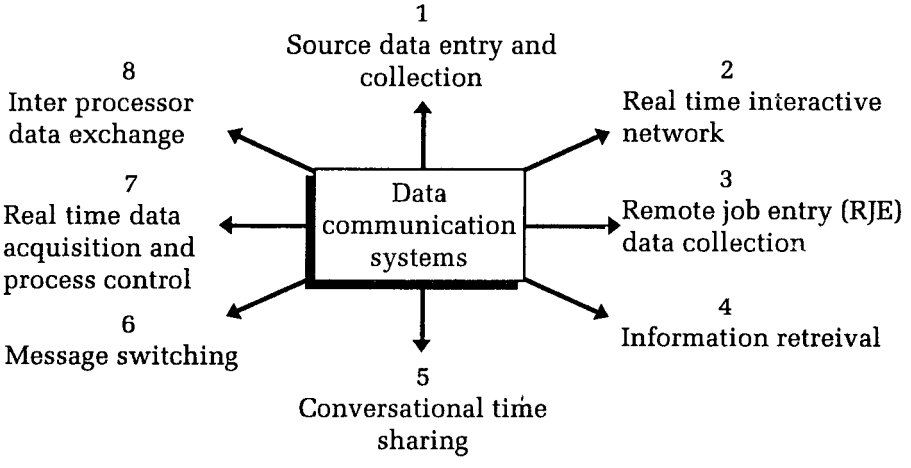


Fig. 1.4 Data communication systems

Networks today are more complex, because they are used for multiple tasks.

1.2 NETWORKS

The computers and communications when the merged will influence, the way the computer systems are organised. In the earlier days, a single computer (of the old model) is used to serve all of the organisations computational needs. This has been replaced, in the recent days by a large number of separate but inter-

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

connected computers, which perform the same job in a better and faster way. These systems are called *Computer networks.* Computer network means an interconnected collection of autonomous computers. These computers (minimum two) are said to be interconnected if they are able to exchange information. The connection need not be physically through a wire. Even fiber optics, microwave, communication satellites can be used. If one computer could influence the other in starting, stopping or controlling, the computers are not autonomous. Hence a system having one control unit and many slaves is not a network.

A *network* connects a variety of terminals and computers. Given the various communication options, one can configure a network of computers and terminal devices in any number of ways.

Networks use distributed processing, wherein a task is divided among many computers. Instead of one large machine held responsible for all aspects of a process, the same is done by individual separate computers (say PC or Work station) which handles portion of the task.

Advantages found in this method are:

- *Security/encapsulation :* A user will have a limited accessibility only to a certain portion of the total database e.g.: Automated teller machines in banks.
- *Distributed database :* No need to have full storage capacity for the entire database. E.g.. Worldwide Web provides users access to information that may be actually stored and manipulated anywhere on the internet.
- *Problem solving is quick :* It is understandable that a number of computers working on parts of a total problem concurrently could solve the problems faster than a single machine working on the entire problem.
- High degree of cohesiveness and transparency.
- Exsistence of multiple autonomous computers is transparent (not visible) to the user. He can type a command to run a program and it runs.

User is not aware of multiple processors and it looks to him as though there is a virtual uniprocessor.

In a network, users must explicitly log-on to one machine, explicitly submit jobs remotely.

Distributed System	Networks
• It is a software system built on top of network. The software gives a high degree of cohesiveness and transparency.	• The distinction between a network and distributed system is with the software (especially OS) instead of hardware.
• The difference between the network and distributed system, though both need to move files, question is who invokes the movement, the system or the user?	—
• This existence of multiple autonomous computers is transparent (not visible to the user.) Only a command is to be	—

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

typed to run a program. It is upto the operating system to select the best processor, transport all the input files to that processor and put the results in the correct place.	
• The user of a distributed system is not aware about multiple processors. Looks to him as though it is a virtual uni-processor. Functions like allocation of jobs to processors, files to disks, files movement between storage to the need places, all system functions are carried out automatically. Here, no explicit working. All automatically done by the system, without the user's knowledge.	• Users must explicitly log-on to one machine, explicitly submit jobs remotely, explicitly move files around and generally handle all the net work management personally.
• Advantages are: – Security/encapsulation, distributed databases, quick problem solving, security through redundancy, collaborative process (i.e. both multiple computers and multiple users may interact on a task.)	• Network criteria are the performance, reliability and security. Under performance number of users, transmission medium type, types of hardware & software are the prominent ones. In reliability, frequent occurrences of failure, recovery time after a failure, protection from catastrophic ones are important. • Under security, unauthorised access and viruses are the ones to be considered. • In networks, the various issues involved are – Resource sharing – Provides high reliability – Money saving – Scalability – Communication medium – Access to remote information (world wide web etc.) – Interactive entertainment (Films live television, game playing etc) – User to user communication (through e-mail, video conference, worldwide news groups) – Social issues (allows citizen to express their views in different ways to different audience that was not possible earlier)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

Network applications

Data communication networks have wide range of applications.It is indispensable part of business, industry and entertainment. Some of them are as shown in the figure 1.5.

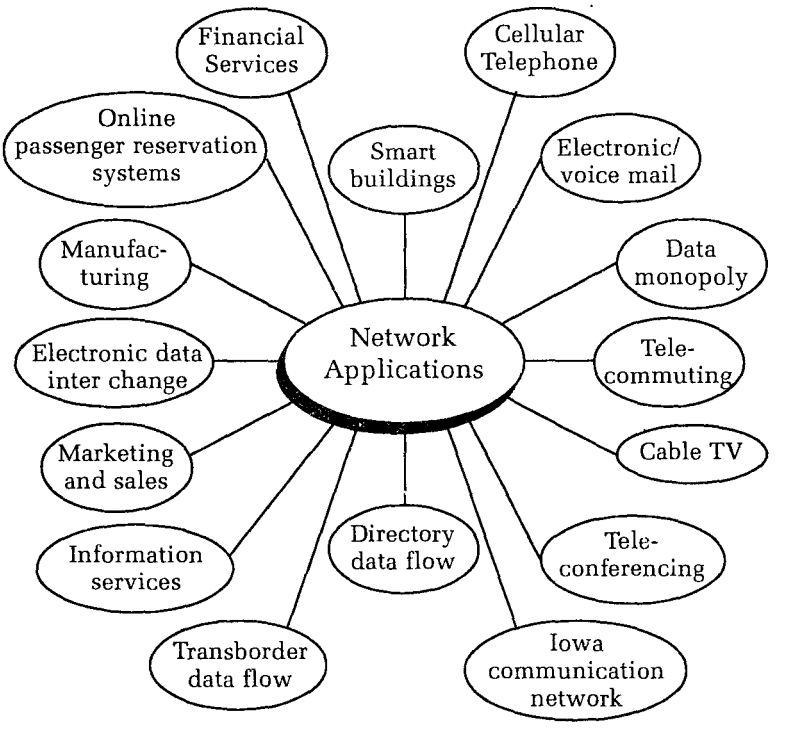


Fig. 1.5 Network applications

Smart buildings : New buildings contain wiring of different uses such as electricity, data/voice communication, image processing and many control systems required in big office buildings. A smart building consists of many automated systems and their associated electrical/net work wiring.

Cellular Telephone : Cellular 'wireless phone connections instead of physical connection as in telephone system can be used to maintain wireless phone connections even while travelling long distances.

Electronic/voice mail : Electronic mail has grown both in business sector and between the homes of individuals who own microcomputers. Voice mail will be growing more as special common carriers and telephone companies offer voice storing and forwarding systems and as more organisations put voice mail software on their networks.

Data monopoly : Further to transborder data flow, it is possible to have an intercompany data flow problem within a single

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

country. The question is that of a data monopoly within a specific country. Example: Airline reservation system; If travel agents scroll through different screens to locate competing carrier flights, they may select those flights that are easy to access, as some of the airlines have a monopoly. The world's first legal issues involves a data monopoly in our information based society.

Telecommuting : Here, the employees perform most of the work at home instead of going to the office each day. Saving of time in dropping to the work place, improved quality of life, optimised scheduling of both your work and personal life, less stress, monetary savings on both clothes and travel, greater time flexibility, higher level of concentration at home are the advantages. At home diagnoses of information systems or data communication problems would be convenient. Telecommuting is much faster than a long unnecessary drive by car.

Cable Television : In future, the services on cable TV may include: Video (on request); Financial and communication services provided by the telephone companies and computer networks.

Tele-conferences : In USA, teleconferencing is one of a major activities.

- More than 20 million meetings are held every day.
- 75% of these meetings last less than 30 minutes.
- 50% of all meetings are handled by voice communication only.
- 90% of the American airlines travel is for business.

In view of this, video conferencing is on the increase. People, from different geographical locations can attend business meeting in both voice and picture format. Documents can be seen and copied at remote locations.

IOWA Communication: Network (ICN) (through fiber optics) In IOWA, the implementation of the ICN is for schools, hospitals, criminal justice system, telemedicine, telepathology, teleradiology, distance learning, telejustice. Its conversion of voice, video and data signals into digital light impulses that are transmitted over hair thin glass fibers throughout the state. It has in its fold 105 schools & colleges, three prisons, an armory of three hospitals (cost of $ 97.5 million) - 200 miles it can operate for the teacher to know what is happening in the distant class rooms. It plans to bring on-line further 100 more schools, libraries and state agencies.

Directory services : It allows list of files to be allowed in a central location for the speedy world wide search of data.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

Transborder data flow	: Flow or movement of data across their national boundaries. USA has no restriction, but only limits transborder data flow to the countries who are less friendly by restricting the sale or delivery of some technological equipment or information. Each country has its own directives. France considers taxing data. Sweden has set up a data inspection board who would approve for export of data files etc.
Information Services	: This includes bulletin boards and data banks. Worldwide web is also an information service.
Marketing and Sales	: Marketing professionals use networks for collection, exchange and analyse data for the customer needs in areas of product development, tele-shopping. Order processing on line reservation services etc.
Electronic data interchange	: Exchanges business information between computers (paperless transmission between companies of order invoices and other business documents) of different companies. Transactions are done electronically, can be viewed on a microcomputer's video screen or on a printed format.
Manufacturing	: Networks can be used in many manufacturing areas including the manufacturing process. Application areas are CAD (Computer aided design) CAM (Computer aided manufacturing), CIM (Computer integrated manufacturing) which allows multiple users to work on a project simultaneously.
Financial Services	: Computer networks are intensively used in: • Credit history searching • Foreign exchange and investment services • Electronic funds transfer (EFT) includes ATM (Automated teller machine), automatic paycheque deposit etc.

1.3 PROTOCOLS AND STANDARDS

Protocol

It is a set of rules and procedures that govern transmission between the components in a network. A *protocol* is a statement that explains how a specific task, such as transferring data, will be performed. Reference models and protocols become standards when they are approved by important standard - setting groups or when industry builds or buys products that support the models and protocols. When the computer or an internet is used, a set of rules and regulations may have to be observed. The common rules are called *protocols*. In the earlier days, *protocols* referred to the customs and regulations dealings with diplomatic formality, precedence and etiquette. The same definition holds good even in the case of computing.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

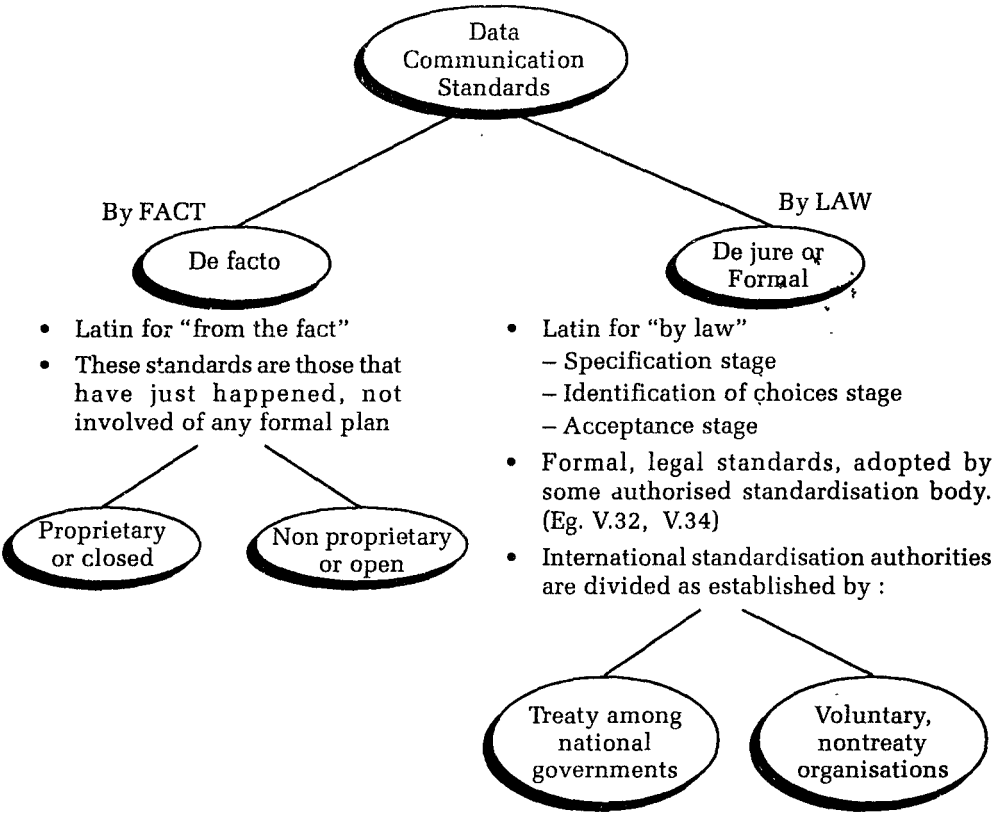


Fig. 1.6 Data communication standards

Example of De facto standards for small office computers are IBM's personal computers, as most of the manufacturers have chosen to copy IBM's machines closely. Similarly UNIX is also de facto to standard for operating systems used extensively in university computer science departments. The difference between proprietary and non proprietary standards are:

- *Proprietary standards :* are the ones which are originally invented by the commercial organisations to operate its products which could form the basis (Also known as closed standards since they close off communications of the systems produced by different vendors).
- *Non proprietary standards* are the ones which are originally developed by various groups or committees that have been introduced for the benefits of the public (known as open standards as they open communication between different systems).
- *Formal standards* takes many years to develop during which time, a new technology might have ushered in making the old technology less appealing. Defacto standards emerge in the market place and supported by several vendors who have no official standing. E.g. Microsoft Windows.
- *Defacto standards* become formal standards when once it is accepted as found in the telecommunication industry.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

A *telecommunications network* contains diverse hardware and software components that need to work together to transmit information. Different components in a network can communicate by adhering to a common set of rules that enables them to talk to each other. This set of rules and procedures of governing transmission between two points in a network is a *protocol.*

Dissimilar devices cannot communicate with each other unless a strict set of communications standards is followed. Such standards are commonly referred to as *protocols.* A *protocol* is a set of rules required to initiate and maintain communication between a sender and receiver device. Protocol specify whether asynchronous or synchronous transmission will be used, how data will be packaged and recognised, and what error-handling procedures will be used. When networks are designed and built, a collection of standard protocols are generally chosen and packaged with hardware and software.

This protocol/hardware/software combination/physical implementation of a collection of protocols, is often called a *network architecture.* One of the most widely known architecture is *System Network Architecture* (SNA) developed by IBM.

Standards

Standards are required in every manufacturing or business organisation and public service entity. In every engineering product or computer hardware , if the items are not standard, one firm could not help the other. The primary reason for standards is to ensure that hardware and software manufactured by different vendors can work together.

Without networking standards it is highly difficult, though not impossible to develop networks which would share information easily. If standards are not there, it would be difficult to procure items from different vendors. Standards also mean that customers are not locked into one another. Standards have advantages in:

- Buying hardware and software from any vendor whose equipment meets the standard.
- Promotes more competition and thus helps in reducing the prices.
- Developing software and hardware easily that links different networks (one layer at a time).
- Early updation, defined by the standard at one network layer (so long as the interface between that layer and the ones around it remains unchanged).

Standards are agreements, pure and simple.

Standards in the LAN and data communication's world are a way of promoting connectivity between products from different manufacturers.

Standards are built and developed with the cooperation of many organisations, committees, forums and government sponsored or regulatory agencies.

Standards in data communication can be classified as in figure 1.6 :

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

- *Specification stage* of formal standards consists of developing a nomenclature and identifying the problems to be addressed.
- *The identification of choices stage* are those working on the standard, identify the various solutions and chooses the optimum solution among the various alternatives.
- *Acceptance stage* : is the most difficult stage. Consists of defining the solution and getting recognised industry leaders to agree on a single uniform solution. Standards making processes are not susceptible to corporate politics and the influence of national governments unlike other organisational processes that have the potential to influence the sales of hardware and software.

1.4 STANDARDS ORGANISATIONS

The network standardisation, can be classified as under:

- Telecommunication standards world
- International standards world
- Internet standards world.

Different standards organisations coming under the above three categories are explained below:

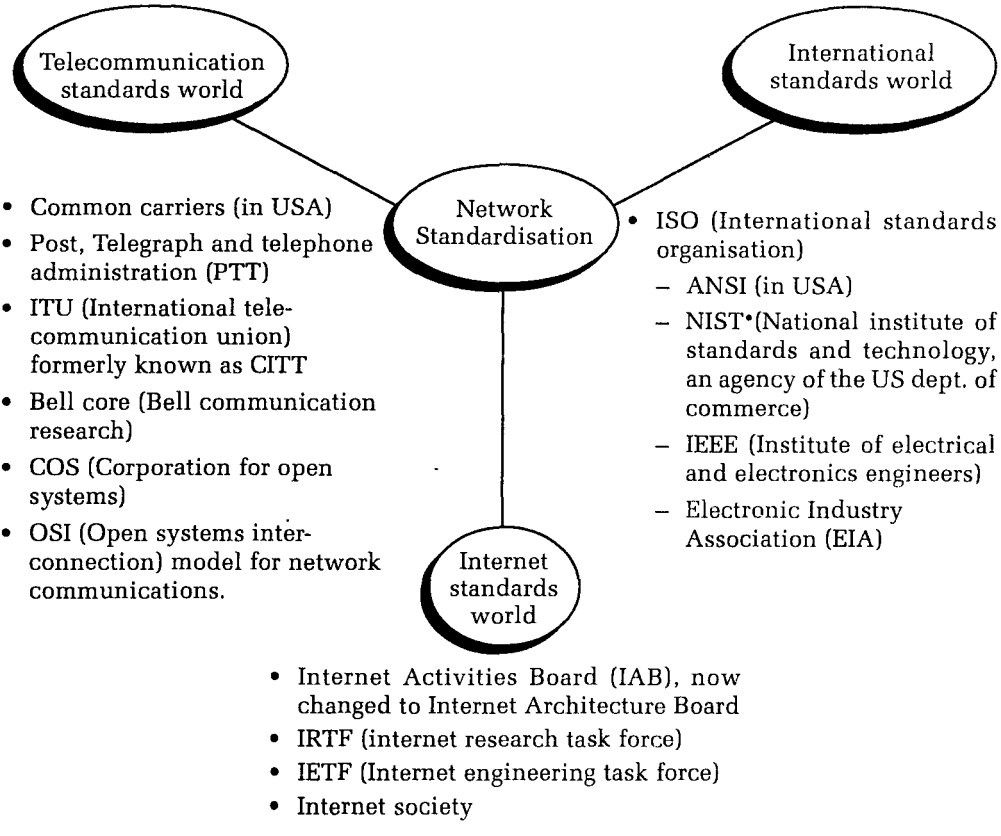


Fig. 1.7

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

A. Telecommunication Standards

(i) Common carriers exclusively provide communication services to the public in USA. Its offerings and prices are based on tariff, a document, approved by the Federal communications commission (both for the interstate and the international traffic, and by the state public utilities commissions for interstate traffic).

There are a good number of countries in which the national government has a complete responsibility on all communications like:

- Mail
- Telegraph
- Telephone
- Radio
- Television etc.

The national exchange carriers associations (NECA) T-1 committee/ accredited by ANSI) have representatives from telecommunication manufacturers carriers, users and other interested parties who develops North American wide area network telecommunication standards.

(ii) In many other countries, the telecommunication authorities is a nationalised company, and in others, it is a branch of the government, known as PTT (post, telegraph and telephone administration). Presently, all over the world it is moving towards total liberalisation and competition, reducing government monopoly.

(iii) ITU (International Telecommunication Union)

Most important thing is to have a clear need to provide compatibility on a world wide scale by different suppliers of goods and services. To achieve this, people from one country, and so also computers can call their counterparts from other countries, which is happening since a long time. In the early part of 1970s, many countries defined national standards in the telecommunication line. Still there was a gap for international compatibility. The United Nations, responded by forming, a part of its International Telecommunications Union. (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT).

Many of the European governments, joined together in 1865, to form the predecessor of the present ITU. The objective was to standardise international telecommunications, which represented telegraphy in those days. Fifty percent of the countries used morse code, while others used some other code ,resulted in problems. ITU succeeded in this by standardising telephony along with radios, when telephone was put into international service. In 1947, ITU was an agency of the United Nations. The three main sectors of ITU are:

1. Radio communication sector (ITU-R)- allocation of radio frequencies worldwide.
2. Telecommunications standardisation sector (ITU-T)
3. Development sector (ITU-D)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

ITU- T is important for us in this book. Hence ITU-T has been explained below:

ITU-T

ITU-T's task is for making recommendations about telephone /telegraph and data communication systems E.g.: V.24 (known as EIA RS-232 in USA) till 1993.

ITU -T was known as CCITT, an acronym for its French name (Comite Consultatif International Telegraphique et Telephonique).

On 1st March 1993, CCITT was reorganised as ITU -T and issued recommendations in the area of telephone and data communications.

CCITT X.25 is the only CCITT recommendation still running though CCITT takes on the ITU-T label.

ITU-T is divided into study groups , each represents a different aspect of the industry.

ISO & IT-UT often cooperates in telecommunication standards.

ITU-T have different classes of members.

- Administration (national PTTS)
- Private operators (AT & T, MCI, British Telecom)
- National committees (ANSI in USA,CEPT in Europe) for submitting proposals to the study groups.
- Telecommunications Organisations (European ETSI)
- Telecommunication vendors and scientific organisations.
- Other interested organisations /Banking and airline networks).

Important ITU-T standards are:

- V.series (V.32, V.33, v.42)for data transmission over phone lines.
- X series (X.25, X.400, X.500) for transmission over public digital networks.
- e-mail and directory services.
- ISDN (Integrated services digital networks).

  Extension of ISDN are known as *Broad band ISDN,* also known as the *information super highway.* These are used in current projects.

Some of the statistics of ITU - T are:

- 200 administrations
- 100 Private operators
- Several hundred other members.
- Current output runs to about 5000 pages of recommendations a year.
- ITU's costs are covered by different countries (Big, rich countries pay up to 30 contributory units a year; small, poor ones pay only 1/16th of a contributory unit). A contributory unit is about US 250,000 $. However, contributions are completely voluntary and everyone pays their free share.

ITU-T's real work is done through study groups (as large as 400 people with working parties, further divided into expert teams and ad hoc groups).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

In telecommunication world, the transition has commenced in 1980's to become national, then to global. Thus standards have become increasingly important. More and more organisations are now involved.

(iv) Bellcore stands for Bell Communication Research, extension of Bell Labs. It provides R & D resources for the advancement in the field of telecommunication technology providing draft standards to ANSI.

(v) **Communication standards :** Without standards, there can be no meaningful communication. The most important concept is standards. Their creation takes years of effort. There is no single standard agency so that everything could be orgainsed well. Various standard agencies and the relevant architecture are shown below:

SNA (System network architecture)	: Before OSI, SNA was introduced by IBM, which has become a defectors standard for mainframe communications. It is the third most widely used architecture, mainly due to their prominence in the mainframe market. IBM has attempted to extend SNA to other uses through Advanced peer Networking (APPN) extensions. Sometimes, groups of people want to converse in real time. They want to be able to type group messages on their boards and want to see what other members are typing.
Internet relay chart	: (IRC) allows one to chat online with many other people. There is now software to allow groups of people to build imaginary worlds called MUDs or MOOS in which individuals take on identities called cyber selves.
Newbies and FAQS	: In asynchronous/synchronous conferences newcomers often do not understand the existing groups informal rules. Many of these newbies ask questions that have already been questioned thousands of times before. This makes veterans unhappy and they get upset. Frequently asked questions can go in a file known as FAQs. The FAQs are questions that are asked by the new people often and the veterans are sick of such questions. Looking through these FAQS first will enable new comers to avoid asking such queries.
Video conferencing	: Though in general Internet links tend to be slow, some operate at 100kilobits per second. This will allow lowcost/low quality video-conferencing. (CUSEEME Program - CUSEEME software, MBONE video conferencing system)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

Internet telephone services: It is user to provide voice telephone service over the Internet. Several standards for Internet Telephone Service are now in use.

For information retrieval, anonymous FTP (File Transfer Protocol) sites open their files to the public. ARCHIE services allow you to identify which anonymous FTP sites have the file you seek. Gopher servers on the contrary organise information in a hierarchy of means. Veronica servers allow you to identify Gopher sites with menu items dealing with specific key words. WAIS servers provide full text key word searching on documents.

COS is a non profit corporation, came into effect in 1986, coming under computer and communication industry association with members of equipment of vendors and users of the above. As a very powerful organisation, its goal is to stimulate the development of inter operable communication products from different vendors. It also operates a centre to test compatible hardware and software in addition to promoting standards.

(vi) OSI

The most widely taught architecture is OSI, developed by ISO the reference model of "open system Inter connection". Reference model means architecture. An open system is one that is open to communicating with other systems using non proprietary architectures. OSI is for interconnecting systems that are open to communication via the nonproprietary standards.

The two standard agencies of ISO are (1) ISO (ii) ITU-T. ISO is the International organisation for standards, setting computer standards besides many other products, like motor oils, screws etc with a broad charter.

ISO is since a long time, a key standard agency for computers. But, ITU-T is dominant in telecommunications standards in telephony. television radio, facsimile etc. ITU-T is International Telecommunications Union - Telecommunications standards sector. Earlier ITU had two separate groups that set standards.

- CCITT - for wire based communication
- CCIR - for Radio.

In 1978, ISO and ITU-T released the OSI framework to guide their future standard setting.

Data communication tasks carried out by the seven layers in OSI Model

This Protocol reference model is composed of seven layers :

1. Physical (handles voltages, electrical pulses, connectors, and switches so that data can be transmitted over network media).
2. Data link (controls grouping data into blocks (message packets) and transferring blocks from one point in the network to another)
3. Network (controls the routing of data and messages through the channels of a network).
4. Transport (controls data transfer for the complete transmission path, from sending point to receiving point)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

5. Session (Establishes and terminates communication links between computers)
6. Presentation (Acts data transfer between different systems)
7. Application (provides network services to users and user applications including file transfer. Provides user interfaces with the systems).

B. International Standards

(i) ISO is an International standards organisation, which produces International Standards, coming under De jure categories. Second type as mentioned above (a voluntary, nontreaty organisation) founded in 1946. It has 89 members situated in 89 member countries and these are two national standard organisations. Some of the prominent members are:

- ANSI (American National Standard Institute)
- BSI (British Standard Institute)
- AFNOR (France)
- DIN (Germany)

ISO is one of the most important standard making bodies which makes technical recommendations about data communication interfaces (ISO comes from its French name, based in Geneva, Switzerland. ISO prepares standards on a wide number of subjects ranging from pen (literally) to big components. More than 5000 standards have been issued which includes the OSI standards.

ISO is also called international organisation for standardisation. It is a multinational body with membership of various governments, (82 industrialised nations) throughout the world from whom the standards creation committees have been formed.

ISO is dedicated to the worldwide agreement of international standards. It has around 200 technical committees, numbered as per its creation. Each deals with a particular subject. Every TC has subcommittees joining into its own Working groups WG s with a strength of more than 10,000 volunteers worldwide who is doing the required work. TC 1 deals with the nuts and bolts (standardising all types of screw thread pitches). Likewise, TC 97 deals with computers and information processing.

ISO aims to assist in the :

- International exchange of goods and services.
- Facilitates by providing good models for compatibility, best quality goods, higher productivity and reduced prices.
- Activity in developing cooperation in the realms of scientific, technological, and economic fields.
- Field of Information technology in the creation of OSI model.

In order to finalise a major formal standard, it takes five to ten years. With vast number of products entering the market every two years, formal standards development may become irrelevant. This process is to be streamlined and proportionalised. The recent networking developments are

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

introduction of fast ethernet, switched ethernet, FDDI, FDDI-II and numerous other products. By the time it is finalised, a standard that was five years in development has now been supplanted by several new generations (*Source :* Network world, Feb. 16, 1995).

(ii) **ANSI (American National Standards Institute) :** The US representative in ISO is ANSI which is a private, non-governmental organisation meant specifically for manufacturers, common carriers and other interested parties who are the members. It is a non profitable organisation. It is adopted by ISO. If any of the national standards organisation feels the need for an international standard in some area, a working group is formed to come up with a draft (Committee Draft). This is circulated to all the member bodies, which gets 6 months to criticise it. If majority approves, then a required document known as DIS (Draft International Standard) will be produced and circulated for comments and voting. The final text of the IS (International Standard) is prepared, approved and published . Sometimes, CD or DIS may take years to get approval in case of controversy. ANSI members include professional societies, industry associations, governmental and regulatory bodies and consumer groups. ANSI published the fiber distributed data interface (FDDI) standard for 100 megabytes high speed fibre optic LANS, The areas of ANSI include:

- Internet work planning and engineering
- ISDN services
- Signalling and architecture.
- Optical hierarchy (SONET)

CEPT (committee of European post, Telegraph and Telephone) and

ETSI (European Telecommunications Standards Institute) provides similar service.

(iii) **NIST (National Institute of Standards and Technology)**

It is an agency of the US department of commerce. Earlier name was National Bureau of Standards. The issues standards are regarding purchases made by the US Government. However US defence, has its own standards.

(iv) **IEEE (Institute of Electrical and Electronic Engineers) :** This is another major institute, a largest professional organisation in the world. It publishes variety of journals and runs numerous conferences every year. It has a standardisation group that develops standards for electrical engineering and computing fields. IEEE's 802 for Local Area Networks is the key standard for LAN (802.3, 802.4, and 802.5 standards). It develops standards for computing, communication, electrical engineering and electronics. It aims at advance theory, creativity and product quality in the fields of electrical engineering electronics and radio as well as in the other branches of engineering.

There are several ways to get access to the Internet. The three most popular ones are through:

- An online service. Using an Internet service provider. Using an Internet gateway on a corporate LAN. In the future, the pressing policy issues surrounding the Internet are:

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

- Who will pay for Internet transmission lines?
- How crime and rude behviour can be curbed?
- How to access speeds?

(v) **EIA (Electronic Industry Associations) :** It is an association of electronic manufacturers in the USA, mainly responsible for developing EIA 232-D, EIA 449, and EIA 530 standards.

EIA's activities are in many fields like:

- Standards development
- Public awareness education
- Physical connection interfaces (in IT field)
- Electronic signalling specifications (for data communication)

(vi) **Asynchronous Transmission Mode (ATM) Forum :** *Forums* are representatives from the corporations who would test, evaluate and standardise new technologies. Many forum's that exist are Frame Relay forum, ATM Forum, Internet society, IETF. Internet Society & IETF have already been explained.

ATM Forum and ATM cosortium have been created to promote the acceptance and use of ATM (Asynchronous Transmission Mode) technology. This forum is constituted of :

- Customer premises equipment vendors (PBX systems)
- Central office providers (Telephone exchange)

ATM consortium is made up of vendors of hardware and software that support ATM.

In addition to the forum regulatory agencies are also there. One such agency regulated by the USA Government is FCC (Federal Communication Commission), which protects the public interest by regulating radio, television and wire/cable communications.

Apart from the above there is electronic data interchange standard which was formulated in 1985 by European and USA network users who are concerned that diverging sets of standards on the two continents could greatly inhibit international EDI. It depends major components of the ANSI EDI Standard.

EDI is the working name for electronic Data Interchange for administration, commerce, and transport (EDIFACT). EDIFACT is supported by users in Europe, Far East. But Canadian and American users are reluctant to embrace it because their investment in networks are based on EDI standards developed by the ANSI Committee. Hence, EDIFACT is not comparable with ANSI Standard.

There are a number of legally enforceable standards which are:

- Federal wire tap statute (in 1968) protects voice communication from interception.
- Electronic communications piracy act of 1986- As per this, intercepting electronic communications such as data communications or electronic

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

mail, or to tamper with the computers in a data network is a crime (Penalties up to US $ 100,000 and ten years imprisonment. For organisations, this can go up to US $ 250,000 as fine)

- Computer fraud and abuse act of 1986 – for interstate computer crimes involving private sector computers (unauthorised access and for damaging records) – Fines up to US $ 100,000 and ten years imprisonment.
- Computers Security Act of 1987 – This act shift power away from the National Security Agency (NSA) to the NIST (National Institute of Standards and technology) to establish security standards and training programs for federal agencies using unclassified information systems. The law gives total control of the data encryptism standard (DES) to NIST.
- Computer virus eradication Act of 1988 to fright the spread of computer viruses.

C. Internet Standards World

(i) Internet Activities Board (IAB) : Internet has its own standardisation mechanism, totally different from ITU-T and ISO. The meetings for the latter, is attended by government and corporate officials, where standardisation is the job. In the case of internet, agreement is needed to make things work.

When the ARPANET (Advanced Research project, Agency Net) was setup, DOD's informal committee to look into the ARPANET was renamed in 1983 as IAB. This was for a broader mission, to keep the researchers involved with the ARPANET. The meaning was later on changed to Internet architecture board.

Some of the statistics of IAB available are:

- Ten members of the IAB headed a task force on some issue of importance.
- IAB meets many a times a year to discuss on various issues and gave feedback to DOD and NSF which were funding mostly. Whenever a standard was needed , IAB members were working on it to enable the students to implement the software. Communication was done by a series of technical reports (RFCs - Request for comments stored on-line & can be fetched by any one interested).These were numbered in the order of creation. Around 2000 members now exist.

(ii) IRTF and IETF (Internet Research task force and Internet engineering task force) : IRTF is the one where researchers were moved from IRTF and a subsidiary to IAB, along with the IETF. The IAB was repopulated with people representing a broader range of organisations than just the research community. Originally, it was a self-perpetuating group, members serving only for 2 year term and new members appointed in their place.

(iii) Internet Society : This was created for the people who are interested in the Internet. It is in a way comparable to ACM or IEEE; governed by elected trustees who approve the IAB members.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

POINTS TO REMEMBER

- Data is the raw material from which useful information is derived whereas information is data placed in a meaningful and useful context for an end user. The two terms are used interchangeably.
- A database is a self describing collection of integrated records. Data processing is the execution of a systematic sequence of operations performed upon data to transform into information.
- Data communications refer to the transmission of computerised data from one location to another. Two types of data transmission are internal (transfer of data within a computer) and external (transfer of data to either local peripheral equipment say printers or remote computers).
- Communication is essentially a perceptual process. The sender must encode intended meaning to create messages. The receiver then encircles message to obtain perceived meaning. Effective communication depends on the sender and receiver sharing an understanding of the rules used to encode meaning into messages.
- Data communication system components are message, sender, receiver, medium and protocol. The basic communication media are software computers, transmission technologies.
- Data communication have three fundamental characteristics:
  Delivery, Accuracy, timeliness. Data communications are grouped as local and remote.
- Data communication networks are established to collect data from remote points, to transact the data to a central point with a more powerful computer, to offer better and more timely interchange of data among their users etc.
- The main objectives of data communication networks are to reduce the time, effort and cost required to perform business tasks, to support improved management control of the organisation.
- Data communication system types have been explained in the chapter.
- A network is a series of points connected by communication circuits The switched telephone network is the network of telephone lines normally used for dialed telephone calls. A private network is a network of communication circuits confined to the use of one customer. Computer network is an interconnected collection of autonomous computers.
- Networks use distributed processing, wherein a task is divided among all aspects of a process. The same is done by individual separate computers which handles portion of the task.
- Distributed processing advantages are: security/encapsulation, distributed data bases, quick problem solving, high degree of cohesiveness and transparency, existence of multiple autonomous computers transparent to the user, user not aware of multiple processors .
- The advantages and disadvantages of distributed system and networks have been compared in this chapter.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

- Network applications are many. Few of them are smart buildings, cellular telephone, electronic/voice mail, data monopoly, EDI, transborder data flow, ICN, Directory/information services etc.
- Protocol is a formal set of conventions governing the format and control of inputs and outputs between two communicating devices. Rules are included by which these two devices communicated as well as hand shaking and line discipline. The rule of communication how a system talks and expects to be talked to - are called protocols.
- Standards are agreements, pure and simple. It is required in every manufacturing or business organisation and public service entity. It is to ensure that hardware and software manufactured by different vendors can work together. Standards in the LAN and data communications world are away of promoting connectivity between products from different manufacturers. These are developed with the cooperation of many organisations, committees, forums and government sponsored or regulatory agencies.
- There are two primary categories of data communication standards, de facto (industry) and de jure (official). The names refer to who develops the specifications and how they become standards.
- De Jure are primal standards and non proprietary which means that no one company makes them or owns right to them. These are developed with the intent of providing for greater connectivity and inter operability by making specifications public so that independent manufacturers can build to them. Subscribing to de jure standards reduces the risk and cost of developing hardware and software for manufacturers.
- De facto standards become formal standards when once it is accepted as found in the telecommunication industry. It arises in the industry itself. These are often proprietary. MS-DOS, UNIX, and Netware are all proprietary and de facto standards. Proprietary standards are sometimes unpublished and unavailable to outside vendors.
- The network standardisation can be classified as telecommunications standards world, International standards world, Internet standards world. Different standard organisations coming under the above three categories are explained in the chapter.

QUESTIONS

1. What do you mean by data and information?
2. What is data processing?
3. Define data communication?
4. What are two types of data transmission?
5. What is a telecommunication system? Explain.
6. What are the communication system elements?
7. What is a communication model? Describe the same.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

8. What are the basic communication media?
9. How are the data communications grouped?
10. What are the three fundamental characteristics of the data communications?
11. Why data communications are established?
12. What are the objectives of data communications?
13. Explain the different types of data communication system with a sketch.
14. What is a computer network? Define.
15. What do you mean by distributed processing?
16. Compare and contrast distributed system with network.
17. Mention at least 8 applications of data communication network and explain the same in brief.
18. What are smart buildings?
19. What do you mean by electronic/voice mail?
20. What are the advantages of distributed processing?
21. Write short notes on:
    - Data monopoly
    - Telecommuting
    - Teleconferencing
    - ICN
    - Transborder data flow
    - Directory services
    - Electronic data interchange (EDI)
    - Smart buildings
22. Explain data communication standards?
23. Define standard. Why standards are necessary?
24. Define protocol.
25. What are the classification of data communication standards? Explain.
26. What are formal standards? How are they classified?
27. What do you mean by de facto standards?
28. What do you mean by de jure standards?
29. What are proprietary and non-proprietary standards?
30. What are the advantages of standards?
31. How are the network standardisation are classified?
32. Which are the different standard organisations working on standards? Which are the most important out of these?
33. Explain few organisations who are working exclusively on telecommunication standards.
34. Expand the following:
    - PTT
    - ITU
    - CCITT
    - IEEE
    - EIA
    - COS
    - IRTF
    - ANSI
    - CEPT
    - ETSI
    - IAB
    - BSI
    - ATM
    - OSI
    - CCITT

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

FILL IN THE BLANKS

1. Data is the collection of facts, which is _____.
2. Data can be made organised into useful _____.
3. Information is _____ data.
4. The conversion of facts into meaningful information is _____ _____.
5. Data communication is the transmission of _____ _____ from one location to another.
6. Two types of data transmissions are _____ and _____.
7. Communication system elements are _____ _____, _____ _____, communication media, modems, communication management devices.
8. Three fundamental characteristics of data communication are _____, _____ and _____.
9. Data communications system components are _____, _____, _____, _____, _____.
10. Data communications is principle enabler of the rapid _____ _____.
11. Data communications can be grouped as _____, _____.
12. Data communication networks are used to reduce _____, _____ and _____.
13. Large number of separate, but interconnected computers perform the job in a _____ and _____ way; such systems are called computer _____.
14. Network connects a variety of _____ and computers.
15. Networks are _____ _____, wherein a task is divided among many computers.
16. The distinction between a network and distributed system is with the _____ instead of the _____.
17. Network criteria are performance, _____ and security.
18. _____ _____ is within a specific country.
19. The employees perform most of the work at home is _____ _____, instead of at office.
20. ICN is IOWA _____ _____.
21. _____ _____ _____ is the movement of data across national boundaries.
22. EDI is electronic data _____; _____ transmission.
23. _____ is a set of rules and procedures that govern transmission.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

24. _____ are agreements, pure and simple.
25. _____ are required in every manufacturing organisation.
26. Standards are developed with the co-operation oforganisations, _____, _____ government sponsored or regulatory _____.
27. Network standardisation includes _____, _____ _____, _____ _____ _____, _____ _____ _____.
28. Common carriers provide _____ _____ to the public.
29. ISO is an _____ _____ _____, founded in _____with _____ members.
30. Prominent members of ISO are _____, _____, AFNOR, DIN.
31. NIST is _____ _____ of _____ and _____.
32. _____ is adopted by ISO.
33. Three main sectors of ITU are _____, _____, _____.
34. Important ITU-T standards are ___, ___ series.
35. _____ and ITU-T often co-operates in telecommunication stanards.
36. _____ stands for Bell Communications Research.
37. _____ are representatives from the corporations who would test, evaluate and standardise new technologies.
38. ATM forum is _____ _____ _____ Forum.

Answers

1. unorganised
2. information
3. processed
4. data processing
5. computerised data
6. internal ; external
7. host computers ; peripheral devices
8. delivery ; accuracy ; timeliness
9. message; sender ; receiver ; medium ; protocol
10. information exchange
11. local ; remote
12. time ; effort ; cost
13. better ; faster ; networks
14. terminals
15. distributed processing
16. software ; hardware
17. reliability
18. Data monopoly
19. Telecommuting
20. communication network
21. Transborder data flow
22. interchange; paperless
23. Protocol
24. Standards
25. Standards
26. Committees ; forums ; agencies

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

27. Telecommunication standards world ; International standards world ; Internet standard world
28. communiction services
29. International Standard Organisation ; 1946 ; 89
30. ANSI ; BSI
31. National Institute Standards Technology
32. ANSI
33. ITU-R, ITU.T, ITU-D
34. V ; X
35. ISO
36. Bellcore
37. Forum
37. Asynchronous Transmission Mode

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:05:21.

UNIT 2

CHAPTER 6

TRANSMISSION OF DIGITAL DATA : INTERFACES AND MODEMS

CHAPTER 7

TRANSMISSION MEDIA

CHAPTER 8

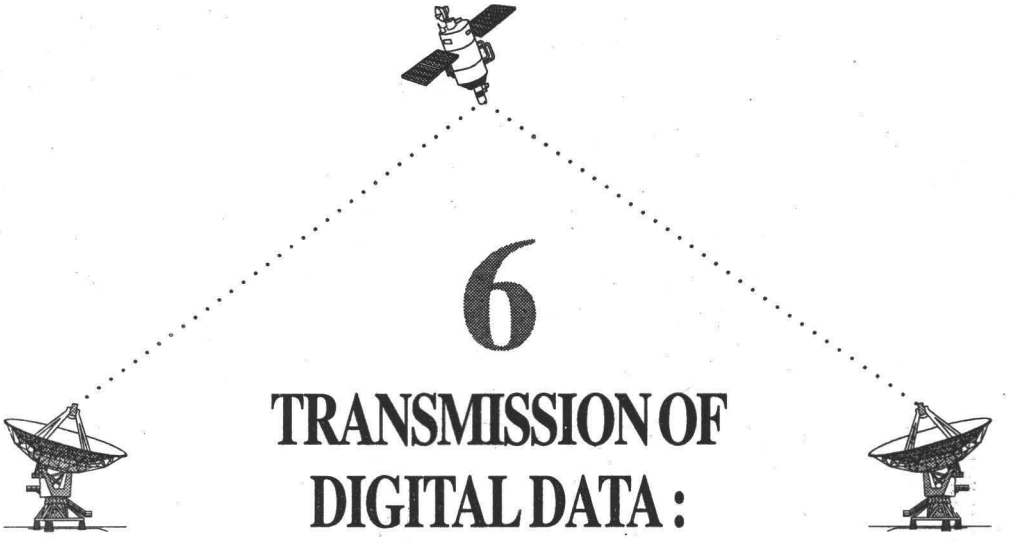
MULTIPLEXING

CHAPTER 9

ERROR DETECTION AND CORRECTION

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.



6

TRANSMISSION OF DIGITAL DATA : INTERFACES AND MODEMS

6.1 INTRODUCTION

Digital transmission offers a number of benefits over analog transmission. This has been indicated in chapter 5.

Digital communication is the transmission of discrete signals over a transmission channel. It involves two discrete voltage for binary 0s and 1s. A digital receiver should be capable of correlating a received signal with a finite set of digital values. The data if it is to be understood by both the sender and receiver, they should agree on a standard methodology for representing the letters, numbers and symbols that is covered in messages. The transmission of data takes place from one device to another through electrical wiring. A copper wire transmitting electricity acts rather like a hose transferring water. The three common terms used in electricity are:

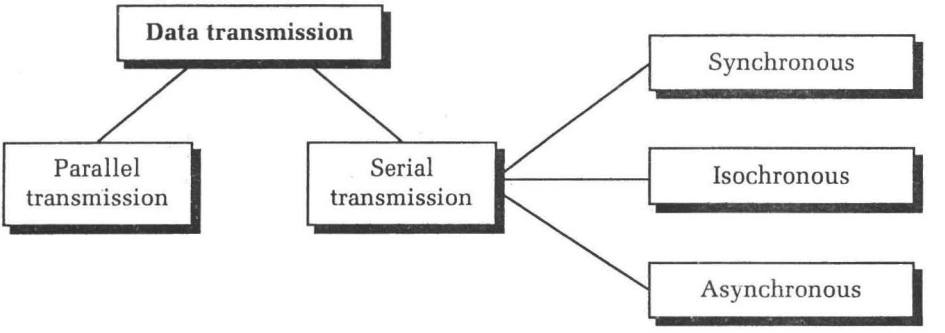
- Voltage
- Amperes
- Watts

While considering the wiring for data transmission, the main concern is how the data stream to be transmitted. The question is whether to send one bit at a time or a larger group after grouping bits. Two ways of accomplishing the transmission of binary data across a link is by :

- Parallel mode (Transmission in which bits in a group are sent simultaneously, each using a separate link)
- Serial mode (Transmission of data one bit at a time using only one single link)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.



Parallel transmission

It is a way the internal transfer of binary data (consisting of 1s and 0s organised into groups of n bits each) takes place inside a computer. If the grouping is arranged, we can send data n bits at a time instead of one bit. It the internal structure of the computer is 8 bit, all 8 bits of the data element are transferred between main memory and CPU simultaneously on 8 separate connections. These are known as parallel transmission. The mechanism appears to be very simple. By using n wires, we can send n bits at one time. This should that each bit has one wire and all n bits of one group can be transmitted together with each clock pulse from one device to another. If we are using 8 wires, it is a 8 bit structure. The eight wires can be bundled in a cable with a connector at each end. The same is true of computers, that use a 32 bit structure - 32 bits are transferred simultaneously on 32 connections.

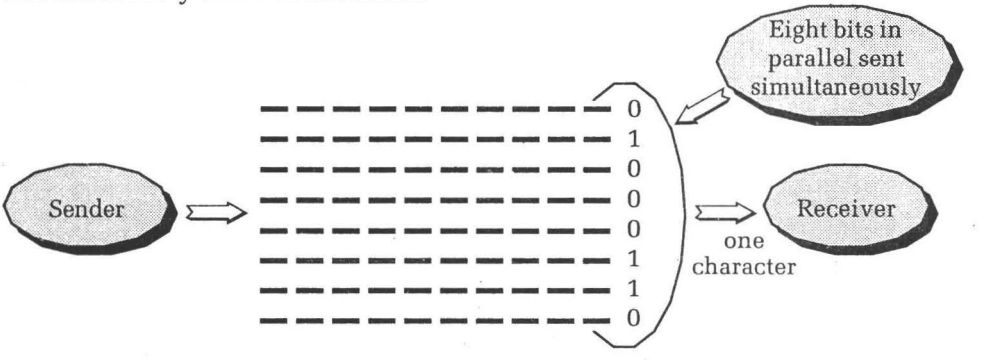


Fig. 6.1 Parallel transmissions of an 8 - bit code

Figure 6.1 shows how eight bits of one character could travel through a parallel communication circuit. The advantage is speed but the disadvantage is cost. Parallel transfer is not generally recommended for data communications in view of the cost, but most printers use parallel communication for achieving speed. It is possible to have parallel cables with many wires (one for each bit) in printer, if the printer is very close to the computer. This will not work reliably if the lengths are more than 25 feet.

Serial transmission

This is the most preferred mode of transferring information in data communications. Here a stream of data is sent over a communication circuit in a

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

sequential way, bit-by -bit fashion as shown below in figure 6.2. Only one communication channel is needed instead of n to transmit data between two communicating devices.

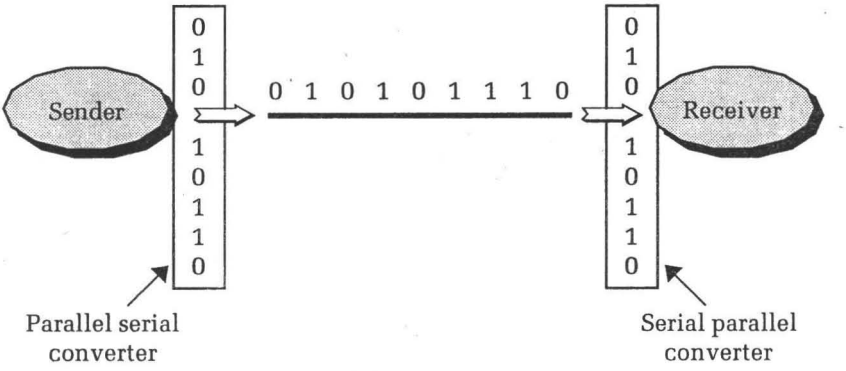


Fig. 6.2 Serial transmission of an 8 bit code.

This mode is distinguished from parallel in the sense that the transmitting device sends a single bit, second bit, third bit and so on until the complete set of bits are transmitted (n iterations/cycles to transmit n bits). Here the conversion devices are required as communication within devices is parallel.

The advantage is cost; disadvantage is lower speed than parallel transmission.

Between the sender and the line (parallel to serial), so also between the line and the receiver (serial to parallel), conversation devices are needed at the interface. This transmission occurs in two ways : Synchronous and asynchronous.

Synchronous transmission and Asynchronous transmission

Synchronous transmission is generally used when large volume of data or information must be transmitted from one device to another at high speed. It transmits multiple bytes in the form of packets or frames.

Asynchronous transmission transmits a byte (character or keystroke) at a time to a receiving computer. It is also called as start stop transmission and transmits one character at a time over a line, each character framed by control bits - a start bit, one or two stop bits and a parity bit. It is used for low speed transmission. It involves less expensive equipment than synchronous transmission.

Serial transmission can occur either asynchronously or synchronously. Both refer to the way that data are packaged as they are sent along a communications medium.

In asynchronous transmission, a data package consists of a single character which is preceded by a 'start-bit' (a 0) and ends with 'a stop bit' (a 1). Asynchronous transmission might occur, perhaps, when an operator at a key board types messages to a computer. As each key is struck, the byte representation of the keystroke is packaged and sent 'up the line' to the computer. As soon as the computer sends a start bit, it prepares itself to read the character. When the sender device is on-line but idle, it is sending the computer continuous stream of stop bits.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

	Synchronous	Asynchronous	Remarks
1. Efficient utilisation of the transmission line	A	D	Periods between blocks kept small and the block itself is sent at maximum line speed.
2. Need forelock buffer storage at the two ends of the line	D	A	To assemble blocks and the need for accurately synchronised clocks at both ends.
3. Equipment is more expensive & needs a modem	D	A	
4. Point No.3 offsets by the greater speed and lower cost from more efficient transmission (though initial cost is high)	A	D	
5. Display terminals are designed for transfer of data at high speeds (data speeds of 2400 bps and higher)	A	D (for low speed)	Asynchronous trans-mission use teleprinters (show typing operation for input and slow mechanical printing head for output)

A-Advantages D-Disadvantages

Table 6.1 Advantages and disadvantages of synchronous and asynchronous transmission

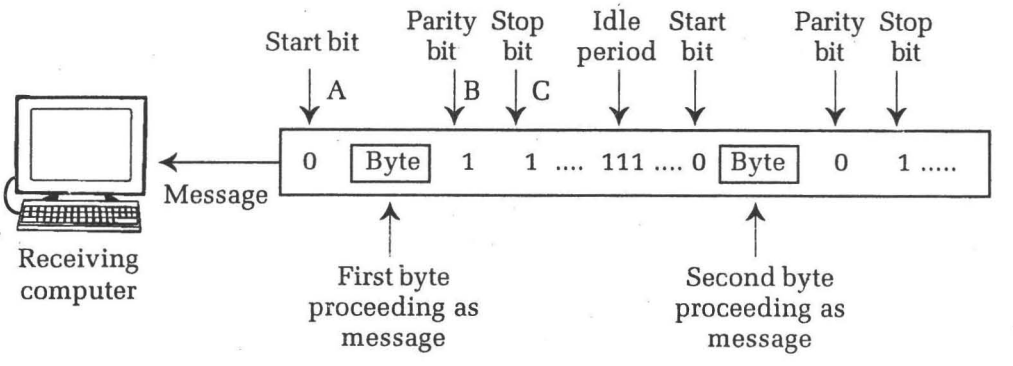


Fig. 6.3 Asynchronous transmission

A start bit precedes each bytes representation of a character (In this case letters N and O are shown as per ASCII representation). 'A' is shown as the start bit and 'B' is the parity bit. A stop bit follows each character (Here 'C' is the stop bit shown). When the sending machine has no character to send, it transmits a steady stream of stop bits. The machine at the receiving end 'listens to the line'

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

for the start bit. When it senses this bit, it counts off the regular bits used to represent the character. When it encounters the stop bit, it reverses to a 'listen to the line' state and waits for the next start bit.

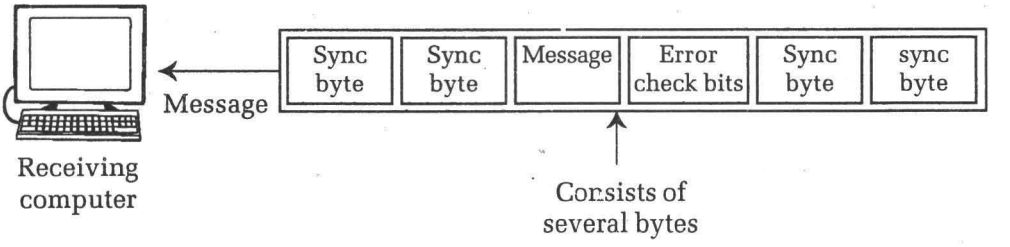


Fig. 6.4 Synchronous transmission

In synchronous transmission, each block of characters is preceded by one or more synchronous bytes. The machine at the receiving end listens to the line for this byte. When it is sure it has sensed it, the receiving machine starts reading the characters in the block. This transmission is used for data speeds of 2400 bps and higher. The receiving machine knows the speed of transmission and number of characters per block. It can interpret the message. After the block is exhausted, the receiving mechanism continues to the 'listen' to the line for the next sync bytes.

In synchronous transmission, each data package may consists of hundreds of characters and used for fast transmission of large block of data. Here the package is sandwiched between one or two 'sync bytes' which serve a function similar to the start and stop bits used for asynchronous transmission. This is used where transmission speeds of 2400 bps or higher are needed along the communications medium. A chain store might send all of its data to a central head quarters facility, using synchronous transmission. Here all the data are ready to go at the transmission with minimum call charges (if sent quickly), the synchronous transmission is preferred.

Parity bits are the primary means of checking errors in asynchronous transmissions. This extra bit added to each byte as a check measure so that the sum of all the bits of every byte come out to either an odd or even number. In odd parity system, the 1 bits always sum to an odd number. In even parity systems, an even number.

Codes

Error Detecting

Errors occur is recording data due to:

- Due to bad spots on the magnetic surfaces.
- Electrical disturbances during transmissions between units.

Methods are to be devised to prevent this. The principle used for their purpose is coded data by introducing extra bits in the code to aid error detection. A common method is the use of a parity check bit along with each character code.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Example :

ASCII Code (Even parity check bit)

Let us take a letter F	Take a letter D
ASCII code for letter F is 1000110	ASCII code for letter D is 1000100
Here the total number of ones are (odd)	Here the total number of ones are two three (even).
A parity check bit is appended to the 7 bits of the code of each character in such a way that the total number of 1s in each character code is even. In this case one more 1 is to be appended to make the total number of ones even.	A parity check bit is appended to the 7 bits of the code of each character in such a way to make it 8 bits is to add one 0. All characters now have 8 bits code including the parity check bit.
With an appended parity check bit code for better F would be 10001101	ASCII code for letter D with an appended parity check bit is 10001000.

Whenever a character is read from a storage or received from a remote location, the number of units code is counted, it has to be even. If it is odd then one bit (atleast) is wrong. A single error thus in any of the eight bits of the code will be detected. Two errors cannot be detected as the total numbers of 1s in the code will remain even after two bits change. As probability of more than one error occurs is in practice very small, this method is accepted as adequate.

Alternatively (odd parity check bit)

Instead of making the total number of 1's in the code even, the code can be made odd by appending a parity check bit, known as odd parity check bit. This also facilitates detection of a single error in a code.

Codes, if deviced to use more than one check bit to detect and to correct errors are called as 'error correcting codes'.

Asynchronous transmission is the transfer of data with start and stop bits and a variable time internal between data units. It is named like this because of the unimportant timing of a signal. Here information is received and translated as per the agreed upon patterns (based on grouping the bit stream into bytes - eight bits). It is also called as start - stop transmission, because the transmitting device can transmit a character whenever it is convenient and the receiving device will accept that character. It is typically used on point to point full duplex circuits (circuits that have only two devices on them) so, media access control is not a concern. If we are using 7 bit ASCII with even parity, the total transmission is 10 bits for each character (1 start bit, 7 bits for the letter, 1 pasting bit, 1 stop bit). Start bit and the stop bit are the opposite of each other.

In asynchronous transmission:

- No fixed distance between characters (the terminal transmits, the character as soon as it is typed, depending upon the speed of the typist).
- Synchronisation (Recognition of the start and stop of each message) takes place for an individual character (The start bit is a signal that directs the receiver to start sampling the incoming bit of a character at a fixed rate so the data bits can be interpreted into proper character structure).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

- A stop bit informs the receiver that the character has been received and resets it for recognition of the next start bit.
- If the sender is waiting for the user to type the next character, no data is sent, the communication circuit is idle (This idle time is artificial - some signal must be sent down the circuit). Asynchronous transmission defines the idle signal as the same as the stop bit.
- If the sender finishes transmitting a letter and waits for some more data to send, it sends continuously stop bits. Older protocols had two stop bits instead of the traditional single stop bit.

Asynchronous here means - asynchronous at the byte level. The bits are still synchronised, durations are the same.

Asynchronous transmission is slower because of the additional bits and gaps. It is cheap and effective; specially for low speed communication it is preferred.

In synchronous transmission, bits are sent one after another without start stop bits or gap. It is the responsibility of the receiver to group the bits. The bit stream is combined into longer frame which may have multiple bytes. This block of data called as a frame or packet depending upon the protocol. The receiver counts the bits as they arrive and groups them in eight bit units. The start and end of the entire packet must be marked, not the start and end of each letter. The user presses a special transmit key. The start and end of each packet (synchronization) is established by appending a predetermined group of characters at the beginning and end of packet. The characters are called synchronisation characters (SYN). After the SYN characters the transmitting device sends a long stream of data bits (may be thousands of bits). Depending upon the protocol adopted such as byte oriented, bit oriented, byte count etc.), there may be any where from one to eight SYN characters.

Isochronous transmission

It combines the elements of both synchronous and asynchronous data transmission in this technique as under:

- Each character will have a start and stop bit as in asynchronous data transmission. All periods of no transmission consists of one or more I - character time intervals.
- The sender and receiver are synchronised as in synchronous data transmission. The synchronisation time interval between successive bits is an even multiple of the length of one code bit.

Data can be transmitted at higher speeds in this transmission.

Difference between the three types of transmission

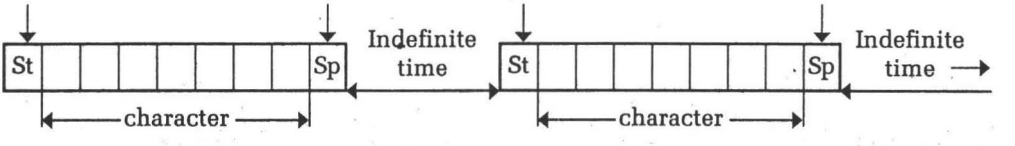


Fig. 6.5(a) Asynchronous transmission

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

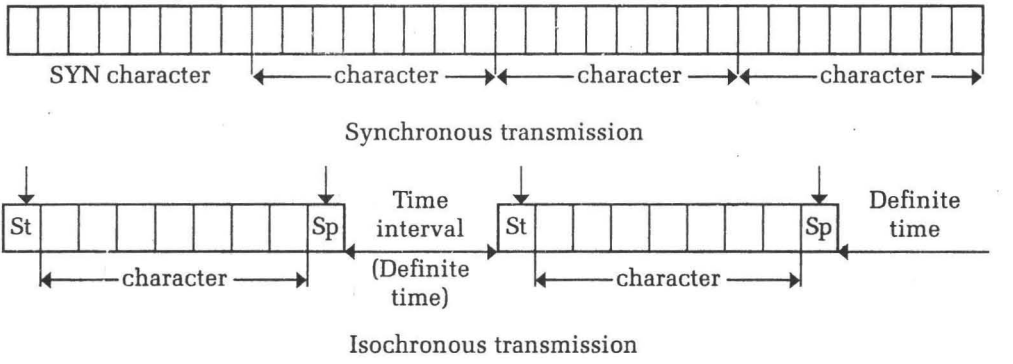


Fig. 6.5(b) Comparison of transmissions

6.2 DTE - DCE INTERFACE

Data terminal equipment (DTE) is a device serves as an information source or an information sink. DTE is connected to a network through DCE (Data circuit-terminating equipment). DCE is a device used as an interface between a DTE and a network. E.g. A modem is a DCE.

A DCE is a device that transmits and receives data in the form of analog or digital signal through a network. It provides all the functions required to establish, maintain and terminate a connection. It includes:

- Signal conversion
- Coding between the DTE and the common carriers circuit (including the modem)

DTE comprises of :

- The data source, (At the physical layer, it can be a terminal, micro computer, computers, printer, FAX machine or any other machine that generates or consumes digital data)
- The data sink or
- Both

DTE is any piece of equipment at which a data communication path begins or ends, such as a terminal. It functions either as a source of or as a destination for binary digital data.

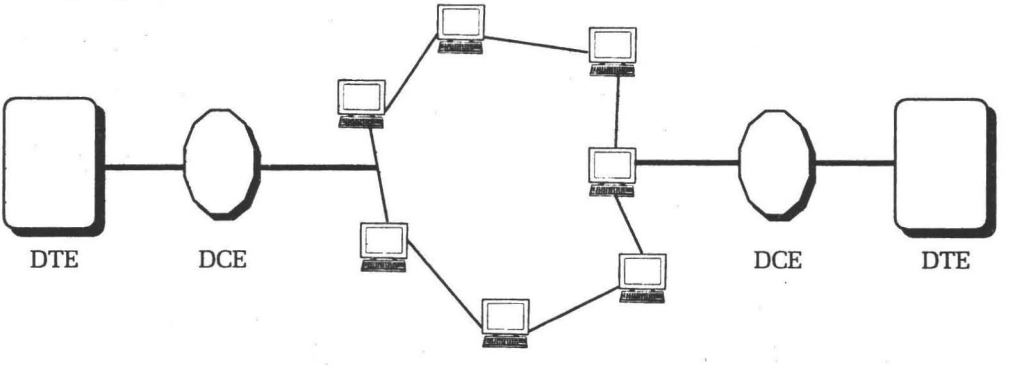


Fig. 6.6 DTE-DCE interface

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

E.g. It may be noted that DTEs do not communicated directly with each other. It acts like brains as shown below:

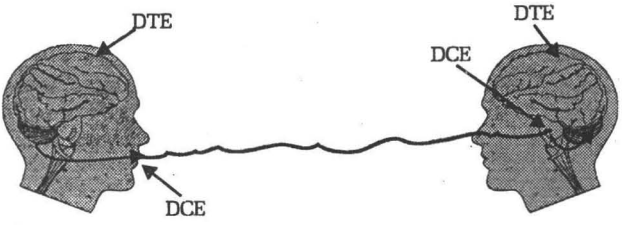


Fig. 6.7 Human compared to DTE and DCE

While conveying a message from person 1 to person 2, their brains act like DTE. Message from person 1 goes (from brain to mouth through local chords) as sound waves to the ears of person 2 (from there to 2nd person's brain). Here, the vocal chords and mouth of a person 1 and ears of person 2 are like DCE.

DCE takes the data generated by DTE at the physical level converts the data (in the form of an analog or digital signal) to an appropriate signal to pass on to the telecommunication link. E.g. Modem (Modulator/demodulator). A DTE generates digital data and passes it to a DCE, which converts the data to an acceptable form to the transmission medium. DCE at the other end of the network converts the data back to form usable by its DTE and delivers the same. Both DCEs at either end must use the same encoding method (like FSK). The coordination is between DTE and DCE and between DCEs so that data transmission is done smoothly without any loss of integrity.

Standards

Many standards, are available and have been developed between a DTE and DCE. Each standards, though they differ in solutions provides a model for various characteristics of the connection.

Out of the many organisations involved in DTE-DCE interface standards, two important ones are:

- Electronic industries association (EIA); EIA 232, EIA 442, EIA 449 are the ones.
- International telecommunication union - telecommunication standards committee (ITU-T). These standards are called V and X series.

The electronic industries association is an ANSI accredited standards organisation that develops a variety of standards covering even equipment standard - one of its most prominent standards is the RS 232 connector cable. Membership is drawn from manufacturers of telecommunication equipment and other electronic components.

EIA 232 is an interface developed by the EIA for DTE and DCE which defines the mechanical, electrical and functional characteristics of the interface. It was first known as RS 232 standard in 1962 (that is RS means recommended standard). It was also known as DB25, since the mechanical standard defines the interface

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

as a 25-wire cable with a male and a female DB-25 pin connector attached to either end. The length of the cable used to be around 50 feet say less that 15 meters. Users normally talk about connector cables as RS 232, DB25, RS 449 or DB 9. Each connector cable is based on a specific standard calling the connector by standards designation, user understands precisely the type of connector used.

RS 232 connector cable revised as RS 232 C in 1969 (3rd revision) and RS 232 D in 1987 (4th revision) and was known as EIA 232 D, RS 232 connector cable is the standard interface for connecting DTE and DCE. RS 232 D is having 25 wires and with a DB 25 connector plug (like the plug used on micro computers). It is just known as DB25 of the connector cable is used on micro computers. If not attached, otherwise called as a RS 232 interface. Outside USA, RS 232 D connector cable is known as V.24 and V.28 standards; which has been accepted by the international standards group known as CCITT (consultive committee on International telegraph and telephone). These standards provide a common description about the signal coming out of or going into the serial port of a computer or terminal looks like electrically. In the DB 25 connectors the pins (male side) and tubes (on the female side) are arranged in two rows, with 13 on top and 12 on the bottom.

EIA 232 provides for a signal changing from a nominal + 15 Volts to a nominal –15 volts. The standard also defines the cables and connectors used to link data communication devices. EIA 232 states that all data must be transmitted as logical 1s and 0s , using a non return to zero, level NRZ - encoding, with 0 defined as a positive voltage and 1 as a negative voltage. No voltages would fall outside ± 15 V. To be recognised as data, the amplitude of a signal must fall between +3 and 15 volts or –3 and –15 volts. By allowing valid signals to fall within two 12 V ranges EIA makes it unlikely that degradation of a signal by noise will affect its recognizability. It is interesting to note that only 4 of the wires in a total of 25 are used for data functions. The rest are kept for functions like control, timing, grounding and testing. ON means more than +3 voltage. OFF means less than –3 Voltage.

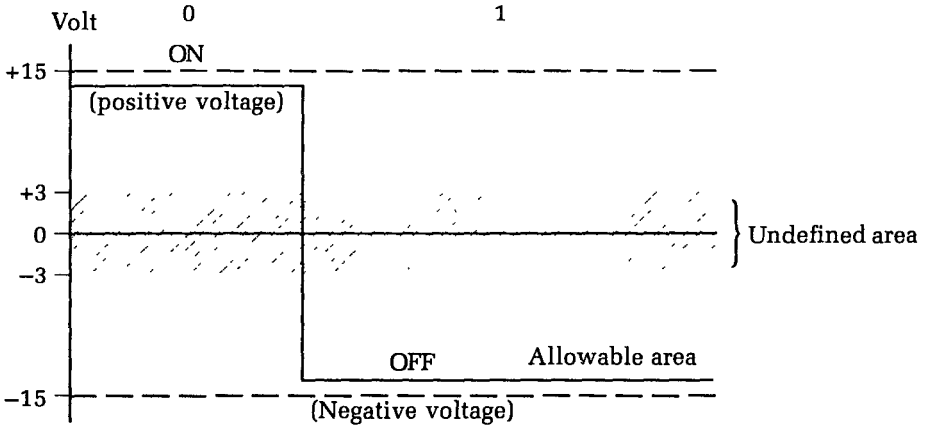


Fig. 6.8 Control signals electrical specification

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

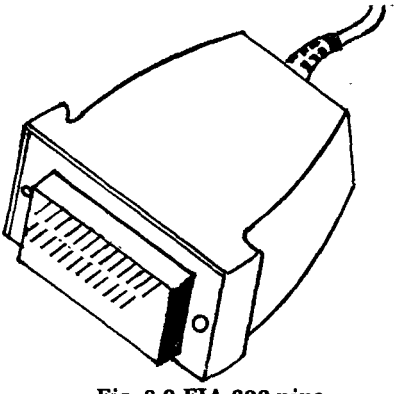


Fig. 6.9 EIA 232 pins

Functions of pins

Top Pins (13 Nos)	Bottom pins (12 Nos)
1. Shield	14. Secondary transmitted data
2. Transmitted data	15. Transmitter signal element timing (DCE - DTE)
3. Received Data	16. Secondary received data
4. Requested to send	17. Receiver signal element timing (DCE - DTE)
5. Clear to send	18. Local loop back
6 DCE ready	19. Secondary request to send
7. Signal ground	20. DTE ready
8. Received line signal detector	21. Remote loop back and signal quality detector
9. Reserved for testing	22. Ring indicator
10. Reserved for testing	23. Data Signal rate select (DTE /DCE source)
11. Unassigned	24. Transmitter signal element timing (DTE - DCE)
12. Secondary received line signal detector Data signal select (DCE source)	25. Test mode
13. Secondary clearance to send	

Table 6.2 Functions of pins

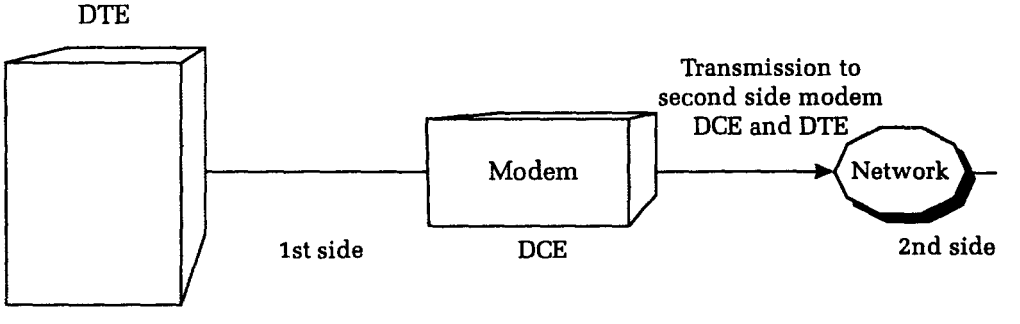


Fig. 6.10 DTE and DCE

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Steps involved

Steps		DTE	DCE		DTE	DCE
1.	Preparation	(1)	(1)			
		(7)	(7)			
2.	Readiness	(20)	(20)			
		(6)	(6)			
3.	Set up	(4)	(4)	Carrier →	2nd side (same step repeats with minor changes)	
		(5)	(5)	← Carrier		
		(8)	(8)			
4.	Data Transfer	(2) →	(2)	Data →		
		(24) →	(24)			
		(3) ←	(3)	Data →		
		(17) ←	(17)			
5.	Clearing	(4)	(4)	Carrier off →		
		(5) –off–	(5)			
		(8)	(8)	← Carrier off		

Note : Pin number details are given in the earlier figure. This figure is for synchronous full duplex transmission.

Fig. 6.11 Functioning of EIA -232

The figure is self explanatory.

Step 1 - Ensures preparation of the interfaces for transmission

Step 2 - Ensures all the devices (four) are ready for transmission

Step 3 - Ensures setting up of the physical connection between sending and receiving modems (DCEs)

Step 4 - Ensures data transfer procedure

Step 5 - Ensures clearing to send circuits (modems turn off their carrier signals, received line signal detectors)

Null modem cables

This enables transmission between two computers close to each other in a building say 6 to 8 feet apart, without using a modem. The null modem cable means, as the name itself says it eliminates the need for a modem. Modems are not needed to connect two compatible digital devices directly. The reason being the transmission never crosses analog lines such as telephone lines, hence no modulation is required. However, interface to handle the exchange of readiness establishment, data transfers, receipts etc. is needed similar to an EIA 232, DTE-DCE cables. If a diskette from one device do not fit into another device, and transmitting over telephone lines is impossible, or that you find that you cannot transmit data easily between devices for any other reason, null modem cable is an ideal solution.

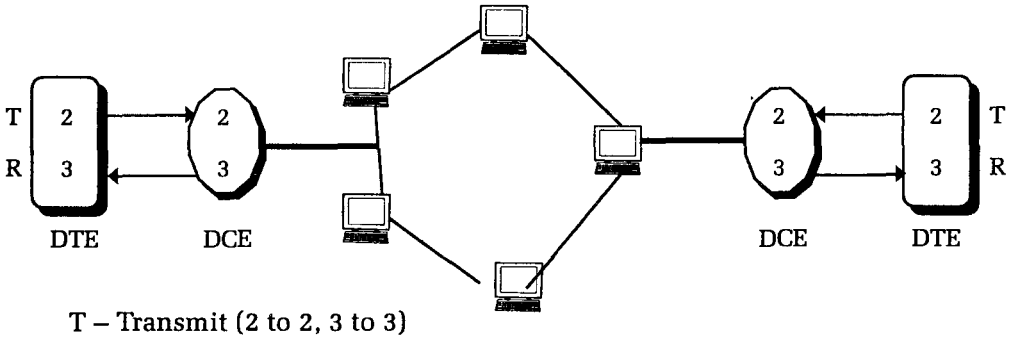
The question arises why a null modem is to be used? What happens if the same standard EIA 232 cable is used? In this case, since DCEs are not required

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

only DTE -DTE interface will be provided instead of DTE-DCE/DCE-DTE interface which would ultimately lead to a bad result as shown below:

Case 1 : Normal transmission: Smooth

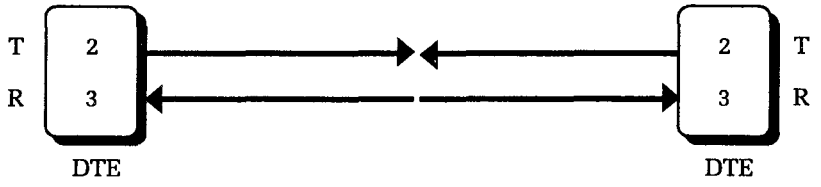


T – Transmit (2 to 2, 3 to 3)
R – Receive (3 to 3, 2 to 2)

Fig. 6.12(a) Normal transmission with DCEs

Case 2 : If only DTEs are used, bad results occur. (No DCEs provided)

Result : Full of collusion noise and signals that can never be received by either DTEs.



Here, T – Transmit 2/2 or vice versa 2/2
R – Receives 3/3 or vice versa 3/3

Fig. 6.12(b) Transmission without DCEs

In the case of null modem, to avoid the above transmission problem, cross connections are made. The wires are crossed so that the pin 2 of the first DTE is connected to pin 3 of the second DTE and also vice versa. In view of this several other pins may also have similar problems and needs reconnection.

The other major difference found i null modem is that unlike EIA 232 DTE-DCE interface cable (which has a male connector at the DTE end and a female connector at the DCE end), it has female connectors at both ends to allow it to connect to the EIA 232 DTE male ports. However, it has 35 pins as shown in figure 6.13.

The null modem cable runs from the serial communication port on the first micro computer to the serial communication port of the second one, by eliminating the need for a modem. This cable can be built by the user himself or buy one from any micro computer store. The main purpose is to switch pins 2 and 3 (Transmit and Receive) of the RS 232 connector plug.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

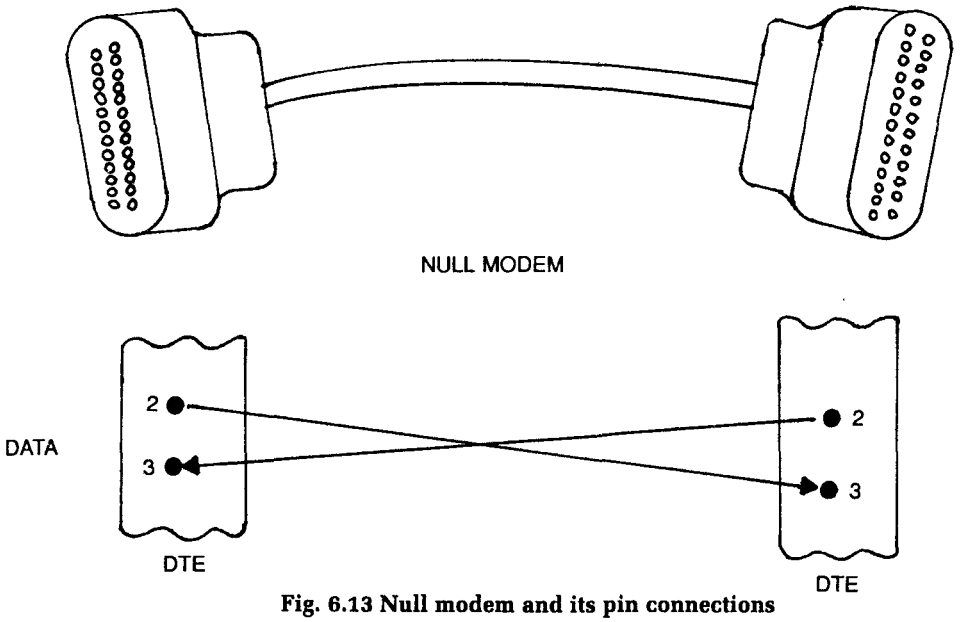


Fig. 6.13 Null modem and its pin connections

RS232 has a maximum of 50 feet cable length, but it can be increased to 100 feet or little more at users request by means of a special low capacitance, extended distance cable. This may have some problem, at the same time, the vendors hesitate to sign maintenance agreements.

The cable length varies according to the speed of transmission.

For example,

~ 900 m at 1200 bits/second
~ 550 m at 2400 bits/second
~ 120 m at 9600 bits/second

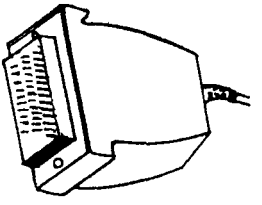
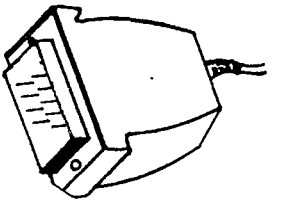
Note : If end users operate at maximum distances they should adhere to the restrictions on all types of equipment, used (such as electrical environment, cable construction, cable wiring etc.) and contact the modem/vendors to obtain the maximum cable distance.

EIA - 449/RS 449

On the contrary to EIA 232, the RS 449 standard, has been adopted as US Federal standard 1031. The RS 449 is as shown below in the figure 6.14. A 4000 foot cable length can be used; 37 pins are used instead of 25 pins (useful for digital transmission as in the case of EIA 232); Various other circuit functions are added (e.g.: Diagnostic circuits, digital circuits etc.); A secondary channel circuits (reverse channel) have been put into a separate 9 pin connector called as DB9. The serial port of your microcomputer may be a DB 9 or a DB 25. RS 449 is a new EIA specification augmenting RS 232 C. RS 449 provides for additional controlling and signalling. EIA 449 mechanical specifications define a combination of both the connectors one with 37 pins (DB 37) and the other with 9 pins (DB 9), for a combined 46 pins. DB 37 properties are similar to DB 25. The secondary channel of DB 37 is removed, as it is not used frequently and it is put in the second, 9 pin connector DB9. Thus, a second channel is available to systems for the needy users.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

MAIN CHANNEL 37 Pin connector		SECONDARY CHANNEL 9 Pin connector	
			
1. Shield	19. Signal Ground		EIA 232 equivalent
2. Signalling rate indicator	20. Receive common	1. Shield	1
3. Unassigned	21. Unassigned	2. Secondary receiver ready	–
4. Send data	22. Send data	3. Secondary send data	14
5. Send timing	23. Send timing	4. Secondary receive data	16
6. Receive data	24. Receive data	5. Signal ground	7
7. Request to send	25. Request to send	6. Receive common	12
8. Receive timing	26. Receive timing	7. Secondary request to send	19
9. Clear to send	27. Clear to send	8. Secondary clear to send	13
10. Local loop back	28. Terminal in service	9. Send common	–
11. Data mode	29. Data mode		
12. Terminal ready	30. Terminal ready		
13. Receiver ready	31. Receiver ready		
14. Remote loop back	32. Select stand by		
15. Incoming Call	33. Signal quality		
16. Select frequency/ signalling rate selector	34. New signal		
17. Terminal timing	35. Terminal Timing		
18. Text mode	36. Stand-by indicator		
	37. Send common		

Note : Underlined ones are different categories of pins used in exchanging of data, control and timing information.

Fig. 6.14 DB 37 and DB 9 connector

Two types of pins are used:

- Category 1 pin functions are compatible with those of EIA 232 functions. EIA 449 defines two pins, one in the first column, and one in the second column (Adjacent to each other that is 4, 5, 6 and 22, 23, 24).

Pins 4 and 22	Send data	Equivalent functionality
Pins 5 and 23	Send timing	
Pins 6 and 24	Receive data	

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

- Category II pins of EIA 449 have no equivalent in EIA 232

Pin No 10	Local loop back	– For testing local loop back
Pin No.14	Remote loop back	– For testing remote loop back
Pin No.16	Select frequency	– Select between two different frequency rates.
Pin No.20	Receive common	– Common signal return line for unbalanced circuits from DCE to DTEs.
Pin No.28	Terminal in service	– Indicates to the DCE about DTEs operational function.
Pin No.34	New signal	– Available for multiple point application if DTE (primary) controls several secondary DTEs.
Pin No.36	Stand by indicator	– Provides the confirmation signal from the DCE in response to select stand-by pin 32.
Pin No.37	Send common	– Provides a common signal return line for unbalanced circuits from DTE to DCE (opposite of pin 20).

Using pin 32 in select stand by on EIA 449, the terminal can instruct the modem to use an alternate stand-by network such as changing from a private leased line to a public network, both for back up or to access another database not normally in use. That is to say a terminal can be connected to two different networks and the operator can enter a keyboard command to switch the connection from one network to the other.

Using pins 10 and 14 (loop back), the terminal can allow basic tests without special test equipment or the manual exchanging of equipment or cables.

With microcomputers,

RS 232, RS 449 } are known as D type connectors

RS 232 may be called a DB 25

RS 449-9 pin may be called a DB9

The standards used for EIA 449 to define electrical specifications are:

RS 422 (For balanced circuits)

RS 423 (For unbalanced circuits)

RS 422 (Balanced mode)

This defines two lines for propagating each signal and use a common return (or ground) to complete the circuit. The conceptional view and specifications for this standard are as shown below: Here EIA 449 uses both the pins in 1st category but will not use the pins of 2nd category. In the case of Rs 423 unbalanced mode, it may be noted that first pin of each pair of category 1 pins and all category of 2 pins are used.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Comparison of RS 422 and RS 423

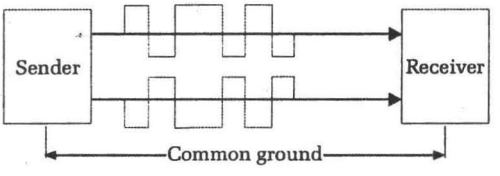
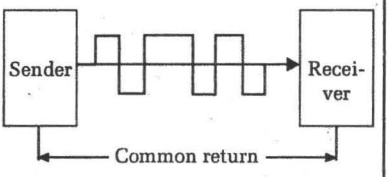
	RS 422	RS 423
(i)	Balanced mode	Unbalanced mode
(ii)	Defines 2 lines for propagation of each signal	Defines only one line for propagating a signal
(iii)	All signals in this standard use a common return (or ground) for the return of the signal	Same as RS 422
(iv)	EIA 449 utilises only the 1st pin of each pair of category 1 pins and uses all category 2 pins	Both pins in category 1 Does not work category 2 pins
(v)	Data rate to distance is 40 ft. → 10 Mbps 4000 ft. ← 1 Kbps	Data rate to distance is 40 ft. → 10 Mbps 4000 ft. ← 1 Kbps
(vi)	Two lines carry the same transmission not identical signals, but they are complement to each other (like a mirror image)  The receiver detects the difference between the two signals (put through a subtracter - a differential amplifier)	Only one line 
(vii)	This mechanism makes the circuit less susceptible to noise.	Here noise is more
(viii)	Improves performance and allows the superior data rates of balanced transmission after neutralising the effects of noise.	Performance comparatively less

Table 6.3 Comparison of RS 422 and RS 423

EIA-530

EIA-449 is functionally better than EIA-232, but needs a DB 37 connector which is expensive as the investment has already been put into DB 25. Hence EIA developed another version EIA-530 which uses DB 25 pins.

Under EIA-530, the pin functions are same as EIA-449 – category 1 plus three pins from category (the loop back circuits) EIA-530 does not support a secondary circuit. Out of the EIA-232 pins, certain pins have been omitted such as ring indicator, signal quality detector and data signal rate selector.

Copyright © 2009. Global Media. All rights reserved.

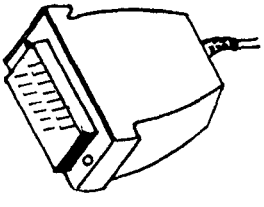
Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

X.20 and X.21

These are interface cables. X.20 interface is for asynchronous communications and X.21 is for synchronous communications. These are based on only 15 pins (wires) connecting DTE and DCE. Fewer pins need an increased intelligence in both DTE and DCE. X.21 interface standard is designed by the ITU-T to address several problems existing in the EIA interfaces and at the same time to suit for all digital communications. EIA interfaces are used for control. The standards implement control functions as separate signals. Thus, control informations with a separate line is represented by positive and negative voltage. If control signals are encoded using meaningful control characters from a system such as ASCII, they can be transmitted over data lines.

X.21 eliminates most of the control circuits, but direct, their traffic over the data circuits. Hence, to make this functionality possible, both DTE and DCE must have added circuit logic that enables them to transfer the control codes into bit streams that can be sent over the data line. The design makes X.21 not only to use fewer pins but also to be used in digital telecommunications, where control information is sent from device to device through a network than between a DTE and DCE. X.21 is useful both as an interface to connect digital computers to analog devices (modems) and as a connector between digital computers and digital interfaces such as ISDN and X.25.

X.21 is designed to work with balanced circuits at 64 Kbps.



DB-15 pins

Fig. 6.15 DB-15 pins

Advantages of a DB connector :

- To control byte synchronisation in addition to bit synchronisation (timing lines). A byte timing pulse (pins 7 and 14 are added).
- Improves the over all synchronisation of transmissions.
- Pins 3 and 5 are added for
  - initial handshake (equivalent of request to send)
  - agreement to begin transmitting (equivalent of clear to send)

Pin functions :

1. Shield
2. Transmit data or control
3. Control
4. Receive data or control
9. Transmit data or control
10. Control
11. Receive data or control
12. Indication

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

5. Indication
6. Signal element timing
7. Byte timing
8. Signal ground
13. Signal element timing
14. Byte timing
15. Reserved

13 most frequently used pins of RS 232 connector cable

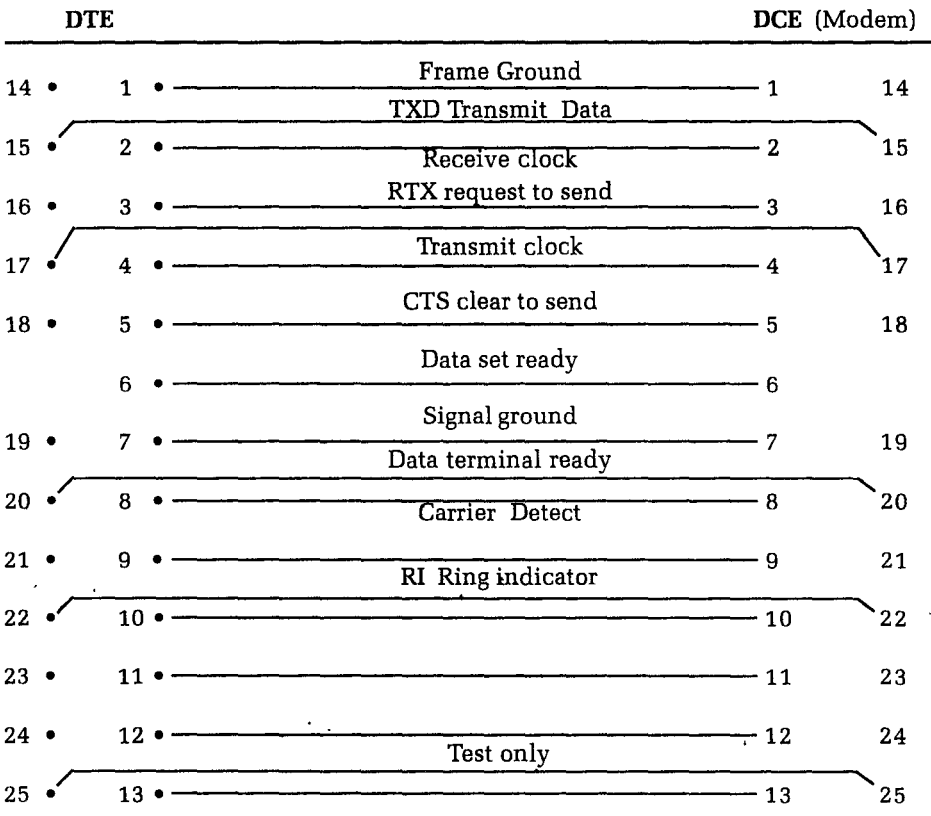


Fig. 6.16 RS 232 modem control (13 most used pins)

6.4 MODEMS

Modem is an acronym for Modulator /Demodulator. It is a composite world referring to two functions that make up the device:

- A signal modulator
- A signal demodulator

A modem is responsible in taking the digital electrical pulses received from a terminal or a computer and converts them into a continuous analog signal, which is very much needed for transmission over an analog voice grade circuit. Similarly a demodulator is another part of modem like modulator works in the opposite way. A demodulator converts an analog signal into a digital signal. A demodulator resembles an analog-to-digital encoder, but in reality it is not an encoder. It does not sample a signal but reverses the process of modulation. Modems are classified on the basis of speed at which they operate.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

The speeds are:

- 2400 bits per second
- 9600 bits per second
- 14400 bits per second
- 28800 bits per second

} Less expensive and operates on microcomputers Low speed (capable of transmitting or receiving)

- 14,400 bits per second
- 19,200 bits per second
- 38,400 bits per second
- 50,000 bits per second
- 56,000 bits per second
- 1,54,000 bits per second

} Expensive and operates on larger and more centralised networks High speed (capable of transmitting or receiving)

Though tremendous progress is being achieved in digital networks and the same is used extensively still modems are needed to pass data over thousands of currently installed analog circuits, since these cannot change over to digital for many years.

A modulator treats a digital signal as a series of 1s and 0s and hence can transform this into analog signal by using digital to analog mechanisms of : ASK, FSK, PSK and QAM which have already been described in chapter 5.

Figure 6.17 is self explanatory. Two PCs on either end represents DTEs. Two modems represent DCEs. DTE creates a digital signal which is converted to analog signal by DCE at the sender's end. The modulated signal is received by the demodulation function of the second modem (demodulator) to convert back to digital signal. The demodulator takes the ASK, FSK, PSK, or QAM signal and decodes into the format for the receiving computer to accept. It receives the resulting digital signal to the receiving computer via an interface. Either of the DCEs is compatible with both its own DTE and with other DCEs. It should also be noted that a modem must use the same type of encoding (NRZ-L etc), the same voltage level and the same timing conversions as its DTE.

Types of modems

Many categories of modems exist in the market. These are:

- V.22 which sends at 2400 bits per second using 2400 baud (one bit per baud using FM)
- V.32 which sends at 9600 bits per second using 2400 baud (one bit per baud using QAM)
- V.32 bits which sends at 14,400 bits per second using 2400 baud (six bits per baud using TCM)
- V.34 which sends at 28,800 bits/second.
- V.42 bits (If V.34 modem used along with this), could provide an effective data rate of 28,800 x 4 - 115 200 bps.

The data rate of a link depends on:

- The type of encoding used,

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

- The duration of the signal
- The size of the voltage used, and
- The physical properties of the transmission medium.

The physical properties of the transmission medium imposes greatest limitations. One method of increasing the speed of data transmission is to:

- Increase the speed (frequency) of the signal carrying it
- Faster the signal means increasing the number of changes per second, which is baud rate.

Every line based on the electrical qualities, accepts only a certain range of signal changes per second.

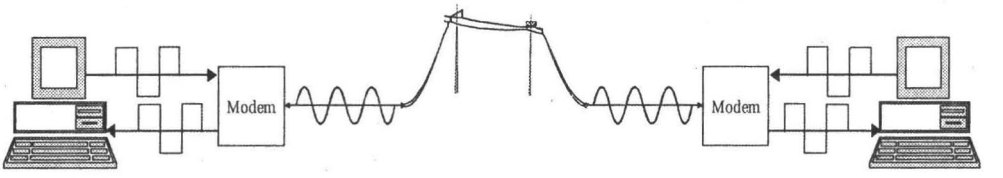


Fig. 6.17 Concept of modem

Every line has both upper and lower limits on the frequencies of the signals it an carry. This range is termed as the band width. Traditional telephone lines have frequencies between 300 Hz and 3300 Hz. (Band width is 3300 Hz – 300 Hz = 3000 Hz)

All of this range is used for transmitting voice. Telephone line for data transmission is between 600 Hz to 3000 Hz range. (Band width is 2400 Hz)

Band width for voice = 3000 Hz

Band width for data = 2400 Hz

We have already talked about ASK, FSK and QAM in the previous chapter.

ASK is for amplitude manipulation

FSK is for frequency manipulation; PSK is for phase manipulation.

QAM is for both phase and amplitude manipulation.

(a) The band width required for ASK transmission is equal to the baud rate of the signal.

(i) Max. baud rate in = Max. bit rate = 2400 (in half duplex ASK) = Band width a telephone line

(ii) Max. baud rate = Max. bit rate = 1200 (in full duplex ASK) = Band width in a telephone line available total = 2400 Hz (or band width available on either direction = 1200)

ASK is not used today because of noise, though it has a good bit rate.

(b) The band width required by FSK transmission is equal to the baud rate of the signal means frequency shift.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

(i) Max. baud rate = Max. bit rate = 2400 – (Frequency of shift) in a telephone line $f_{c1} - f_{c0}$

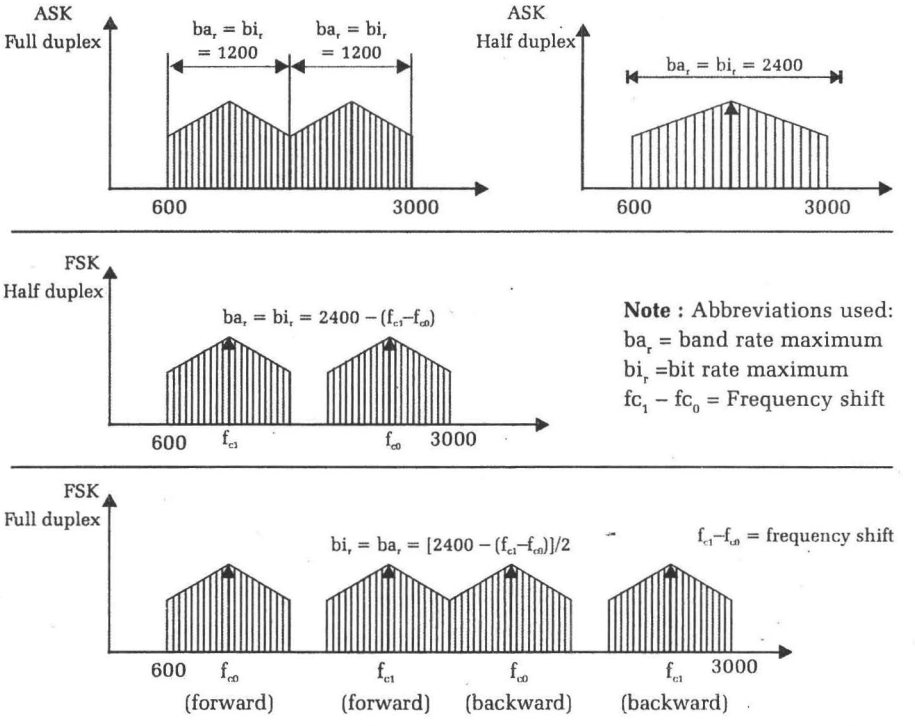


Fig. 6.18 Baud rates in ASK, FSK (Half/Full duplex)

The bid and band rate comparison has already been given in the previous chapter dialog to analog encoding. A similar table for half duplex and full duplex is given below:

Encoding	Bit rate	Half duplex	Full duplex
ASK, FSK, 2 PSK	N	2,400	1,200
4 PSK, 4 QAM	2 N	4,800	2,400
4 PSK, 8 QAM	3 N	7,200	3,600
16 QAM	4 N	9,600	4,800
32 QAM	5 N	12,000	6,000
64 QAM	6 N	14,400	7,200
128 QAM	7 N	16,800	8,400
256 QAM	8 N	19,200	9,600

[Multiply N by 2400 for half duplex
Multiply N by 1200 for full duplex]

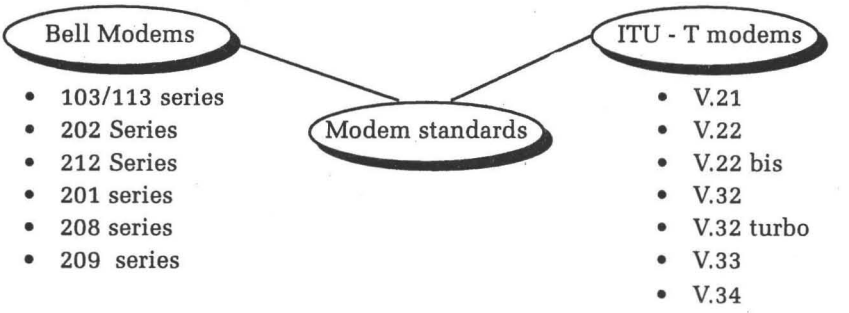
Table 6.4 Theoretical bit rates for modems

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Modem standards

Two types of modem standards are given below :



Modems can be classified as:

- Standard modems
- Short haul modems
- Intelligent modems
- Wireless modems

Bell Modems

In the early 1970 s, Bell telephone company introduced the first commercial modems. It provided a de facto standard since this was the first and the only company producing modems for a long time. Today, number of companies are producing modems.

Refer table 6.5.

ITU - T Modem standards

In the recent days, we find many of the modems which are based on ITU-T standards. ITU-T modems are compatible with modems of bell series and the same is as shown in the last row and of table 6.5 Bell modems.

ITU - T modems are compared in the table 6.6.

V.42 bis modems (Data compression)

A modem's transmission rate determines the through put rate of data. This is not the only factor. Data compression also increase through put of data over a communication link literally by compressing the data.

To compress data in a simple way is to examine it and send an instruction that provides a count of any characters which repeat themselves in sequence. This technique is called run length encoding and it is used normally combined with other techniques. One more technique is called code book compression uses specific codes to indicate a pattern of characters and phrases stored in each data compressor's memory. One character can be sent over a link to indicate many other characters. V.42 bis is the consultative committee on International Telegraph and Telephone (CCITT) standard for data compression.

Huffman encoding employs coding tables using a different number of bits to represent characters based on how often that character is used. This technique is a complex method of encoding replaces ASCII and EBCDI code standards. Adaptive Huffman encoding uses a mathematical algorithm to update the tables in real time to optimise the compression capability.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

103/113 series	202 series	212 series	201 series	208 series	209 series
• One of the earliest modem series • Operates in Full duplex mode • Two wire switched telephone lines. • Asynchronous transmission with FSK encoding • **Originator frequencies:** 1070 Hz = 0 1270 Hz =1 • **Answer frequencies:** 2025 Hz = 0 2225 HZ =1 Data rate = 300 bps • 113 series is a variation of the 103 series	• Half duplex mode • Two line switched telephone lines • Asynchronous with FSK encoding • One pair of transmission frequencies, used 1200 Hz = 0 2400 Hz = 1 • Secondary transmission frequency in both directions used 387 Hz ASK encoding data rate = 5 bps. • In 202, two frequencies used to send different bits in one directions.	• Operates on 2 speeds; 2nd speed allows compatability with a wider number of systems. Operates on full duplex mode. • Slower speed 300 bps, uses FSK encoding for asynchronous transmission. • Higher speed 1200 bps operates either in asynchronous or synchronous mode, uses 4 PSK encoding • Efficiency of transmission increases, by moving from FSK to PSK encoding. In 212, two frequencies represent two different directions of transmission. • The encoding is done by varying the phase on either frequency, (each of four phase shifts representing two bits).	• Half duplex mode • Two wire switched telephone lines or full duplex mode over four wire leased lines. Synchronous using a 4-PSK encoding (only one frequency is needed for transmission over each pair of wires. • Data rate is doubled to 2400 bps for 1200 baud) in both half and full duplex modes.	• Full duplex mode • 4 wire leased lines • Synchronous using 8 PSK encoding Live 201 series the 208 series, modem achieve full duplex status by doubling the number of kwires used and entire line to each direction of transmission. • Able to desting with between eight different phase shifts. • Band rate of 1600, transmits means a bit rate of 4800 bps.	• Full duplex mode • 4 wire leased line • Synchronous using 16 QAM coding • Achieves full duplex status by doubling the number of wires so that each direction of transmission has a channel • Allows for use of the entire band width of each channel. • Each shift represents a quad bit, with 16 QAM, the data rate in 9600 bps.
FDX FSK 100 1070 1270 2025 2225 3000 0 1 0 1 300 baud, 300 bps 2 wire	**HDX** ASK FSK 387 1200 2400 3000 0 1 1200 baud, 1200 bps 2 wire	**FDX** 4 PSK 600 1200 2400 3000 800 baud, 1200 bps 2 wire	**HDX/FDX** 4 PSK 600 1800 3000 1200 baud, 2400 bps 2/4 wire	**FDX** 8 PSK 600 1800 3000 1600 baud, 4800 bps 4 wire	**FDX** 16 QAM 600 1800 3000 2400 baud, 9600 bps 4 wire
V.21	V.23	V.22	V.26	V.27	V.29

Table 6.5 Bell Modems (Note V numbers of last row are equivalent ITU-T modems

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

V.22	V.22 bis	V.32	V.32 bis	V.32 terbo	V.33	V.34
• Standard modems used for many years. • Fast becoming obsolete. Transmit at either 1200 baud or 2400 baud (lower baud rate than a normal voice grade line of 3000 baud) • Less affected by noise • Uses frequency modulation (FSK) to send one bit/ baud resulting a data rate of 1200/ 2400 bps.	(bis means twice in Latin) • Second generation of V.22 series • Two speed modem • It can operate at 1200 or 2400 bps. • Speed depends on DCE'S speed at the receiver end. (if it receives at 2400 bps modem, it operates at 2400 bps mode for compatibility. **FDX** 4 DPSK 16 QAM 600 1200 2400 3000 600 baud 120/2400 bps 2 wire • In 1200 bps mode it uses 4 DPSK (dibit) encoding at a transmission rate of 600 baud. • In 2400 bps mode it uses 16 QAM (quadbit)	• Enhanced version of the V.29, uses a combined modulation and encoding technique called Trellis coded modulation and encoding technique. (QAM + a redundant bit) • Allows 5 bits per baud. • Calls for a 32 - QAM with a baud rate of 2400 The resulting speed is 4 x 2400 = 9600 bps **FDX** 32-QAM (Trellis) 600 2400 3000 2400 band 9600 bps 2 wire • Used with 2-wire switched line in pseudo duplex mode	• First of the standards to support, 14,400 bps transmission, uses 64 QAM transmission (6 bits per second) at a rate of 2400 baud (2400 x 6 =14,400 bps) • Automatic fall back and fall forward feature enables the modem to adjust the speed upward downward, depending on the quality of the line or signal. **FDX** 64-QAM 600 3000 2400 baud 14,400 bps 4 wire	• Enhanced version of V.32 bis (third version) uses 256 - QAM to provide a bit rate of 19,200 bps. **FDX** 256-QAM 600 3000 2400 baud 19,200 bps 4 wire	• Based on V.32, Uses trellis coded modulation based on 128-QAM at 2400 baud. • Each signal change represents a pattern of 7 bits and one redundant bit speed = 6 x 2400 =14,400 bps **FDX** 4096-QAM 600 1800 3000	• First of a new breed, developed based on telephone network, uses digital not analog transmission beyond the local loop. • V.34 uses baud rates above 2400 baud used by V.32 and V.32 bis. Actual baud rate depends upon the quality of the circuit (2700, 3000, 3300, 3600) **FDX** 4096-QAM 600 1800 3000 2400 baud 28,800 bps 4 wire • Standard speed is 28,800 bps with data compression can achieve speeds upto three times that rate. Also known as V. Fast.

Table 6.6 Comparison of ITU–T modems

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Frequently used characters may be defined as less number of bits and seldom used characters may be defined as more number of bits, e.g. letter E may be only 4 bits; letter X may be 11 bits.

V.42 bis specialities are :

- It uses a dictionary (commonly used 4 byte character combination); Instead of sending an actual data, it sends an index to the dictionary.
- Actual gain from V.42 bis compression depend on the actual data sent (ranges from 3.5 to 1 or 4 to 1 - almost 4 times data sent per second using V.42 bis than without it)
- It provides twice the data compression capability of MNP5 (a compression standard common in USA and is more established. The data compression ratio range in MNP5 is 1.3 : 1 and 2 : 1. This means that for every two characters in the original signal, only one is needed in the compressional signal; say 1000 bytes in the original signal needs only 500 in the compressed signal)
- V.42 bis compression can be added to almost any modem standard. This can provide a data rate of 57,600 bps when a V.32 modem providing a data rate of 14,400 bps is updated to V.42 bis. Similarly a V.34 bis modem provides 133.4 kbps with V.42 bis.

POINTS TO REMEMBER

- Digital communication is the transmission of discrete signals over a transmission channel. Digital transmissions can be either in parallel or serial modes. Serial transmission can be either synchronous, asynchronous, Isochronous.
- In parallel transmission, the internal transfer of binary data (consisting of 1s and 0s organised into groups of n bits each) takes place inside a computer. Here transmission takes place where in bits in a group are sent simultaneously, each using a separate link.
- In serial transmission, a stream of data sent over a communication circuit in a sequential way, bit-by-bit fashion (one bit at a time using only one single link)
- Asynchronous transmission is the transfer of data with start and stop bits) and a variable time interval between data units (variable length gap between each byte)
- In synchronous transmission, bits are sent one after another without start and stop bits or gap between bytes. Receiver takes the responsibility of regrouping the bits into meaningful bytes.
- Data terminal equipment (DTE) in a device serves as an information source or an information link. It is connected to a network through data circuit terminating equipment (DCE). DCE is a device that transmits and receives data in the form of an analog or digital signal through a network. DCE is a device used as an interface between DTE and a network. E.g. a modem is a DCE.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

- DCE includes signal conversion; coding between the DTE and the common carriers circuit. DTE includes the data source, the data link or both. DTE is any piece of equipment at which a data communication path begins and ends, such as a terminal.
- Many standards are available and have been developed between a DTE and DCE. Two important organisations involved in DTE - DCE interface standards are : Electronic Industries Association (EIA) and International Telecommunication Union-Telecommunication Standards Committee (ITU-T). The former involves EIA 232, EIA 442, EIA 449; the latter covers V and X series.
- EIA 232 earlier known as RS 232 standard (RS means recommended standard) also known as DB 25, since the mechanical standard defines the interface as a 25 wire cable with a male and female DB 25 pin connector attached at either end.
- Null modem cables enable transmission between two close computers to each other in a building say 6 to 8 feet apart, without using a modem. (compatible DTEs do not need network or modulation).
- EIA 449 known as RS 449 provides improved data rates and distance capabilities than EIA 232 standard with 37 pin connector (DB 37) used by the primary channel and 9 pin connector on the secondary channel known as DB 9. DB 37 pins have two categories pins (pins compatible with EIA 232 - as category I and pins not compatible with EIA 232 - as category II).
- The standards used for EIA 449 to define electrical specifications are RS 442 (for balanced circuits) RS 423 (for unbalanced circuits). RS 422 defines two lines for propagating each signal and use a common return (or ground) to complete the circuit. Signal degradation from noise is less a problem in RS 422 as compared to RS 423.
- EIA 530, the pin functions are same as EIA 449 category 1 plus three pins from category 2. It does not support a secondary circuit.
- X.20 and X.21 are interface cables. X.20 interface is for asynchronous and X.21 is for synchronous communications. These are based only on 15 pins connecting DTE and DCE.
- A modem uses ASK, FSK, PSK or QAM modulation to change digital signals to analog signals. A modem is an acronym for modulator/demodulator. These are classified on the basis of speed at which they operate 2400 to 28800 bits/second as low speed; High speed goes upto 1,54,000 bits/second and is very expensive. (A telephone line uses frequencies between 600 Hz to 3000 Hz for data communication requiring a band width of 2400 Hz).
- ASK has a good bit rate but not used today because of noise. FSK modulation needs more bandwidth as it has two carrier frequencies. PSK and QAM modulation have some advantages over ASK - one is noise and signal change represent more than one bit.
- Two types of modem standards are Bell modems and ITU-T modems. Bell modems are 103/113, 202, 212, 201, 208, 209 series; ITU-T modems are V.21, V.22, V.22 bis, V.32 terbo, V.33, V.34, V.42 bis modem known as data compression.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

QUESTIONS

1. Explain digital transmission
2. Which are the two modes of digital transmission?
3. What do you mean by parallel transmission?
4. What do you mean by serial transmission?
5. What are the different constituents of serial transmission?
6. Compare and contrast synchronous transmission, asynchronous transmission, isochronous transmission.
7. Define asynchronous transmission. Why it is so named?
8. Define synchronous transmission. What are its specialities?
9. What is the function of start and stop bit in an asynchronous transmission?
10. What is the function of data terminal equipment?
11. What is the function of Data Circuit terminating Equipment ? Give an example of DCE.
12. Compare and contrast DTE with DCE.
13. What does DTE and DCE composes of?
14. Mention two important organisations available for DTE–DCE interface standards and the interface developed by them.
15. Explain the following specifications of EIA 232
    a) Mechanical b) Electrical and c) Functional
16. Explain the functions of all pins in EIA 232 standard.
17. Which are the pins used for data transfer in EIA 232 standard?
18. Prior to data transmission, which pins are needed in EIA 232 standard for other activities?
19. What are the various steps involved in DTE–DCE interface?
20. List the pins used in the secondary channel?
21. Explain EIA 449 and the main channel.
22. What is secondary channel? What are its functions?
23. Which are the different categories of pins used in exchanging data, control and timing information of a 37 pin connector?
24. Explain the balanced mode RS 422 and the unbalanced mode RS 423. Compare and contrast.
25. Explain the function of EIA 530. Compare and contrast EIA 449 and EIA 530
26. Compare and contrast X.20 and X.21 interface cables.
27. Define a modem? What are its functions? How are they classified?
28. What are the different types of modems?
29. Which of the Bell modems use FSK modulation?
30. Which ITU-T modem standard uses trellis coding ?
31. Explain Bell modem. Compare and contrast different types of bell modems.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

32. Explain ITU-T modem standards. Compare and contrast different types of ITU-T modems.
33. What do you mean by trellis - encoding technique?. Why it is used?
34. What is data compression?
35. What do you mean by Huffman encoding?
36. Explain V. 42 bis modem. What are its specialities?

FILL IN THE BLANKS

1. Digital communication is the transmission of _____ _____ over a transmission channel.
2. The two modes of digital transmission are _____ and _____.
3. Under serial transmission, we have three types of transmissions _____, _____, _____.
4. If bits are transmitted over a single wire, one at a time, it is known as _____ transmission.
5. If bits are in a group sent simultaneously, each using a separate link, it is known as _____ transmission.
6. If the transfer of data is done with a start and stop bit frame a character byte, it is known as _____ transmission.
7. Synchronous transmission does not have a _____ and _____ bit.
8. In asynchronous transmission, the gap time between bytes is _____.
9. _____ transmission is also called as _____ transmission.
10. A _____ _____ _____ is a device serves as an information source or an information link for binary digital data.
11. A _____ _____ _____ _____ is a device that transmits or receives data either in the form of an analog or digital signal through a network.
12. One _____ do not communicate with another directly.
13. _____ takes the data generated by _____ at the physical level converts the data to an appropriate signal to pass on to the telecommunication link.
14. EIA 232 defines _____ _____ _____ characteristics of the DTE-DCE interface.
15. The EIA 232 standard specifies that 0 as a positive voltage _____ voltage using _____ encoding method.
16. The EIA 232 standard has _____ wires and with a _____ connector plug.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

17. In EIA 232 standard data transfer are done through pins _____ and _____.
18. Negative voltage represents _____ and operates from _____ to _____ volts in EIA 232 standard.
19. For local loop back testing pin _____ is used; for remote loop back testing pin _____ is used.
20. _____ has a maximum of 50 feet cable length, but can be increased to 100 feet at users request.
21. Category I pins functions are compatible with those of _____ pins in EIA 449, while category II pins have no equivalent for the same.
22. The standards used for EIA 449 to define electrical specifications are _____ and _____ for balanced and unbalanced circuits respectively.
23. With micro computers, RS 232, RS 449 are known as _____ connectors; RS 232 may be called a _____; RS 449–9 pin may be called a _____.
24. In the RS 422 circuit if the noise changes from 8 to 10 V, its complement is _____ volts.
25. If +2 volts of noise corrupts a bit is an RS 422 circuit _____ volts, will be added to the complementary bit.
26. EIA 449 balanced mode utilises both pins in each category ____ and does not use the category ____ pins:
27.

RS 422 (Distance/Data rate)	RS 422 (Distance/Data rate)
40 feet → 1 Kbps	40 feet → 1 Kbps
100 Kbps ← 4000 ft.	_____ ← 1 Kbps

28. X.20 interface is for _____ communications and X.21 interface is for _____ communications.
29. X.21 interface standard is designed by _____ to suit all digital communications.
30. X.21 eliminates most of the _____ circuits, but directs their traffic over the data circuit.
31. X.21 uses a DB _____ pins and DB ____ plug.
32. The band width required for ASK transmission is equal to the _____ _____ of the signal.
33. ASK has a good bit rate, but not used today because of _____.
34. The bandwidth for _____ transmission is equal to the _____ _____ of the signal minus frequency shift.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

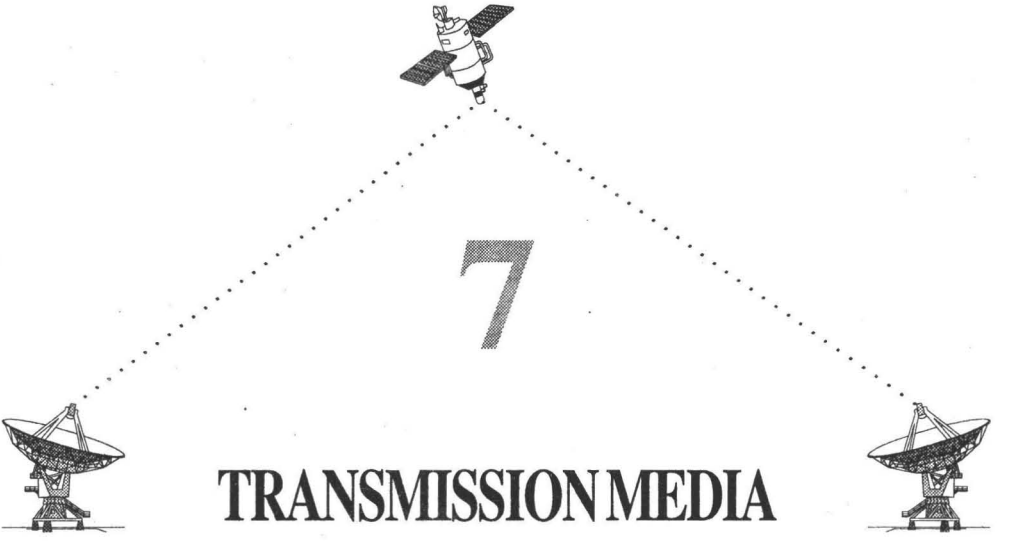
35. Bell modems use modulation techniques of _____, _____, _____, _____, _____.
36. Bell 103/113 series, 202 series uses _____ modulation.
37. ITU-T modem V.33 standard uses _____ coding.
38. Trellis encoding technique uses _____ _____ the number of transmitted bits.
39. The bit rate is always same as band rate in _____ type of signal.
40. The signal between two modems is _____.
41. Modulator converts a _____ signal to an _____ signal.
42. The bit rate for a _____ duplex is twice that of _____ duplex.
43. _____ is the CCITT standard for data compression.
44. Actual gain from V.42 bis compression is _____ times data sent per second using V.42 bis without compression.

Answers

1. discrete signals
2. parallel ; serial
3. synchronous ; asynchronous ; isochronous
4. serial
5. parallel
6. asynchronous serial
7. start ; stop
8. variable
9. Start ; stop
10. data terminal equipment
11. data circuit terminating equipment
12. DTE
13. DCE ; DTE
14. mechanical ; electrical ; functional
15. +3 ; NRZ–L
16. 25 ; DB 25
17. 2 ; 3
18. 1 ; –3 ; –15
19. 10 ; 14
20. RS 232
21. EIA 232
22. RS 422 ; RS 423
23. D type ; DB 25 ; DB 9
24. –2
25. +2
26. I ; II
27. 10 Mbps
28. asynchronous ; asynchronous
29. ITU-T
30. control
31. 15, 15
32. baud rate
33. noise
34. FSK ; baud rate
35. FSK ; ASK ; 5 PSK ; 8 PSK ; 16 QAM
36. FSK
37. trellis
38. more than
39. FSK
40. analog
41. digital analog
42. half, full
43. V.42 bis
44. four

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.



7

TRANSMISSION MEDIA

A data communications channel is a path through a medium that data can take to accomplish a communication task channels which are 'data highways' carrying signals from sending stations to receiving stations along predefined routes.

The *medium* (or media in plural) is the matter or substance that carries the voice or data transmission. Transmission Media can be divided into two broad categories :

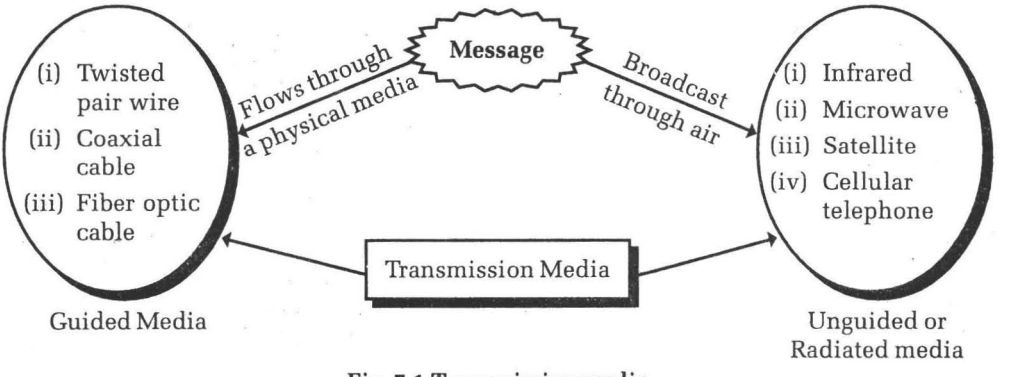


Fig. 7.1 Transmission media

The common media used in modern communications is shown in figure 7.1.

7.1 GUIDED MEDIA

As already shown in figure 7.1 *Guided Media* provides a physical connection (say a conduit) from one device to another device. The physical limit directs and restricts the signal travelling along these media. Twisted pair wire, coaxial cables

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

and fiber optic cables are the examples of guided media. In these, the first two uses metallic (copper) conductors for accepting and transporting signals whereas the last one, optical fiber is made of glass or plastic and transmits signals in the form of light.

Twisted pair wire : This is a pair of insulated, copper wires twisted into a single wrapped set. It is the basis of standard phone lines, commonly used for data communications as well as voice-grade communications. Special conditioned lines are also available to reduce transmission errors and increase transmission rate. It is ideal for both short and long distances and can be dedicated (reserved for only one user).

These are insulated pair of wires which are packed quite closely together. This consists of two copper conductors separated and within its own coloured plastic insulation (for identification within a cable to know which wires belong in pairs and their relationship in other pairs specially in a large bundle). Bundles of several thousands of wire pairs we might have observed under city streets and also in large buildings. The wire cables are generally twisted to minimise the electromagnetic interference between the pairs in the bundle. Wire cables are also replaced by more efficient transmission media as indicated above in Fig 7.1 under guided and radiated media (from coaxial cable to.. satellite) twisted pair cable are generally found in two forms (i) unshielded and (ii) Shielded. If the lines are run parallel, noise effect will be high since electromagnetic interference from devices such as a motor can create noise on the wires. (The wire closest to the noise gets more interference and will have a higher voltage than the other, resulting in an uneven load and a damaged signal.

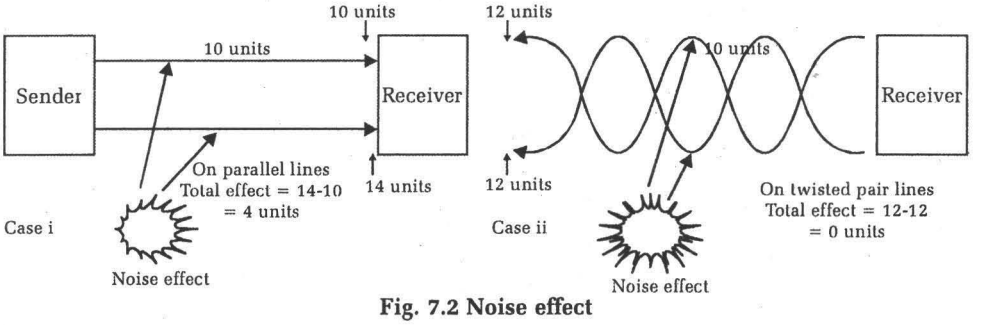


Fig. 7.2 Noise effect

Case (i) :

The noise at the line which is close = 14 units
The noise at the distant line = 10 units
Net effect = (14 – 10) = 4 units

Case (ii) :

The noise at both the lines will be 12 units since each wire comes closer to the noise surface for half the time. Average will be 12 units. The cumulative effect will be (12 – 12) = 0 units. However, it may be noted that twisting will not always eliminate the impact of the noise but definitely would reduce it.

Unshielded twisted pair (UTP) cable

It is a most commonly used cable in telephone system, its frequency range is suitable for transmitting both data and voice. It is widely used in telecommunication medium today.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Advantages are :

- (i) Less cost (ii) Ease of use
- (iii) Flexible (iv) Easy to Instal
- (v) Higher grades of UTP are suitable for LAN technologies (includes Ethernet & Token ring)
- (vi) Good Security (vii) Low error rates
- (ix) Transmission speed - Low, High

Five types of twisted pair cabling are available as per Electronic Industries Association (EIA) standards to grade them on the basis of quality. (1 is lowest, 5 is the highest).

Grades	Quality and application
1.	Telephone systems; Fine for voice, Inadequate for all but low speed data communication.
2.	Suitable for voice and for digital data transmission upto 4 Mbps
3.	Minimum of at least 3 twists per foot required, suitable for 10 Mbps. Ideal for most telephone systems.
4.	Same as 3 (to take the transmission up to 16 Mbps.
5.	Up to 100 Mbps.

A snap- plug similar to telephone jacks are used to connect UTPs to the network devices which are either male (plug type) or female (receptacle). A repressible tap known as key to have interconnection between male and female connectors and to lock them is used. For a four twisted pair, an eight conductor RJ45 connector is used.

Shielded twisted pair (STP) cable

STP cable using a metal foil or braided mesh covering encases each pair of insulated conductors which would help in preventing the penetration of electromagnetic noise. The noise on a line caused by signals travelling along another line is known as cross talk. It is the most undesired effect. This is observed sometimes when we are conversing with somebody (some other conversation is heard in between). Shielding prevents most of the effects of cross talk.

	UTP	STP
(i) Quality considerations	Identical	Identical
(ii) Connections	Similar	Similar (But shield connected to the ground)
(iii) Cost	Less	High (Because of material and manufacturing requirements)
(iv) Noise	Susceptible	Less susceptible

Coaxial cable (Coax)

It consists of copper or aluminium wires wrapped in one or more layers of insulating metallic and or fibrous sheathing, thus protecting the data carrying wires from external electrical static and noise. It is commonly used in LAN (Local Area Networks) and for undersea data communications.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

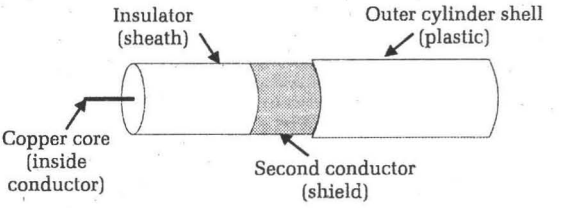


Fig. 7.3 Coaxial cable

Each coaxial cable has a copper core (the inner conductor) with an outer cylindrical shell (insulation). The outer shield just under the shell is the second conductor. Coaxial cable has more transmission capacity than a twisted pair cable and is more efficient (2" diameter coaxial cables can handle 20000 voice or data telephone calls simultaneously). These have very little distortion and are less prone to interference, and have low error rates. The outer metallic wrapping serves as the second conductor. It shields against noise. This second conductor is enclosed in a insulating sheath and is protected (using plastic material).

Every coaxial cable is defined by their radio government (RG') ratings. Each RG number denotes

- Unique set of physical specifications
- Wire gauge of the inner conductor
- Thickness and type of inner insulator
- Construction of the shield
- Size and type of the outer casing.

Each RG rating cable is adapted for a particular function.

E.g. RG 8, RG 9 and RG 11 are of ethernet (thick) and RG 58 for ethernet (thin), RG 75 is for TV.

Several connectors are found for use with coaxial cable from various manufacturers to seek specific solution for specific product requirements. Some are standardised e.g. barrel connector because of its shape. Under this, bayonet network connector is the most popular one known as BNC which pushes on and locks into place with just mere half turn. Others are either screwed together and needs more effort to instal or push on without locking and hence less secure. Every coaxial connector has a single pin protruding from the center of the male connector that slides into a female of the female connector. These are commonly found in cable TV and VCR hook ups (uses threaded and slip-on styles).

- In T-connectors, a secondary cable or cables would branch off from a main line. These are used in thin ethernet e.g. a cable running from a computer can branch to connect several terminals.
- Terminators used in bus topologies where the main cable would be like a backbone branches off to several devices (but does not itself terminate in a device). If main cable is left unterminated the signal terminated over the line echoes back and interferes with the original signal.

Optical fiber

This is a relatively new medium and is widely used. Instead of carrying telecommunication signals in the traditional electrical from, this technology utilises

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

high speed streams of light pulses from lasers of LEDs (Light emitting diodes) which carry information inside hair-thin strands of glass or plastic known as optical fibers.

These are long, thin, glass filaments that can conduct high frequency laser pulses. They are typically wrapped in cables and, because of the optical properties of the fibres, can bend light around corners without losing their signals. It is capable of carrying over ten times the amount of data as coaxial cable and over 1000 times that of microwaves. The limitation in the distance is approximately 50 KMS (unless there are repeaters to strengthen the signal); their size, weight and carrying capacity make them an important alternative to standard coaxial cable. These are not affected by electro-magnetic and hence ideal for factory applications and other installations where electrical interference might be a problem.

Plastic is used less rather than glass since the latter can be made into a purer product, enabling the signal to be transmitted over a greater distance. Extremely pure halide glass can increase the distance that fiber optic cables can travel.

Fiber optic technology is a revolutionaly departure from the traditional systems of copper wires or microwaves or satellites.

Advantages are :

(i) Can carry huge amounts of information at extremely fast data rates.

(ii) Huge capacities make it ideal for the simultaneous transmission of voice, data and image signals.

(iii) Less restricted under harsh environmental conditions than its metallic counterparts.

(iv) Not fragile or brittle as might be expected.

(v) More resistance to corrosion than copper (only hydroflouric acid affects)

(vi) Can withstand higher temperatures than copper (in cases of fire). A fiber optic system will be operational in an emergency signalling system, even if the outside jacket melts.

We all know that light is a form of electromagnetic energy travelling at 300,000 Kms/second (186000 miles/second) in a vacuum. The speed gets decreased if the medium through which the light travels becomes denser.

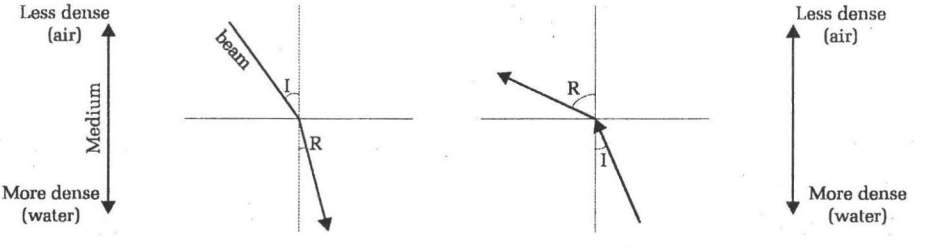


Fig. 7.4 Example of refraction

In the case of reflection, angle of incidence is equal to angle of reflection.

Optical fibers use reflection to guide light through a channel. The various propagation modes are (i) single mode and (ii) multimode.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

An average cable bundle contains about 72 fibres where as a large cable would have 144 fibres. In a building, a cable bundle use 24 to 36 fibers. The comparison of different modes are as under :

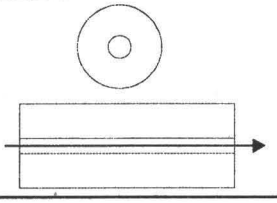
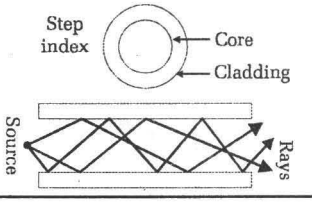
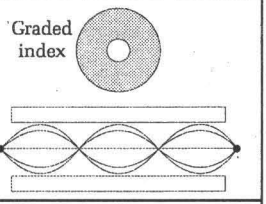
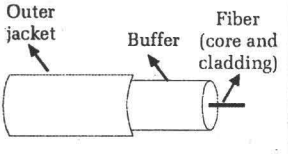
Single mode	Multimode	
		
(i) Transmit a single direct beam of light. (ii) Achieves higher performance (core diameter reduced from 50 microns to 8/10 microns) (iii) Small diameter core allows the fiber to send a concentrated light beam farther than multimode, since the light strikes the core/cladding boundary at a much smaller angle. (iv) Hence, less attenuation and dispersion. (v) It uses step-index fiber and manufactured with a much smaller diameter than multimode fibers and lower density (index of refraction) (vi) Density decrease results in a critical angle equal to 90° to make the propogation of beams almost horizontal. All of the beams at the destination arriving together can be recombined without distortion to the signal. (vii) Fiber type 8.3/125 with core 8.3 microns & cladding 125 microns is used for single mode 	(i) Earlier systems were multimode carried several light waves down the fiber at the same time. (ii) Excessive signal weakening (attenuation) and dispersion (spreading of the optical pulse). (iii) Multiple beams from a light source move through the core in different paths. (iv) The density of the core remains constant from the center to the edges. (v) Light beam moves in a straight line until it reaches the interface of the core and the cladding. (vi) Beams strike the interface of the core and cladding at an angle smaller than the critical angle. Such beams penetrate the cladding and are lost. Others hit the edge of the core at angles greater than the critical angle and reflect back into the core and off the other side, bouncing back and forth down the channel till they reach the destination. Step index means (suddenness of change) (vii) Every beam reflect off the interface at an angle equal to its angle of incidence. More bounces will be there if this angle is small and must travel farther to reach the destination. Hence different beams arrive at different times. These beams are recombined at the receiver, but the signal is not an exact replica of the signal that was transmitted. This is distorted by propogation delays. In the case of multimode fibre type 62.5/125, 50/125, 100/140 and core 62.5, 50, 100 and cladding (microns) 125, 125 and 140 are used.	Same as (i) and (ii) of step index Same as (iii) of step index (iv) Graded index decreases, the distortion of the signal through the cable. Index (here it is index of refraction) is related to density. Varying densities are found. Highest at the centre of the core-lowest at the edge only. The horizontal beam moves in a centre line through the constant density at the center. Density difference causes each beam to refract into a curve-varies the distance of each beam travels in a given period of time resulting intersection of beams at regular intervals.

Table 7.1 Comparison of different modes

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Optical fibers are defined as the ratio of :

$$\frac{\text{Diameter of their core}}{\text{Diameter of their cladding}} \text{(in microns)}$$

The core and cladding are made of either glass or plastic material with different densities. The inner core would be ultrapure, regular in size and shape. Any variations (material, size, shape, etc) would alter the angle of reflection and distort the signal. The outer jacket called as sheath can be of Teflon or plastic coating or fibrous plastic, metal tubing/mesh. The disadvantage with plastic is that it does not provide structural strength, emit fumes when burnt. But it is light and inexpensive. Alternatively metals are vice-versa. Teflon on the other hand is lightweight, but expensive and does not increase cable strength.

Connectors for fiber optic cable

There are several types of connectors developed by various manufactures to cover the following objectives :

(i) Precise and easy to use

(ii) Barrel shaped with male and female (cable is equipped with a more versions cable is equipped with a male connector that locks or threads into a female connector attached to the device to be connected).

(iii) Avoiding misalignment (of one segment of core either with another segment (or with a photodiode) results in the signal reflecting back towards the sender)

(iv) Avoiding difference in the size of the two connected channels (results in a change in the angle of the signal)

The light sources for optical cable can be either a light emitting diode (LED) or an injection laser diode (ILD)

(i) LEDs – Cheaper source, provides unfocussed light (strikes the boundaries of the channel at uncontrollable angles and diffuses) over distance limited to short distance use.

(ii) Lasers – Focused to a very narrow range allowing control over the angle of incidence. Preserves to character of the signal over considerable distances.

Advantages and Disadvantages of optical fiber

Advantages	Disadvantages
(i) Can be used for any type of network	(i) High cost
(ii) Moderate transmission	(ii) Installation/maintenance needs proper attention
(iii) Very good security	(iii) Fragility high (Glass fiber is easily broken)
(iv) Very low error rates	
(v) Very high transmission speed (high data rates)	
(vi) Noise resistance (immunity to noise)	
(vii) Less signal attenuation	
(viii) Higher band width	

Table 7.2 Advantages and disadvantages of optical fiber

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Unguided media (Radiated media)

Unguided media are wireless, media transport electromagnetic waves without using any type of physical conductor. *Radiated media* are the one in which the message is broadcast through the air such as infrared, microwave or satellite. E.g. Radio waves are used to transmit data and are usually propagated through the air.

Radio waves : Both microwaves and lower frequency radio waves can be used to create long distance satellite transmissions. Many communication satellites are in stable "parking orbits" approximately 22,300 miles above the earth. These Satellites are operated by private companies viz American Satellite Co., AT&T, COMSAT, Intellsat, RCA etc. The earth stations operated by these private carriers are located mostly in USA cities and project radio waves to the satellites. These signals are then reflected to other earth stations for distribution to computer users. This is also based on a long distance, line-of-sight communications medium.

Radio communication is divided into eight ranges (bands) as under :

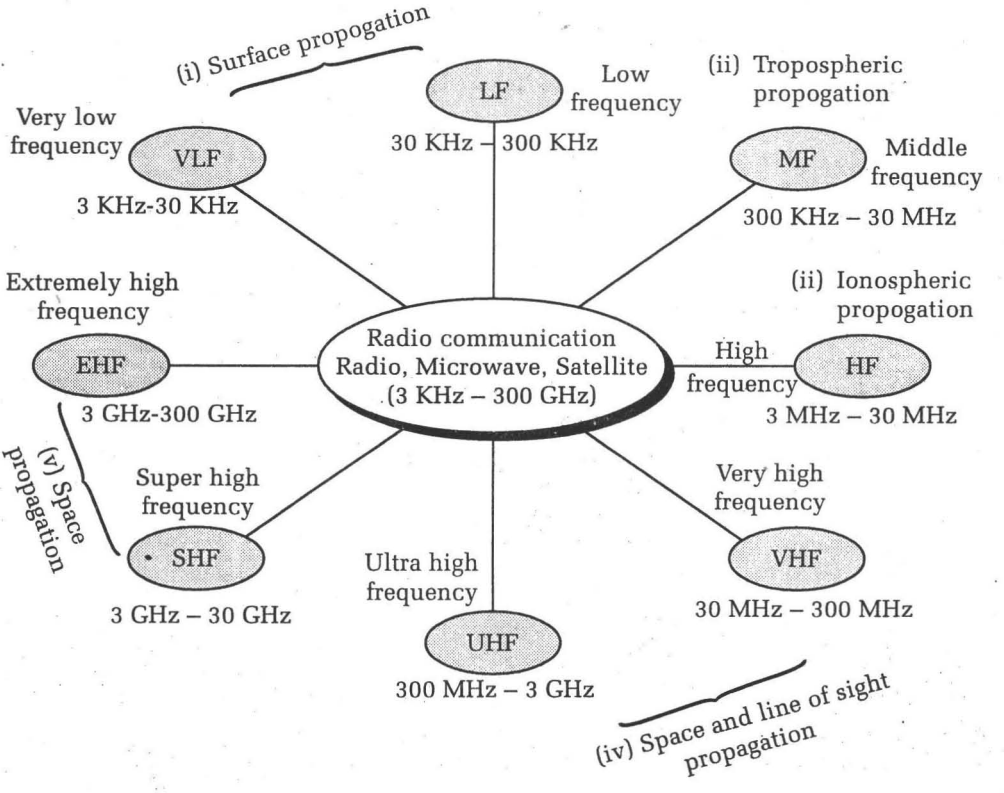
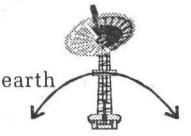
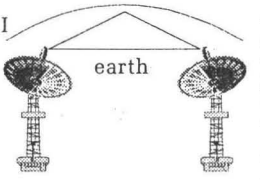
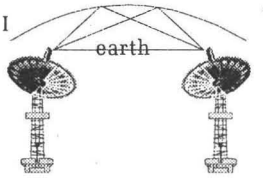
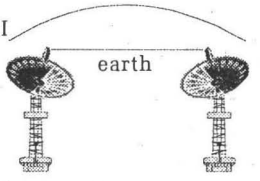
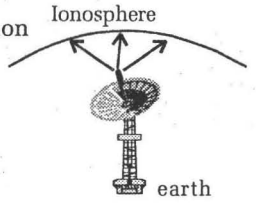


Fig. 7.5 Radio communication

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Types of Propagation	How it works
(i) Surface propagation (Troposphere) 	Radio waves travel through the lowest portion of the atmosphere. Signals emanate in all directions at lowest frequency from the antenna and follow the curvature. Distance is proportional to the power of the signal.
(ii) Tropospheric propagation (Troposphere) 	Antenna to Antenna in a straight line or can be broadcast at an angle into the upper layers of the troposphere where it is reflected back to earths surface. The former is to place the receiver and the transmitter within line of sight distances, limited by the curvature of the earth and the height of the antennas. The latter allows grater distances.
(iii) Ionospheric propagation (Troposphere) 	
(iv) Line of sight propagation (Troposphere) 	Very high signals are propagated in straight lines from antenna to antenna. Antennas are to be kept face to face (directions), tall and close enough (not to be affected by the curvature of the earth). It is tricky because radio transmissions cannot be completely focused.
(v) Space propagation (Troposphere)  I is Ionosphere	Utilises satellite relays instead of atmospheric refraction. A broadcasting signal reaches the orbiting satellite. The signal is rebroadcasted to the receiver back on the earth. It is line of sight transmission with an intermediary as satellite. It increases the distance coverable by a signal.

Radio technology considers the earth as two layers of atmosphere

(i) Troposphere – Portion of the atmosphere extending outside the earth about 30 miles from the earths surface – this is a high altitude layer and contains air, clouds, wind, temperature variations, weather occurs. Aeroplane travels.

(ii) Ionosphere – Portion above the troposphere; Beyond what we think of atmosphere, contains free electrically charged particles.

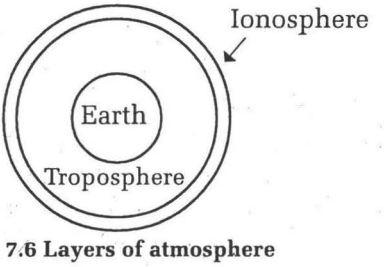


Fig. 7.6 Layers of atmosphere

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Signals

The comparision of different types of signals are as under :

Details	VLF	LF	MF	HF	VHF	UHF	SHF	EHF
Propogated	As surface waves (in air, sometimes water)	As surface waves (as VLF)	In the troposphere frequencies are absrobed by the Ionosphere	As ionospheric	As line-of-sight	Same as VHF	As line of sight & space	As space propagation
Long range radio navigation	Suitable	Suitable (For radio beacons or navigational locators)	Suitable for AM radio, mari time radio, radio direction finding and emergency frequencies	Suitable for amateur radio (Ham radio), citizens band (CB) radio	FM radio, aircraft, AM radio, aircraft navigational aid	Cellular radio	–	–
Submarine communication	Yes	–	–	–	–	–	–	–
Frequency range	3 KHz - 30 KHz	30 KHz - 300 KHz	300 KHz - 3 MHz	3 MHz - 30 MHz	30 MHz - 300 MHz	300 MHz - 3 GHz Microwave begins at 1 GHz goes upto 300 GHz	3 GHz - 30 GHz	30 GHz - 300 GHz
Attenuation in transmission	Not much	Greater during the day time	–	–	–	–	–	–
Atmospheric noise high levels (heat & electricity)	Susceptible active at low altitudes	–	–	–	–	–	–	–
Absorption problem	–	–	More during the day time (Rely on line-of sight antennas to increase control) and to avoid the absorption problem	–	–	–	–	–
Other applications	–	–	–	International broadcasting, military communication, long distance aircraft and ship communication, telephone, telegraph, fascimile	VHF television TV channels 2 to 6 (54 to 88 MHz) 7 to 13 (174 to 216 MHz) FM radio 88-108 MHz aircraft 8-174 MHz	UHF television, mobile telephone paging, microwave link UHF TV channel 14 to 69 470 to 806 MHz	Terrestrial and Satellite microwave Radar communication	Scientific including radar, satellite and experimental communication

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Microwaves transmission

Microwaves : These are high frequency radio waves that can transmit data signals up to 40 miles, commonly transmitted and received by antennas placed on tall buildings or hill tops. The waves travel in straight lines. Microwaves are a line of straight communications medium, requiring antennas to face one another exactly for accurate data reception. They travel freely in air and therefore do not require physical point to point connection. MCI corporation- a long distance telephone service uses microwave data transmission extensively.

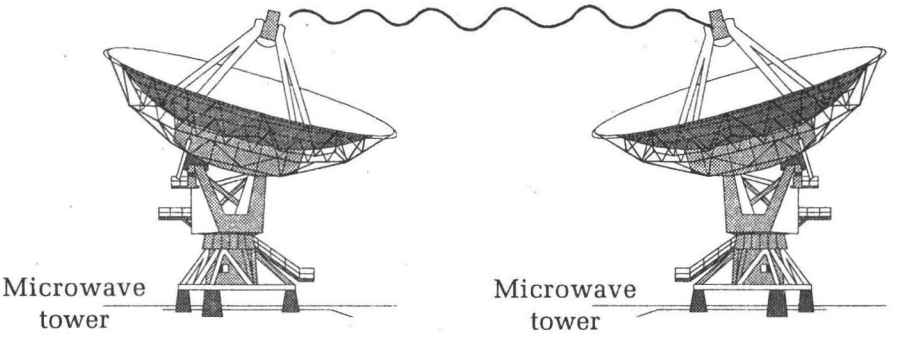


Fig. 7.7 Microwaves

A microwave signal is an extremely short wave length and hence the word MICRO wave. It performs the functions same as cables e.g., point A communicates with point B through the air microwave transmission path. They exhibit the same characteristics as light waves, such as reflection, focussing or reflection, since microwave signals approach the frequency of visible light waves. These signals can be focused into narrow, powerful beams that can be projected over long distances. A parabolic reflector focuses a high frequency into a narrow beam similar to a parabolic reflector focuses a search light into a beam. If the distance between the communication points is increased, towers are used to elevate the radio antennas to suit the earth's curvature and to maintain a clear line-of-light path between the two reflectors. Microwave acts as a carrier for innumerable number of simultaneous messages, may be for standard voice telephone calls or data transmission. It propagates one direction at a time (two frequencies are required for two communications as in telephones) each frequency requires its own transmitter and receiver (can be combined together as one piece known as a transreceiver) allowing a single antenna to serve both frequencies and functions.

Repeaters

These are used to increase the distance a microwave can travel. A system of repeaters are used with each antenna. Signals received at one antenna is converted into transmittable form before relaying to the next antenna. The distance between repeaters varies with the frequency of the signal and the environment in which the antennas are found.

Copyright © 2009. Global Media. All rights reserved.

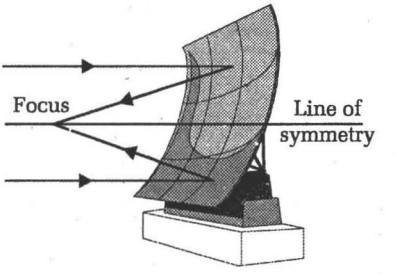
Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

ANTENNAS

Two types of antennas are :

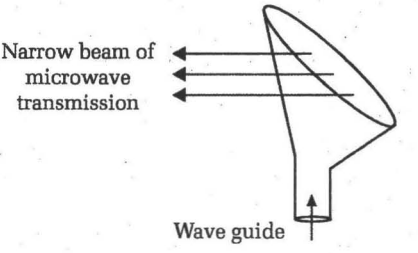
- **Parabolic Dish**

  Based on the geometry of a parabola. Every line parallel to the line of light reflects off the curve at angles. They intersect in a common point called focus. More of the signal would be possible with a single point receiver.



- **Horn antenna**

  A typical long distance horn antenna might be 10 feet wide, although over shorter distances in the inner cities, the dish antennas might be less than two-feet in diameter. It looks like a gigantic scoop. Out going transmissions are broadcast up a stem (like a handle) and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish.



SATELLITE COMMUNICATION

Satellite transmission is similar to transmission via microwave except instead of transmitting to another nearly microwave dish antenna, the transmission is done to a satellite 22,300 miles in the space.

Satellite transmission

(Satellite and earth stations with satellite dish. 22300 miles distance of transmission)

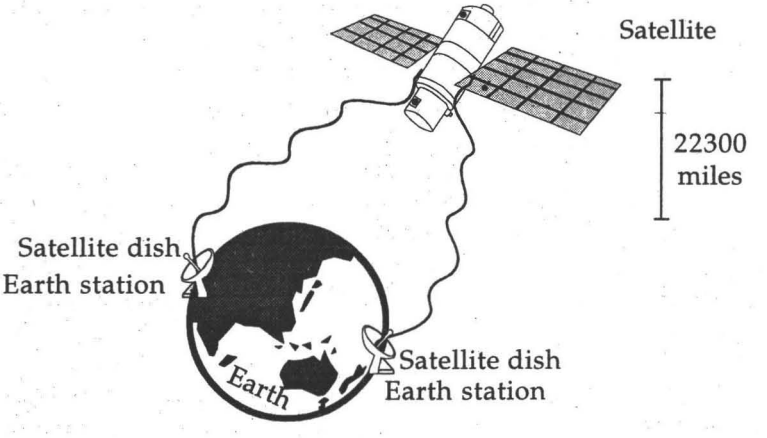


Fig. 7.8 Satellite transmission

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

These are extra terrestrial communications that pass messages between micro wave stations on earth. Satellites rotate more synchronously with the rotation of the earth and appear stationary to a ground observer.

VSTA (very small aperture terminals) are popular, relatively inexpensive and unobstructive satellite dishes.

Communication satellites

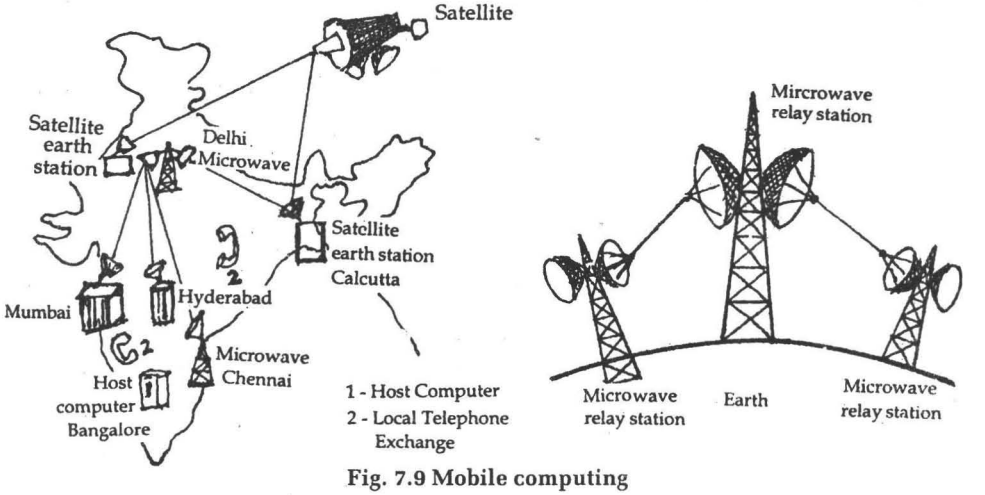


Fig. 7.9 Mobile computing

These were developed to reduce the cost of long distance transmission via terrestrial repeater stations as well as to provide a cheaper and better overseas communication medium than underseas cable. It is a microwave relay station in the sky with a signal to 6 GHz beamed to it from a transmitter on the earth. This is amplified and retransmitted to the earth at a 4 GHz by a system called a transponder mounted on the satellite. The retransmission frequency is purposely kept different as the powerful transmission signal will interfere with the weak incoming signal. It is a single microwave relay station visible from any where in the country. Transmission and reception can be between any two randomly chosen places. The bandwidth of signals which is handled by a transponder is about 36 MHz which would give 1200 voice channels, supporting 4800 bps data rate or 400 digital channels of 64 kbps each. This type of satellite provided with a number of transponders has enormous communication capabilities competing with microwave links on earth (works at a cost less than microwave).

Figure 7.8 shows that the satellite depicts a geosynchronous satellite 22,280 miles from earth revolving at the same speed as the earths rotation and hence remains stationary over one point on earth. The disadvantage of satellite transmission is the delay that occurs because the signal has to travel out in the space and back to earth (propagation delay). For half duplex transmission, the typical signal propagation time is approximately half a second for the round trip delay; that is from point A on the ground to the point B on the satellite and back to point A. This covers four links of 22,300 miles each and 4 times 22,300 (since the acknowledgement that the message was received without errors must do the reverse) divided by 1,86,000 equals 0.48 second, as Microwaves travel at 186,000 miles per second.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

The principle of satellite communication is the same as terrestrial microwave, with a satellite acting as a super tall antenna and a repeater. Satellite transmission signals must travel in straight lines, the limitations imposed on distance by the curvature of earth are reduced. Satellite relays allow microwave signals to span continents and oceans with a single bounce. The high quality communication can be made available to any underdevelopments places of the world without huge investment in ground based infrastructure. If satellites become expensive, leasing time or frequencies on one would be cheaper. It may be noted that one geosynchronous satellite is not sufficient to cover the whole earth, though it is possible to have line-of-sight contact with number of stations, but the curvature of the earth keeps much of the earth out of sight. Hence at least three satellites equidistant from each other in geosynchronous orbit would cover full global transmission (at 120⁰ around the equator). The view is from the north pole.

New Kuband satellites use waves that are so short they can be caught and concentrated in much smaller dish antennas, called very small aperture terminals (VSAT) which can be installed on any building (or vehicle). This network provides either one way or full duplex communications among VSATs installed at a large number of remote branch offices and a large earth dish or hub installed at a central site. Each satellite sends or receives over two different bands. Transmission towards the satellite from the earth is called uplink. Viceversa is downlink.

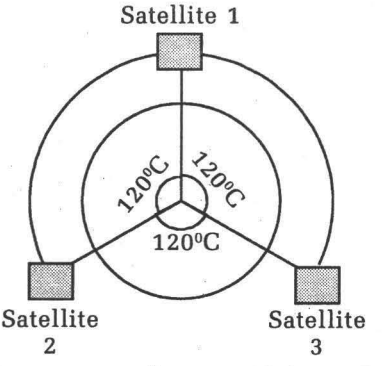


Fig. 7.10 3 satellites round the earth at 120⁰

Satellite frequency bands are as under :

Band	Down link (GHz)	Uplink (GHz)
C	03.7–04.2	05.925–06.425
Ku	11.7–12.2	14.000–14.500
Ka	17.7–21.0	27.500–31.000

Cellular transmission

(Switching station and cellular phone. Distance of transmission 8-10 miles)

Cellular Phones operate by keeping in contact with transmitter stations called cell station or cells. These stations resemble tall metal telephone poles and are operated by private franchises that have successfully applied to the government for licenses to provide public communication services, are strategically placed throughout a calling area. Cells perform two essential functions:

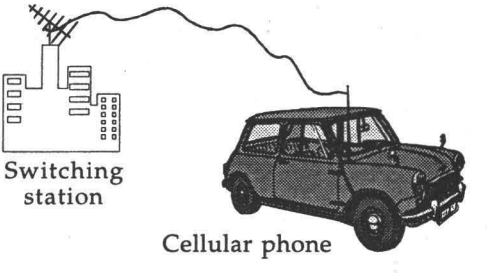


Fig. 7.11 Cellular transmission

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

- Provide an interface with the regular public phone network.
- Enable a moving vehicle with a phone to receive uninterrupted transmitting power by passing signals off to contiguous cells located in the zone into which the vehicle is moving.

Cellular technology maintains a quality transmission free from interference and eaves dropping. Cellular phones are not a complete departure from the past, they do provide one very alluring advantage over conventional telephones. They are not wired to a wall, they theoretically can put two people into contact with each other anywhere, even if they are in motion. You can even hook up a lap top computer to a modem on a cellular phone and gain access to huge database of information while you are far from an office or a regular phone. Here you will get billed for incoming calls also. Though cellular phones may be considered a luxury now, their prices are expected to come down.

Cellular telephony is designed to provide communication connections between two moving devices or between one mobile unit and one stationary (land) unit. The cellular network is also being used more and more often with telecommunication devices such as pagers and personal digital assistants (PDAS).

A service area or city is divided into small regions called cells each with its own antenna. Cellular telephony is a form of high frequency radio in which antennas are placed at strategical points throughout a metropolitan area. Each cell with its antenna is controlled by a small office called the cell office. Each cell office inturn is controlled by a switching office called a mobile telephone switching office (MTSO). This arrangement provides subscribers with reliable mobile telephone service of a quality almost that of a hardwired telephone system. Users (voice or data transmission) dial or log into the system and their voices or data are transmitted directly from their automobile, home or place of business to one of these antennas. Thus the cellular system replaces the hardwired local loop. The cell size is not fixed but can be varied depending on the population of the area. The typical radius of each cell is about 1 to 12 miles. High density areas require more, geographically smaller cells to meet traffic demands than lower density areas.

The system is intelligent. When you are driving your automobile, across any service are or city, you move away from one antenna and closer to another. The signal weakens at the first antenna and the second antenna automatically strengthens the signal by picking up your signal. Transmission is switched automatically to the closest antenna without communication being lost.

The problem with cellular telephone is anyone might be listening to your conversation. Calls are transmitted over the 870 to 890 MHz frequency bands, which are easily accessible by todays scanners. Thousands of people own scanners to do this mischief.

Many a times security EPROM is being taken out and replace it with thumb wheel EPROM substitutes to arrive at some other persons security code after adjustment, to make the telephone bill go to the other man which is known as cellular telephone fraud. Fraud penetrators use scanners and lap top micro computers to find large number of telephone codes automatically.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

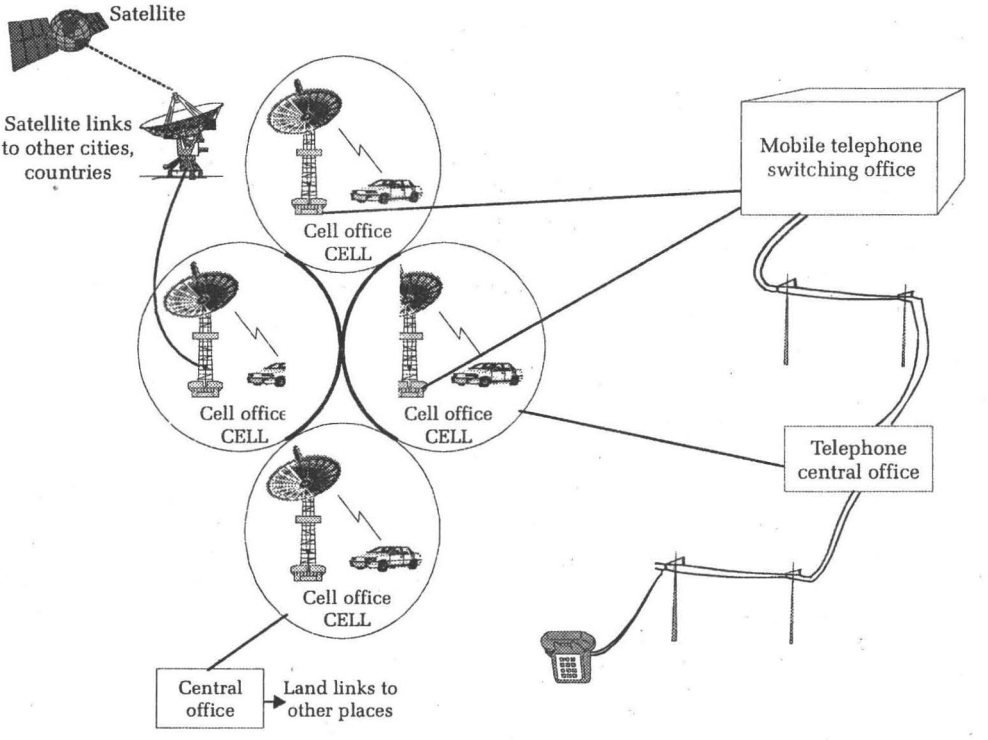


Fig. 7.12 Cellular radio system

Cellular bands

It may be noted that traditional cellular transmission is analog. In order to maximise noise immunity, frequency modulation (FA) is used for communication between the mobile telephone itself and the cell office. Two bands of cellular use identified by FCC are :

- Band between 824 and 849 MHz communications initiated from mobile phones – Divided into 416 channels.
- Band between 869 and 894 MHz – communications initiated by land phones – Divided into 416 channels.

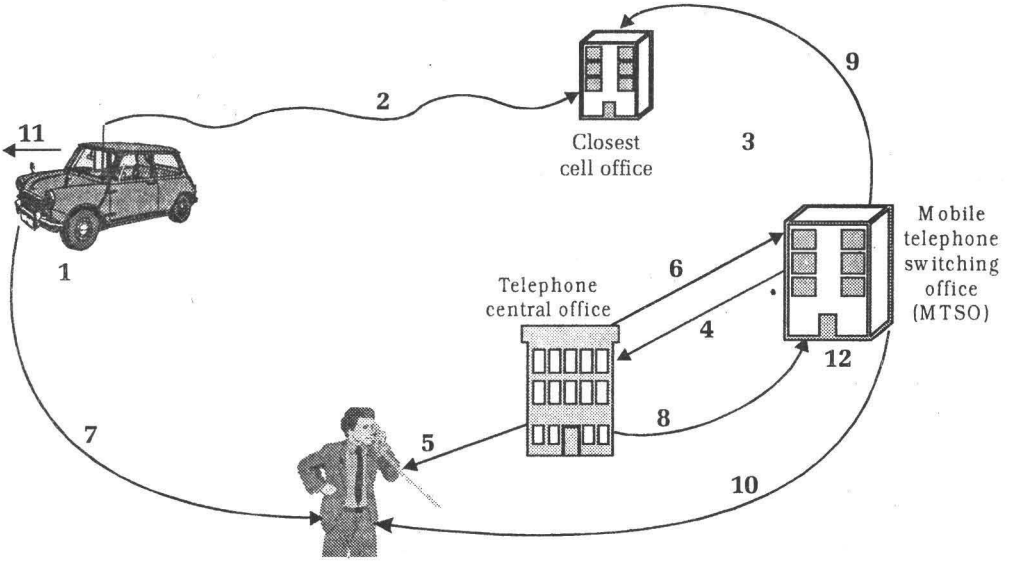
Carrier frequencies are spaced every 30 KHz allowing each band to support up to 833 carriers (Two carriers are required for full duplex communication, which doubles spacing to 60 KHz and leaves only 416 channels available for each band).

Each band is divided into 416 FM channels. Some are reserved for control and set up data rather than voice communication. To prevent interference, channels are distributed among the cells so that the adjacent cells do not use the same channels. This shows that each cell would have to access to only 40 channels.

Analog (FM) based cellular services are based on a standard known as Analog Circuit Switched Cellular (ACSC). In order to transmit digital data with ACSC service, a modem is required with a maximum speed of 9600 to 19,200 bps.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.



1. Caller enters a code of 7 or 10 digits (phone numbers) presses the send button
2. Mobile phone scans the band, seeks the setup channel with a strong signal sends the phone number to closest cell office
3. Relays the data to MTSO
4. Sends the data to telephone central office
5. Party is getting contacted.
6. Result back -1
7. Mobile phone automatically adjusts its tuning to be new channel and voice communication starts
8. Assigns an unused voice channel; connection established.
9. Searches for the location of the mobile phone by sending query signals to each cell in a process called paging.
10. The mobile phone is found. MTSO transmits a ringing signal. Mobile phone is answered. Assigns a voice channel to the call. Voice communication begins.
11. Mobile phone moving to a different cell. The signal becomes weak.
12. MTSO monitors the level of the signal every few seconds. If the signal strength gets reduced MTSO seeks a new cell for better communication. MTSO changes the channel carrying the call (hands the signal off from the old channel to a new channel). User do not observe the hand offs which are smoothly done.

Fig. 7.13 Stages of working of a cellular phone

The cellular data standard used at present is cellular digital packet data (CDPD) which provides low speed digital service over the existing cellular network and is based on the OSI model. CDPD also uses a trisector for 56K switched service to use the existing digital services which is a combination of three cells of 19.2 kbps, for a total of 57.6 (accommodated on a 56 K switched live by eliminating certain overhead). Whole of USA is divided under this into 12000 trisectors with one router for every 60 trisectors

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Cellular telephony is keeping a fast pace and is integrating the existing system with satellite communication (Fig. 7.12). This integration is possible to communicate between any two points on the globe. One more goal is to combine both cellular telephony and personal computer communication, a scheme named as mobile personal communication to enable people to use small mobile PCs to send and receive data, voice, image, video etc.

Media selection

While evaluating a media for a specific application following factors are to be examined :

- Cost
- Transmission speed
- Type of Network
- Error rates
- Attenuation
- Security
- Electromagnetic Interference (EMI)
- Transmission distance

(i) **Cost** is an important factor for decision. As new technologies evolve, competition among vendors drives prices down and costs changes. Twisted pair wire is the cheapest, Fiber optic cable is the most expensive.

(ii) **Transmission speed :** This varies with the different media. Its difficult to specify speed for different media, as transmission speeds are continuously improving. Speed is the maximum number of bits per second, a medium can transmit reliably and varies with the frequency (Higher frequency means more bits per second it can transport), with the physical size of the medium/ transmission equipment and with the conditioning of the conductor.

(iii) **Type of network :** Certain media are used only for a particular type of network. Some others could be for any type.

(iv) **Error rates :** Radiated media are most susceptible to interference and hence have higher rates. Fiber optics provides lowest rate under guided media.

(v) **Attenuation :** Electromagnetic signal tends to become weak or distorted as the distance increases. The signal's energy is absorbed or dissipated by the medium itself (emits in the form of heat).

(vi) **Security :** Radiated media are the least secure since their signals are intercepted. Protection against eves dropping required. Unshielded twisted pair cable are easily intercepted. Optical fiber is more secured.

(vii) **Electromagnetic Interference (EMI) :** The susceptibility of the medium to external electromagnetic energy if inadvertently introduced onto a link will interfere with the intelligibility of a signal. The effects of EMI are static in audio and snow in visual.

(viii) **Transmission distance :** The distance to which data as transmitted varies on the media; coaxial cable transmits data 100 to 300 meters. Fiber optic cable can transmit up to 40 KMS. If longer distance data transmission is required, cost increases & more devices to be added.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Transmission media summary

Media → / Factors ↓	Twisted Pair		Coaxial cable	Optical Fiber	Radio	Micro Wave	Satellite	Cellular
	UTP	STP						
Cost	Low	Moderate	Moderate	High	Moderate	High	High	High
Speed	Low	Low-High	Low-High	High-very High	Low-High	Moderate	Moderate	Moderate
Type of Net work	LAN	LAN	LAN	ANY	WAN	WAN	WAN	WAN
Error rates	Low	Low	Low	Very Low	Highest	Low - Moderate	Low-Moderate	Low-Moderate
Atten-uation	High	High	Moderate	Low	Low-High	variable	variable	Low
Security	Low	Low	Low	High	Low	Moderate	Moderate	Low
EMI	High	Moderate	Moderate	Low	High	High	High	Moderate
Trans-mission distance	Short	Short	Short	Moderate	Moderate	Long	Long	Long

POINTS TO REMEMBER

- Electromagnetic spectrum consists of power, voice; radio communication (Radio, Microwave, Satellite); Infrared light; visible light; ultraviolet light; X, gamma cosmic rays.
- Transmission medium is the physical path linking two communication devices. Transmission media are usually categorised as (i) Guided media and (ii) Unguided or radiated media. A guided medium contains physical boundaries, while an unguided medium is boundless. The most popular type of guided media are : Twisted pair wire, coaxial cable, Fiber optic cable. Similarly, the most popular unguided media are : Infrared, Radiowaves, Microwave, satellite, cellular telephony. Twisted pair cable and coaxial cable are metallic whereas optical fiber is of glass or plastic.
- Twisted pair cable is of two types : Unshielded twisted pair (UTP) cable, Shielded twisted pair (STP) cable. Shielded twisted pair consists of insulated twisted pairs encased in a metal shield or braided mesh covering. Twisted pair cable have two insulated copper wire twisted together. Twisting makes each wire to have approximately the same noise environment.
- UTP is cheap, flexible and easy to instal as compared to STP.
- Coaxial cable has five layers : A metallic rod known as inner conductor at the center, insulators to cover rod and shield; a metallic outer conductor (shield), a plastic cover. Coaxial cable in a similar way to twisted pair cable transmit data in the form of an electric current.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

- Fiber optic cable is made of glass or plastic and transmits signals in the form of light. Fiber optic technology takes the advantages of the properties such as refraction, critical angle and reflection. The propagation modes are of two types : Single mode and multimode. Multimode in turn can be implemented in two forms. Step index or graded - index. The light sources for optical cable can be either a light emitting diode (LED) or an Injection Laser Diode (ILD).
- Fiber optic cables are surrounded by cladding all encased in an outside jacket. The signal is propagated along the inner core by reflection. It is increasingly popular due to its noise resistance, low attenuation and high band width capabilities.
- Single mode transmits a single direct beam of light. In multimode, multiple beams from a light source move through the core in different beams. In step index, every beam reflect, off the interface at an angle equal to its angle of incidence. More bounces will be there if this angle is small and must travel farther to reach the destination. These beams are recombined at the receiver, but the signal is not an exact replica of the signal that was transmitted. Graded index decreases the distortion of the signal through the cable. Index is related to density.
- Radiated media or unguided media are wireless, media transport electromagnetic waves without using any type of physical conductor. Radiated media are the ones in which the message is broadcast through the air such as infrared, microwave or satellite.
- The various types of propagation are :
  - (i) Surface propagation (Troposphere) with VLF & LF (3 KHz to 30 KHz and 30 KHz – 300 KHz) follows the contour of the earth.
  - (ii) Tropospheric propagation (Troposphere) with Middle frequency (300 KHz to 30 MHz) with Ionosphere as the upper band.
  - (iii) Ionospheric propagation (Troposphere) with high frequency (3 MHz – 30 MHz) travels to the Ionosphere and reflected back.
  - (iv) Line of sight propagation (Troposphere) with very high frequency and ultrahigh frequency (30 MHz – 300 MHz and 300 MHz to 3 GHz)
  - (v) Space propagation (Troposphere) with super high frequency and extremely high frequency (3 GHz–30 GHz) and (30 GHz to 300 GHz)
- Microwaves use line of sight propagation for data transmission. Repeaters are used to increase the distance and a microwave can travel. Two types of antennas used for transmission and reception are (1) parabolic dish and (2) Horn antenna
- Satellite communication uses a satellite in geosynchronous orbit to relay signals. A system of three correctly spaced satellites (120^0 to each) can cover most of the earth Geosynchronous orbit occurs at the equatorial plane at 22,300 miles above the earth.
- Cellular telephones are designed to provide communication connections between two moving devices or between one mobile unit and one stationary

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

(land) unit. The cellular system consists of mobile phones, cells, mobile telephone switching offices, telephone central office and land phones. Now a days, satellite communication links also provides to integrate with the existing system which enables communication between any two points on the globe.

QUESTIONS

1. What do you mean by data communications channel?
2. What is transmission media? Explain.
3. What are the two types of transmission media? Give examples for the same.
4. Compare and contrast guided media with unguided or radiated media.
5. Explain twisted pair cable and its application.
6. What are the two different types of twisted pair cable? Explain them.
7. Compare and contrast UTP and STP. Write down the advantages.
8. Explain coaxial cable and its application.
9. What are the different types of connectors and terminators used along with coaxial cable?
10. Explain optical fiber and its application. What are its components?
11. Compare and contrast twisted pair cable, coaxial cable and optical fiber.
12. Explain what cross talk is and how it is created? What is needed to reduce it?
13. Why should the light be reflective instead of refractive in fiber optics?
14. Which are the layers in the atmosphere? What types of radio communication utilise these?
15. If the speed of light is 186,000 miles/second, and a satellite is at geosynchronous orbit, how much minimum time would it take for a signal to go from the earth station to the satellite?
16. What is Ionosphere? How does Ionospheric propagation work? What are the uses for this type of propagation?
17. What is LED and ILD?
18. What is microwave transmission? Why repeaters are used in a microwave transmission. Mention the two types of antennas used?
19. In what way satellite transmission is similar to microwave transmission?
20. What do you mean by Kuband satellites?
21. Why cellular telephony is becoming popular? Explain how it operates?

FILL IN THE BLANKS

1. Transmission media are categorised as _____ or _____.
2. Twisted pair cable, coaxial cable and fiber optic cable come under _____ media.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

3. Frequency range for twisted pair cable varies from _____ Hz to _____ MHz.
4. _____ cable consists of an inner copper core and a second conducting metal shield.
5. Two types of twisted pair cable are _____ and _____.
6. In fiber optics, the signal source is _____ waves.
7. Frequency range of coaxial cable varies from _____KHz and _____MHz.
8. In twisted pair cable the total effect of noise at the receiver end becomes _____.
9. Twisted pair cable and coaxial cable transmit data in the form of an _____.
10. _____ _____ _____ _____ primarily uses guided media.
11. At the beginning of the electromagnetic spectrum we have _____ ___ _____ and at the end where frequency is high we have __ _____ _____ _____.
12. With high voltage devices, the best transmission would be _____ _____.
13. _____ cable has more transmission capacity than a twisted pair cable and is more efficient.
14. The major factor that makes coaxial cable less prone to noise is the _____ _____ _____.
15. RG number denotes _____ _____ ratings and is used for _____ cable.
16. The information is carried in optical fiber is through strands of _____ or _____.
17. The core and cladding of optical fiber are made up of glass or plastic material with different _____.
18. Any variations on the _____ _____ would alter the angle of reflection and distort the signal.
19. Geosynchronous satellites move at the same speed as the _____.
20. Orbital speed is based on distance from the planet, only one orbit can be _____. The orbit occurs at the _____ _____ and occurs at approximately _____ miles from the surface of the earth.
21. _____ dish is based on the geometry of a parabola
22. Radio technology considers the earth as two layers of atmosphere. These are _____ and _____.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

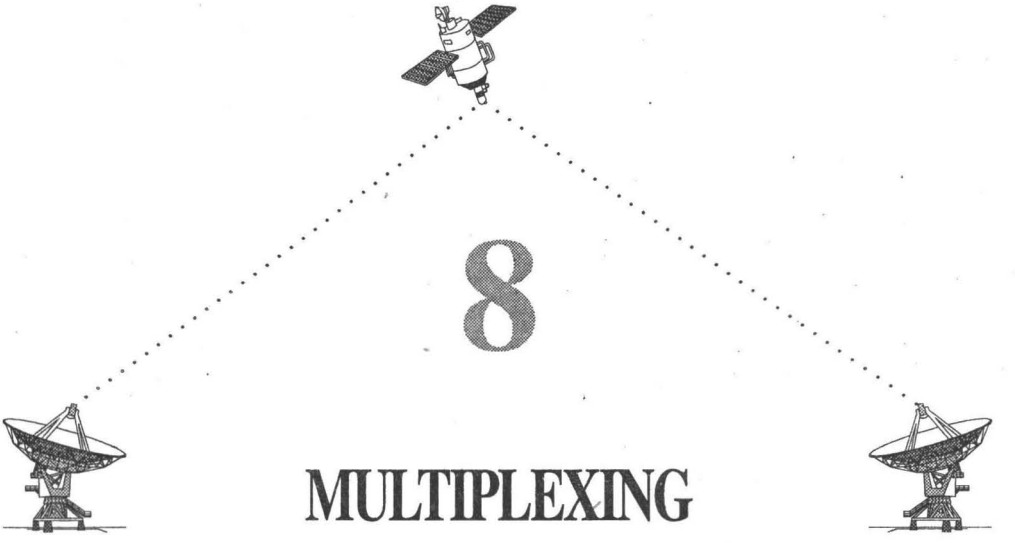
23. A beam of light travels through media of two different densities, if the angle of incidence is greater than the critical angle, _____ takes place.
24. If angle of refraction is _____ than the angle of incidence, the light beam is travelling from a more dense to a less dense medium.
25. If the angle of refraction is 90 degrees and the angle of incidence is 45 degrees, the critical angle is _____ degrees.
26. If the angle of refraction is 70 degrees and the angle of incidence is 45 degrees, the critical angle must be greater than _____ degrees.
27. _____ node transmit a single direct beam of light.
28. The light source for optical cable can be either a _____ or an _____.
29. In cellular telephony, a service area is divided into small regions called _____. Cell size is determined on the basis of _____ of the area.
30. The MTSO searches for the location of a mobile phone, which is called _____.
31. MTSO monitors the level of the signal every few seconds. If the signal strength is less, it seeks a _____ _____ for better communication and changes the channel carrying the call known as _____ ____.
32. In a _____ _____ _____ propagation, the core is of varying densities.

Answers

1. guided ; unguided
2. guided
3. 100 ; 5
4. Coaxial cable
5. shielded ; unshielded
6. light
7. 100 ; 500
8. zero
9. electric current
10. unshielded twisted pair cable
11. Power and voice, X gamma cosmic rays.
12. optical fiber
13. Coaxial
14. outer metallic wrapping
15. radio government ; coaxial
16. glass ; plastic
17. densities
18. inner core
19. earth
20. geosynchronous ; equatorial plane ; 23000
21. Parabolic
22. troposphere ; ionosphere
23. refraction
24. greater
25. 45
26. 45
27. Single
28. LED ; ILD
29. cells ; population
30. paging
31. new cell ; hands off
32. graded index multimode

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.



8

MULTIPLEXING

8.1 MULTIPLEXING

Multiplexing is the process of combining signals from multiple sources for transmission across a single data link. It is usually done in multiples of 4, 8, 16 and 32 simultaneous transmissions over a single communication circuit. Multiplexing a voice telephone call means that two or more separate conversations are sent simultaneously over one communication circuit between two different cities.

To multiplex is to place two or more simultaneous transmissions on a single communication circuit. In a multiplexed system, number of devices share the capacity of one link. A multiplexed circuit is as shown below :

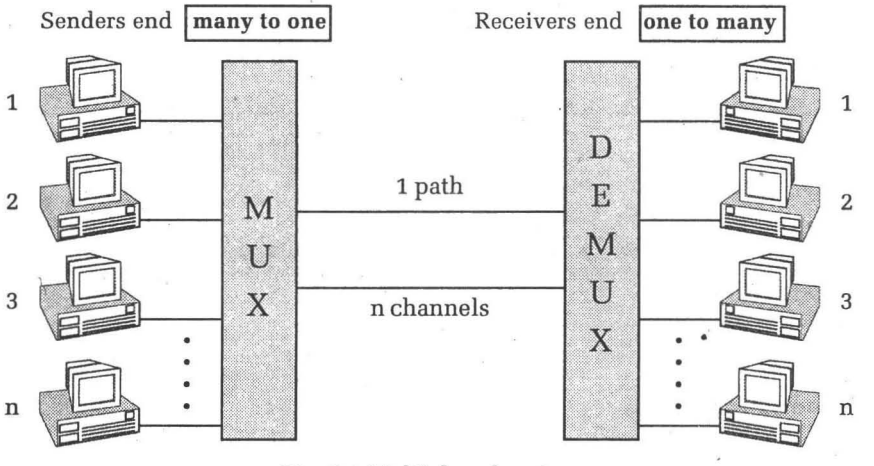


Fig. 8.1 Multiplexed system

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

n devices share the capacity of one link. The n devices on the left direct their transmission streams to a multiplexer (MUX) which combines them to form a single stream. At the right, the single stream is fed into a demultiplexer (DEMUX) which separates the stream back into its component transmission and directs them to the destinated devices. Path refers to the physical link; channel refers to a portion of path that carries a transmission between a given pair of devices. One path can have any number of channels.

The primary benefit of multiplexing is to save money.

8.2 TYPES OF MULTIPLEXING

The two types of multiplexing are as shown in figure 8.2

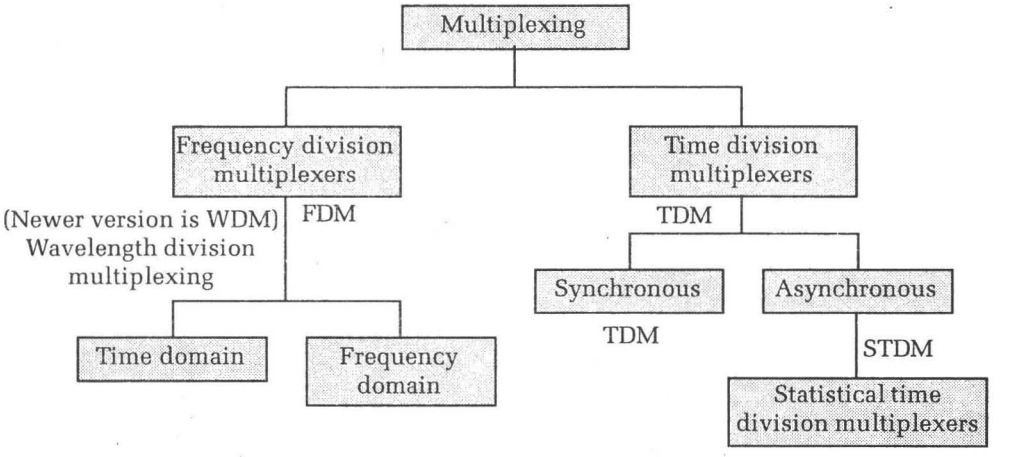


Fig. 8.2 Multiplexing

TDM is preferred to FDM as (i) it provides higher data transmission speeds and (ii) it is simpler. STDM is also common because of its more efficient use of the available circuit capacity. WDM is a newer version of FDM optic cable that may increase network capacity dramatically. TDM is divided into two types. Synchronous called as TDM only and asynchronous called as statistical time division multiplexer or concentrator.

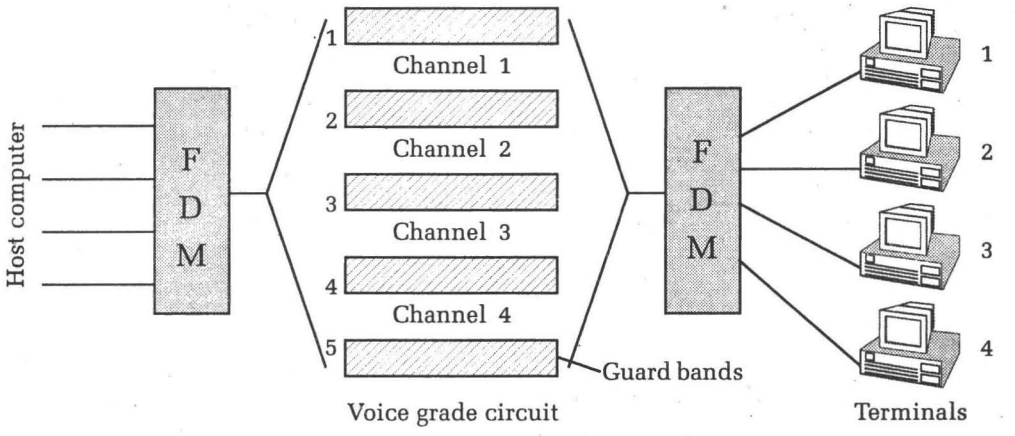
Frequency division multiplexing (FDM)

This sort of multiplexing is dividing the circuit 'horizontally' so that many signals travel a single communication circuit simultaneously. The circuit is divided into a series of separate channels, each transmitted on a different frequency. It is an analog technique which can be applied, if the bandwidth of a link is greater than the combined bandwidth of the signals to be transmitted. Signals generated by each sending device modulate different carrier frequencies and these signals are combined to form a single composite signal that can be transported by the link carrier frequencies are separated by bandwidth to accommodate the modulated signal. The bandwidth ranges are the channels wherein the different signals travel. Channels are separated by guard bands which are strips of unused bandwidth. This present signals from overlapping. Further carrier frequencies should not interfere with the original data frequencies.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Figure below illustrates the use of FDM. Here one circuit is divided into four different parts or sub channels. The signals in a FDM circuit is similar to the way the radio stations must be assigned separate frequencies.



Note : 1, 2, 3, 4, 5 are Guard bands

Fig. 8.3 Frequency division multiplexing (FDM)

The guard bands are the unused portions of the circuit which separates the frequencies from each other. The transmission path is divided into 4 parts, each representing a channel to carry one transmission. It keeps the modulated signals from overlapping and interfering with one another.

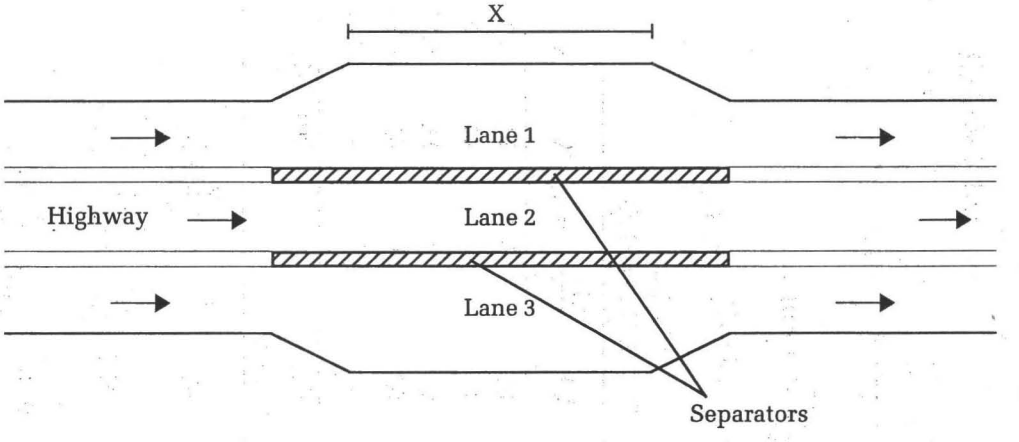


Fig. 8.4

Imagine a 3 lane highway separated into 3 lanes in position X, which are separated by separators for a short distance X. The transmission path discussed above resembles this. Each vehicle can travel in its own lane without interfering with other vehicles of the other lanes. In FDM, actual channel divisions are achieved by frequency rather than by space. An application of FDM is cable television.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

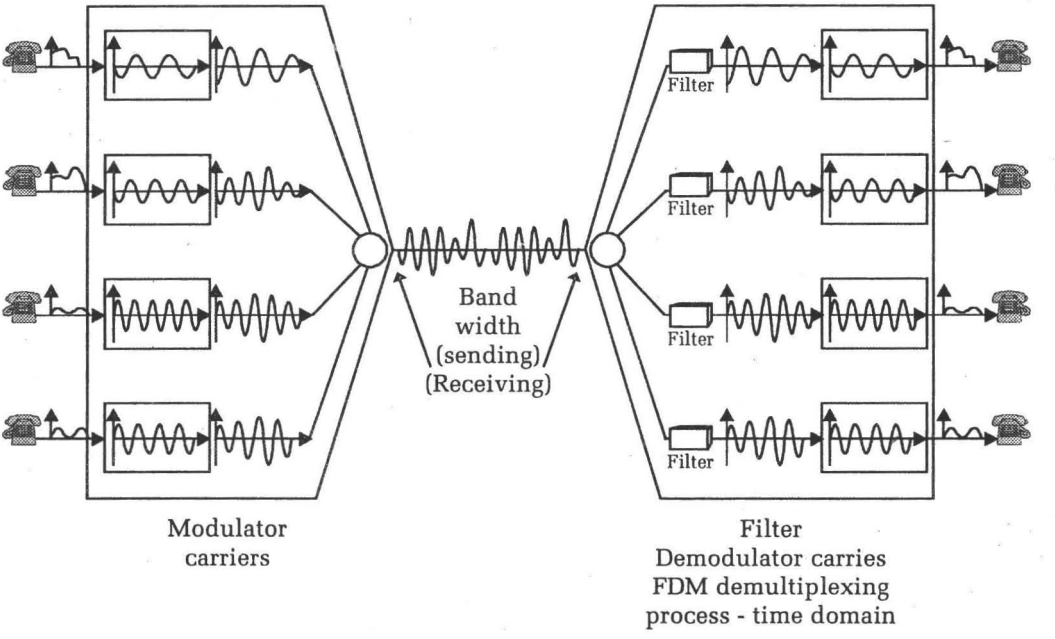


Fig. 8.5 Multiplexing/demultiplexing process – time domain

Horizontal axis in figure 8.6 denotes frequency. Hence it is FDM. All four carrier frequencies exist at the same time within the band width. Here signals are modulated into separate carrier frequencies f_1, f_2, f_3, f_4 using either AM or FM modulation. It is noted that modulating a signal on to another results in a bandwidth of twice the original. The resulting composite signal is more than three times the bandwidth of each of the input signals (Three times the bandwidth to accommodate the necessary channels + extra bandwidth for the required guard bands).

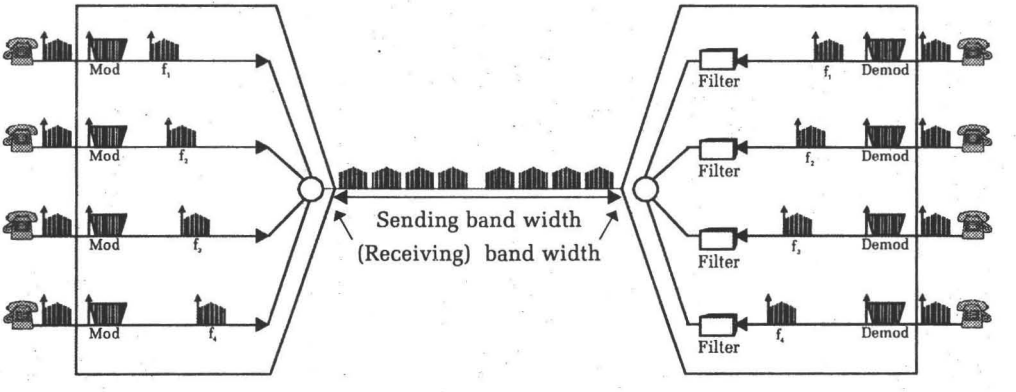


Fig. 8.6 FDM Multiplexing/demultiplexing process - frequency domain

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Demultiplexing

A number of filters are used in the case of demultiplexing to decompose the multiplexed signal into its constituent component signals. The individual signals when passed through a demodulator that separates them from their carriers and passes them to the waiting receivers (Ref. Fig. 8.6)

Time division multiplexing (TDM)

The speciality of this is that it shares a communication circuit among two or more terminals to enable it to have turns, dividing the entire circuit in a vertical way. It is a digital process applied when the data rate capacity of the medium is greater than the data required by the sending and receiving devices.

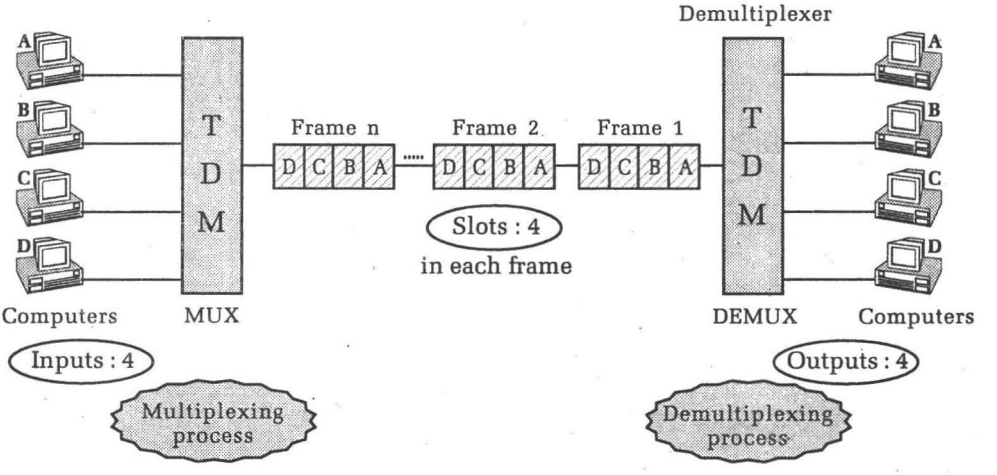


Fig. 8.7 Synchronous TDM

Comparison of FDM with TDM

	FDM	TDM
1. Efficiency	Efficient, Major weakness is empty slots found	More efficient (No empty slots)
2. Guard bands	—	Not required (Guard bands are space on the circuit that otherwise could be used to transmit data)
3. Changing the number of sub channels	—	Easier
4. Originate at one location and terminate at another generally	All subchannels need not end at the same location (different floors in a building different location within a city	Yes
5. Cost to maintain	More	Less
6. Common to share a line	—	32 different low speed terminals

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

7. Preference	Inflexible once you determine how many subchannels are required, it is difficult to add more. An entirely new multiplexer is to be purchased to handle additional subchannels	More preferable because of higher transmission speeds and simplicity
8. Circumstances used	Ideal to use in a multipoint network where each terminal operates a different frequency and each terminal is in a different location.	

In the case of time division multiplexing, though the same link is used as in the FDM, the link is shown sectioned by time instead of frequency. A character is taken from each terminal, transmitted down the circuit, and delivered to the appropriate device at the other (far) end. Time on the circuit is allocated, whether the data is transmitted or not. As a result, some capacity is wasted when certain terminals are idle.

Synchronous TDM

This means here the same time slot is allocated exactly to each device at all times, whether the device has to transmit or not. E.g. Time slot A is assigned to the 1st device A alone and this cannot be used by other devices. During this time slot, a device is enable to send a portion of its data If unable to send or does not have to send, the time slot for that device remains empty.

Time slot are grouped into frames; each frame consists of one complete cycle of time slots, which includes one or more slots pertaining to each sending device plus framing bits. The operation will be as under :

(i) For n input lines ® Frame will have at least n slots. Each slot carries data from a specific input line.

(ii) If all the n input devices shares a link and transmits at the same data rate, then each device has one time slot per frame.

(iii) It is possible to have varying data rates. A transmission having two slots per frame, will traverse twice as quickly as compared to one slot per frame. The time slots dedicated to a given device occupy the same location in each frame and contributes to that devices channel.

The interleaving principle is used here as the same can be compared to a fast rotating switch. To illustrate the principle, alphabets with indexes in the sketch are shown below (for easy understanding).

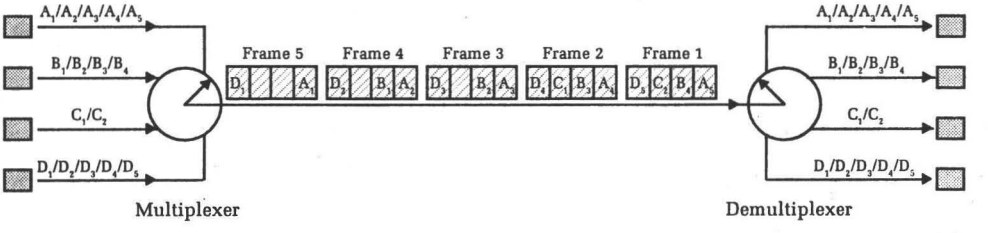


Fig. 8.8 Example of interleaving principle

Copyright © 2009. Global Media. All rights reserved.

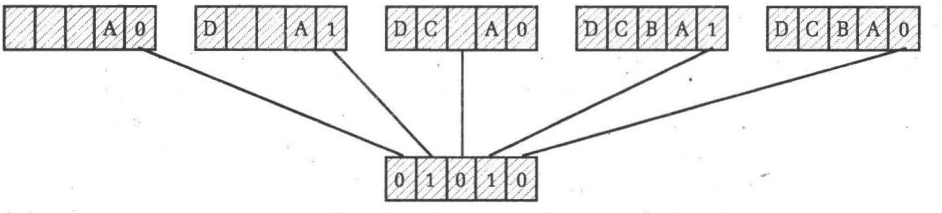
Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

The switch opens in front of each of the devices to enable the device to send a specified amount of bits (data) onto the path. The switch traverse device to device at a constant rate and in a fixed order which is known as interleaving. This may be used for transfer of bits or bytes, or any other data unit. Byte by byte, the multiplexer takes from the device (units will be of the same size). The multiplexer interleaves the different messages to form frames and puts them on the link.

The demultiplexer on the other hand, works vice versa by decomposing each frame into bytes and extracting each character from the frame and passed on to the appropriate receiving device.

The major deficiency (as found in Fig.8.8) in synchronous TDM is empty slots in some of the frames, by assigning each time slot to a specific input line. In the above figure, out of 5 frames of 4 slots each which amounts to a total of 20 slots, 4 slots are empty resulting in 20% loss in the capacity of the link.

Time slot order is same in a synchronous TDM and as such very little overhead information needs are to be included in each frame. Further, the order in which it is received tells the demultiplexer where to direct each time slot and hence no addressing is required. However, various factors still cause timing inconsistences. To prevent this, one or more synchronisation bits are usually added at the beginning of each frame. These bits known as framing bits follow a pattern, frame to frame, that allows the demultiplexer to synchronise with the incoming stream to enable it to separate the time slots accurately. The bits alternate between 0 and 1 in a synchronisation pattern 01010101010.



Synchronisation pattern

Fig. 8.9 Synchronisation Pattern

Data rate calculation for frames are calculated as follows :

$$= n \times 8 \times N = n \text{ synchronisation bits per second.}$$

where n is the number of characters per second per device.

N is the number of devices

fox example if $n = 250$ characters per second

$N = 5$ devices

Data rate for frames $= 250 \times 8 \times 5 + 250$

$= 10000 + 250 = 10,250$ bps

10,000 bits of data + 250 overheads (synchronisation bits) = 10,250 bps.

Each of the devices can also have different data rates. E.g. A uses two time slots, B can have only one time slot; the number of slots in a frame and the input slots to which they belong remains fixed through a given system; devices of data rates may control different numbers of those slots. Time slot length is fixed. Hence

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

the different data rates must be integer multiplex of each other. E.g. A device four times faster can be taken where as a device four and half times faster cannot be taken since half a time slot cannot be put into the frame. To accommodate four time faster in one of the devices, this device is given four slots as against one for each of the other devices.

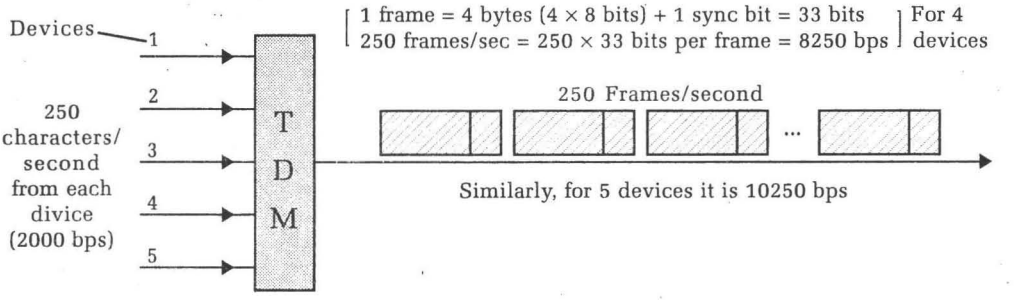


Fig. 8.10 Data rate for frames

Bit stuffing technique is used when the speeds are not integer multiples of each other and they are used to behave as if they were with the addition of an extra bit (0) to achieve data transparency. In synchronous TDM, the addition of extra bits is to equalise different data rates. The multiplexer adds extra bits to a devices source stream to force the speed relations between the various devices to make it integral multiples of each other. A bit rate of one device with 3.75 times that of the other devices can be made 4 times by adding additional bits. The demultiplexer discards the extra bits.

Asynchronous TDM or Statistical time division multiplexing (STDM)

The purpose of designing this is to avoid waste (empty slots). Asynchronous means flexible or not fixed. If the slot is empty, path is wasted. E.g. If ten identical computers output are multiplexed on to a single line, the speed of that line should be ten times the speed of each input line. In this, suppose only 5 computers, the capacity of the line is wasted 50%. To avoid this, asynchronous TDM has been designed. STDM is the exception to the rule that the capacity of the multiplexed circuit must equal the sum of the circuits it combines. It allows more terminal or computers to be connected to a circuit than FDM or TDM.

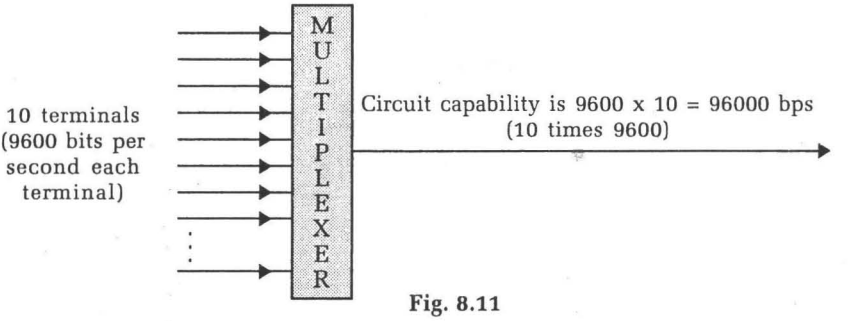


Fig. 8.11

In the case of STDM, not all terminals will be transmitting continuously at their maximum transmission speed. Users typically pause to read their screens or spend time typing at lower speeds. There is no need to provide 9600 bps on

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

the circuit. Alternatively, only 5 terminals are transmitting at the same time with half of 9600 bps, that is 48000 bps might be enough, depending on how quickly the specific terminals or microcomputers and their users/generate or request data.

STDM is known as statistical since selecting the transmission speed for the multiplexed circuit is based on a statistical analysis of the usage requirements of the circuits to be multiplexed.

The benefits are :

(i) provides more efficient use of the circuit (can use a less expensive circuit than FDM or TDM).

(ii) saves money.

STDM poses two problems

I. Since data from different devices are intermixed on the multiplexed circuit, all data are to be identified by an address to make sure that to which device it belongs. Hence a terminal address is added to the character and is inserted into the data stream.

For example : STDM multiplexer individual characters from 12 terminals. The terminal address is also added to the character and is inserted into the data stream. Hence in additional to eight bits for a character, another 5 bits are to be added to each character for the address space. Given the same link, asychronous TDM can support more devices than synchronous TDM.

The working of STDM is given below.

Note : The numbers for the alphabets are given to identify them easily in the example given below.

1. *Three input lines sending data :*

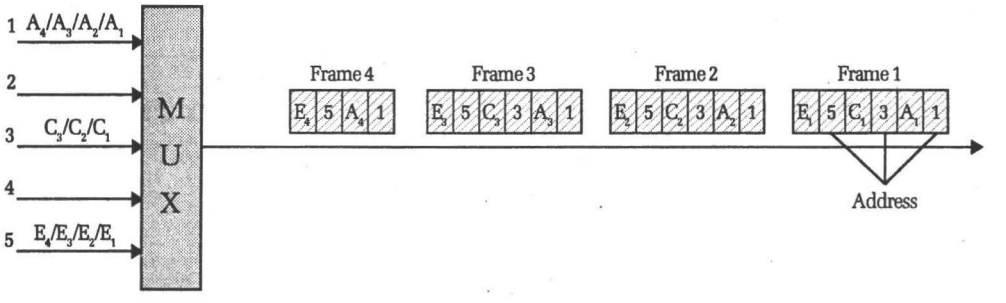


Fig. 8.12 Three input lines

The multiplexer picks up the A_1 from device 1 and puts it in address 1, scans downs the line to the 3rd line and picks up C_1 and puts it in address 3 and then again scan down the line to the 5th line, puts E_1 against the address 5. This forms the first frame. The second frame and third frame are worked out in a similar way. Finally A_4 and E_4 are left out. These are put in Frame 4 which is incomplete. Frames 1, 2, and 3 are full. With the asynchronous system frame 4 is transmitted partially empty. During the rest of the transmission line, the entire capacity of the link is active.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

2. *Four input lines sending data :*

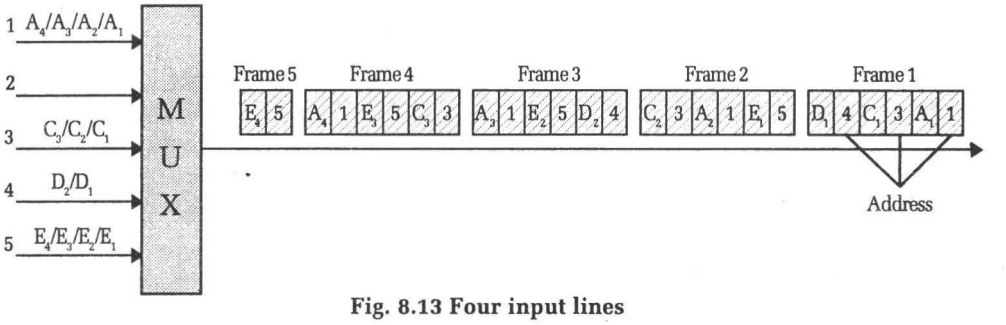


Fig. 8.13 Four input lines

3. *Five input lines sending data :*

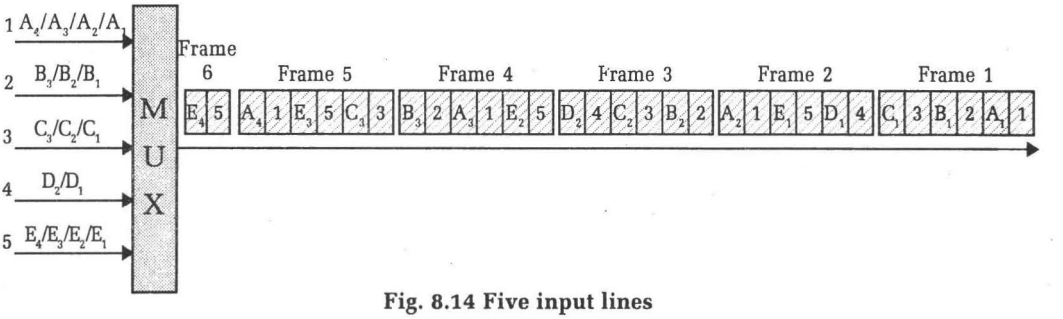


Fig. 8.14 Five input lines

Working of the multiplexer in cases (2) and (3) will be the same as shown in case (1). In the second case, frames 1, 2, 3, and 4 are filled fully and the fifth frame is partially empty.

In case (3), the frames are filled full except frame 6. All five input lines are active. Device 1 controls the first slot in the first frame, the third slot in the 2nd frame and no slots at all in the third frame, 2nd slot in the fourth frame and 3rd slot in frame 5.

II. The second problem is that STDM cause time delays. If every device in the input lines start transmitting and all devices receiving at the same time, the multiplexed circuit cannot transmit all the data it receives since it does not have sufficient capacity. Hence it is necessary to have an internal memory to store the incoming data which cannot be transmitted immediately. In case of heavy traffic, it may need 1 to 30 seconds delay.

Adding address bits to every time slot increases the overhead and thereby limits potential efficiency. Hence to limit their impact, addresses consists of a small number of bits and can be made even shorter by appending a full address only to the first portion of a transmission with abbreviated versions to identify the next portions. The need for addressing makes STDM inefficient for bit or byte interleaving. If one bit interleaving with each bit carrying an address or one bit of data plus say three bits of addresses it becomes four bits to transport one bit of data (only a quarter of the capacity is used to transport data, rest is overload).

If various lengths of time slots are allowed, STDM can accommodate traffic of varying data rates.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Multiplexing entire message from terminals

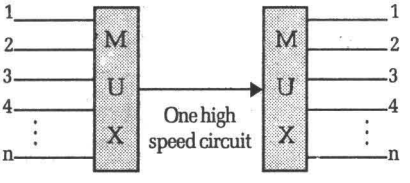
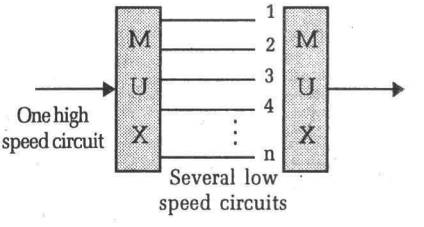
This type of multiplexer allows to interleave entire messages rather than characters. It picks up the entire message (all of its characters) from device 1 and puts it in a frame, after which it scans the next terminal that has an entire message to send. In this way, it continues the process. This reduces the amount of overhead addresses transferred but can increase delays.

Fast packet multiplexing (FPM)

It is the latest form of STDM that combines voice, video and data transmissions. This supports high data transmission rates (1 to 2 Mbps). FPM decides which transmissions are more important such as voice transmissions (voice transmissions exhibit talk spurts). It sends the more important voice transmission first and fast being vital (not tolerant of delays). Delays can cause gaps in words that are very distracting to the people. This removes repetitive characters from data transmissions and gaps at the time when no one is speaking from digitized voice transmissions. This allows both the data and voice to be sent with less capacity on the multiplexed circuit. The remaining capacity will be used for more data or voice transmissions.

Inverse multiplexing

Multiplexing was developed to combine several low speed circuits for transmission across one high speed circuit. Reverse is also possible to take high speed circuits and break then into portions that can be sent across several low speed circuits simultaneously. Multiplexing is the opposite of inverse multiplexing.

Multiplexing	Inverse Multiplexing
Data transmitted through several low speed lines  Multiplexing was developed to combine several low speed circuits transmission across one high speed circuit. Reverse is also possible to take high speed circuits and break them into portions that can be sent across several low speed circuits simultaneously which is called as inverse multiplexing. Multiplexing is the reverse of inverse multiplexing.	Data transmitted through high speed circuit  Inverse multiplexing is used because of different data rates are required for data voice and video. Voice needs a 64 Kbps link Data needs a 128 Kbps link Video needs a 1.544 Mbps link Hence the organisation has to go in for a common carrier (lease a 1-544 Mbps channel telephone company and use the full capacity only sometimes) or it can lease several separate channels of lower data rates. Voice transmission can be sent on any of the channels whereas the data and video signals are to be broken up and sent over two or more lines. The most common use is to provide T-I circuits for wide area networks which provide data transmission of 1.544 Mbps (1,544,000 bits per second) by combining 24 lower speed circuits (64000 bps)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

8.3 APPLICATION OF MULTIPLEXING

Telephone industry uses extensively multiplexing as an essential tool. We shall analyse the various carriers as a single entity called the telephone network and the line known as a service line connecting a subscriber to that network. Many common carriers offer local and long distance services to subscribers.

Earlier technology in the telephone network was providing analog services to the subscribers by the telephone companies using analog networks. The technology later on changed to the introduction of digital services and networks. It is presumed that soon the network would be digital. At present both types of services are available along with FDM and TDM.

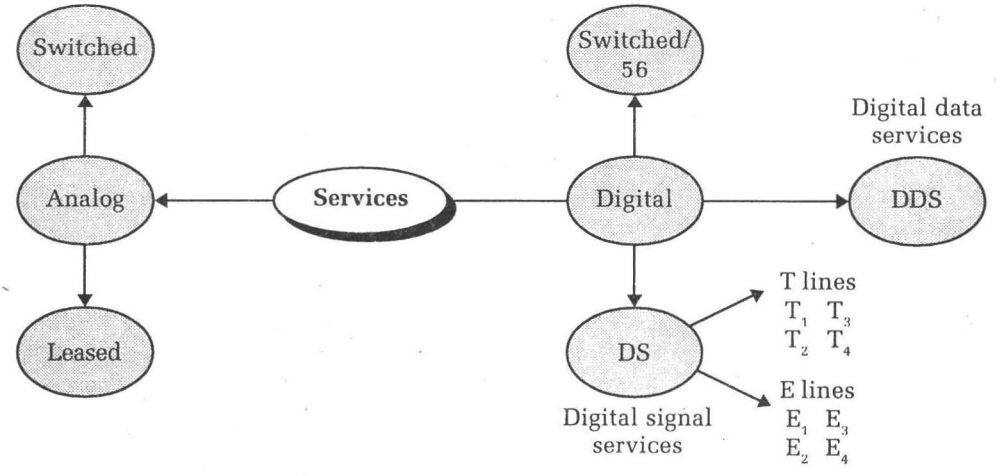


Fig. 8.15 Categories of telephone services

Analog services

In this, we have two types of services : switched and leased services.

Analog switched service

It is a most common dial-up service encountered quite often when using a home telephone. It si a common public telephone service that connects two of the customers temporarily through the use of switches and switching stations. Dialing is required. It uses two-wire (sometimes four wires) twisted pair cable to connect the suers handset to the network via an exchange. This connection is called the local loop and the network to which it is joined is referred to as a public switched network (PSTN). The signal is analog, the band width is 0 to 4000 Hz. When the caller dials a number, the call is conveyed to a switch or series of switches at the exchange. When once the appropriate switch is activated to link the caller's line to the person being called, the switch connect, automatically the two lines.

Analog leased service

Analog leased service is a public telephone service that provides a dedicated connection between two customers and no dialing is required. This service offers the customers an opportunity to lease a line known as dedicated line that is

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

permanently connected to another Though in reality the connection passes through many switches in the telephone network, subscribers feel it as a single line because the switch is always closed.

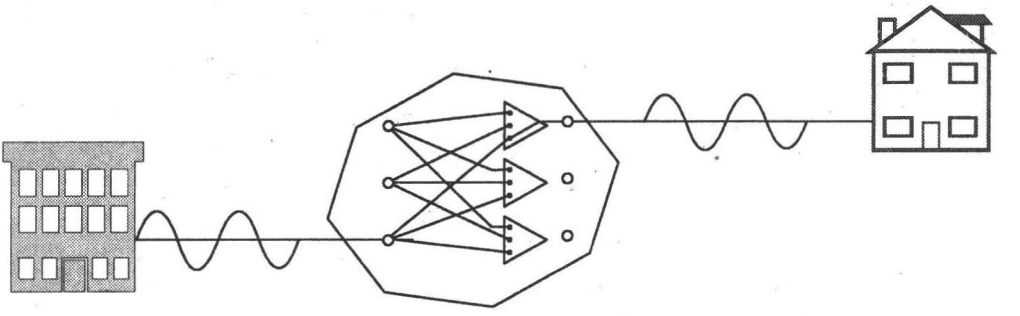


Fig. 8.16 Analog switched service

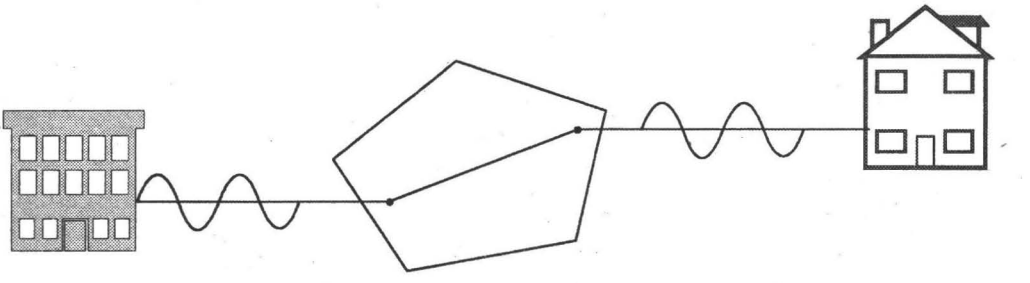


Fig. 8.17 Analog leased service

Another service offered by telephone carriers is called 'conditioning'. It is a means of improving the quality of a line by :

(a) lessening attenuation

(b) signal distortion or delay distortion

Conditioned lines will also be analog but the quality permits them usable even for digital communication if they are connected to modems.

Digital services

In the recent days telephone companies are offering digital services to subscribers. Digital services have several advantages over analog.

(i) less sensitive to noise and other forms of interference (telephone acts like an antenna and will pick up noise)

(ii) signal is digital but the interference is still analog (signal can be easily distinguished and separated)

(iii) less cost (uses less expensive electronics)

Switched / 56

It is digital version of an analog switched line and allows data rates upto 56 Kbps. Both parties must subscribe. Here a caller with normal telephone service cannot be connected to a telephone or computer with a switched/56 even if using a modem. Subscribers do not need modems to transmit digital data as switched/

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

56 service is digital. However another service DSU is required known as digital service unit. The digital rate of 56 kbps created by subscribers device is changed by the DSU and is included in the dialing process along with dial pad. It is understood that DSU is costlier than modem. A subscriber would still buy switched/56 service along with DSU because of advantages like speed, better quality and susceptibility to noise etc. than an equivalent analog line.

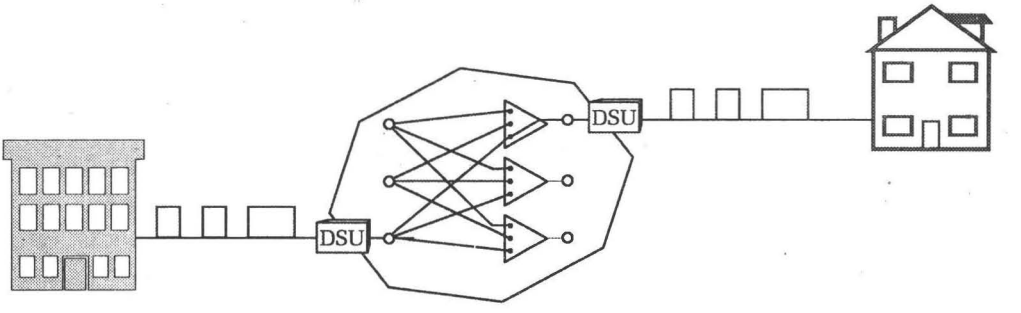


Fig. 8.18 Switched / 56 service

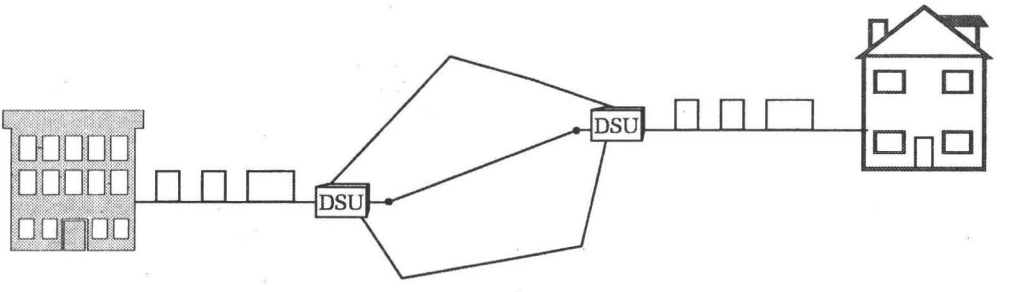


Fig. 8.19 DDS Service

DDS (Digital data service)

It is the digital version of an analog line. It is a service featuring a digital leased line using a data rate of upto 56 kbps (same as switched/56). The five different rates available are 2.4, 4.8, 9.6, 19.2 or 56 Kbps. The speed is to be chosen by the subscriber, after which the telephone company sets the same and must be observed.

Like switched/56, DDS also needs the use of a DSU, but it is cheaper here comparatively and does not need a dial pad.

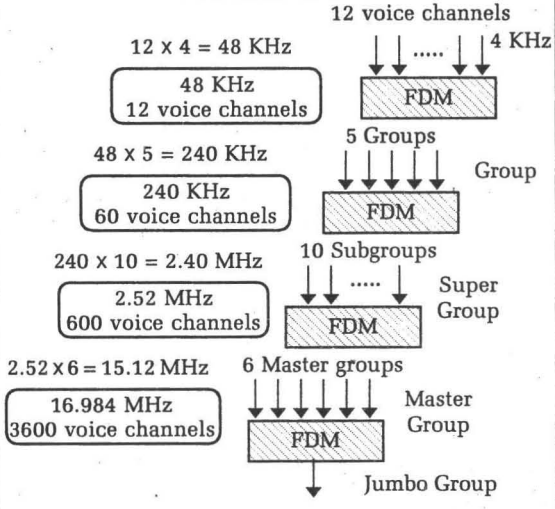
The analog hierarchy and the digital hierarchy

Telephone companies multiplexed signals from lower band widths on to a higher band width lines to maximise the efficiency of the infrastructure switched or leased lines can be combined into fewer or bigger channels. FDM is used in the case of analog channels.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Analog Hierarchy (used by AT&T)



Level 1 : (4 KHz × 12 = 48 KHz)

- 12 voice channels multiplexed → higher bandwidth line

Level 2 : (Group) (48 KHz × 5 = 240 KHz)

Five groups multiplexed → A composite signal called super group (supports 60 voice channels)

Level 3 : (Super groups) (240 KHz × 10 = 2.4 MHz)

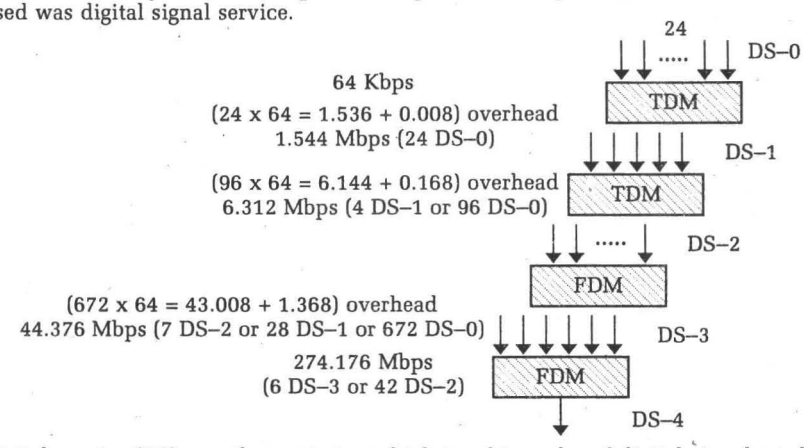
Ten super groups multiplexed → Master group. Need for guard bands increases the band width to 2.52 MHz

Level 4 : (Master groups) (6 × 2.52 MHz = 15.12 MHz)

Six master groups can be combined into a jumbo group. Need for guard bands increases the band width to 16.984 MHz

Digital Hierarchy

Similar to analog services, telephone companies developed digital services. A hierarchy used was digital signal service.



Digital service (DS) was the next step which is a hierarchy of digital signals and the data rates supported at each level are as shown above.

Level 1 : DS-0 service resembles DDS. It is a single digital channel of 64 kbps.

Level 2 : DS–1 is 1.544 Mbps (24 times 64 Kbps + 8 Kbps overhead). It can be used either as a single service of 1.544 Mbps transmission or to multiplex 24 DS–0 (of 64 Kbps each) or any other combination within 1.544 Mbps. Line T_1 is used.

Level 3 : DS–2 is 6.312 Mbps (96 times 64 Kbps + 168 Kbps overhead) This can be used for a single service of 6.312 Mbps or to multiplex four DS–1 or 96 DS–0 channels or any other combination within 6.312 Mbps. Line T_2 is used.

Level 4 : DS–3 is 44.376 Mbps (672 times 64 Kbps + 1.368 Mbps overhead) This can be used either as a single service of 44.376 Mbps or to multiplex seven DS–2 channels, 28 DS–1 channels, 672 DS–0 channels or any other combination within 44.376 Mbps. Line T_3 is used.

Level 5 : DS–4 is 274.16 Mbps (4032 times 64 Kbps + 16.128 Mbps overhead) This can be used either as a single service of 274.16 Mbps or to multiplex six DS–3 channels, 42 DS–2 channels, 168 DS–1 channels, 4032 DS–0 channels or a combination of any of the above within 274.16 Mbps. Line T_4 is used.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

T and E-lines

Telephone companies use T lines from T_1, T_2, T_3, T_4 to take up the data rates of DS–1 to DS–4 respectively. These lines have 1.544, 6.312, 44.376, 274.176 Mbps data rates as shown above and voice channels 24, 96, 672, 4032 respectively. DS–0 is not offered as a service, but it forms the basis of others and used only for reference. This can be substituted for DDS.

T carrier circuits, which are the special forms of digital services are leased digital circuits with a wide range of transmission capacities (North American telephone industry standard). It is a hierarchy of digital transmission and multiplexing standards, ranging form T_1 to T_4.

T_1 circuit operates at a synchronous data rate of 1.544 Mbps. It can be transmitted over this circuit at speeds ranging from 56 Kbps to 1.544 Mbps. Digitised voice using pulse code modulation (PCM) uses 64 Kbps. By digitizing voice signals and multiplexing then with TDM, T_1 circuits allow for 24 simultaneous voice channels which transport data or voice messages according to a signalling format called DS–0, known as North American Digital Hierarchy.

Adaptive differential pulse code modulation (ADPCM)

Digitised voice usually is transmitted over T carriers and new methods of digitising voice are frequently found every year. One of the newest methods is ADPCM makes the T_1 carrier twice efficient (can handle 48 voice channels as against 24 of PCM). Refer table shown below.

Digital signal	T-carrier circuit (Line)	Number of voice channels PCM	ADPCM	Speed (bits/second)
DS–0*		1		64000
DS–1	T–1	24	48	1,544,000
DS–1C	T–1C	48	96	3,152,000
DS–2	T–2	96	192	6,312,000
DS–3	T–3	672	1344	44,376,000
DS–4	T–4	4032	8064	2,74,176,000

* DS–0 is the standard that divides frames into channels.

AT&T makes extensive use of PCM internally and transmits most of its information in pulse code modulated digital format over T carriers. It may be noted that a T_1 carrier with a capacity equivalent to 24 voice grade lease lines costs about the same per month as 12 to 14 individual voice grade leased lines separately taken.

Fractional T–1 (FT–1)

This offers portions of a 1.544 Mbps T–1 circuit for a fraction of its full cost.

T–lines for analog transmission

T–lines meant for digital data, voice, or audio signals transmission can also be used for analog transmission (telephone connections) if the analog signals are sampled and TDM applied. T_1 line for analog transmission helped for new generation of services for telephone companies. Now organisations can combine 24 lines into one T_1 line and run the same to the exchange.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

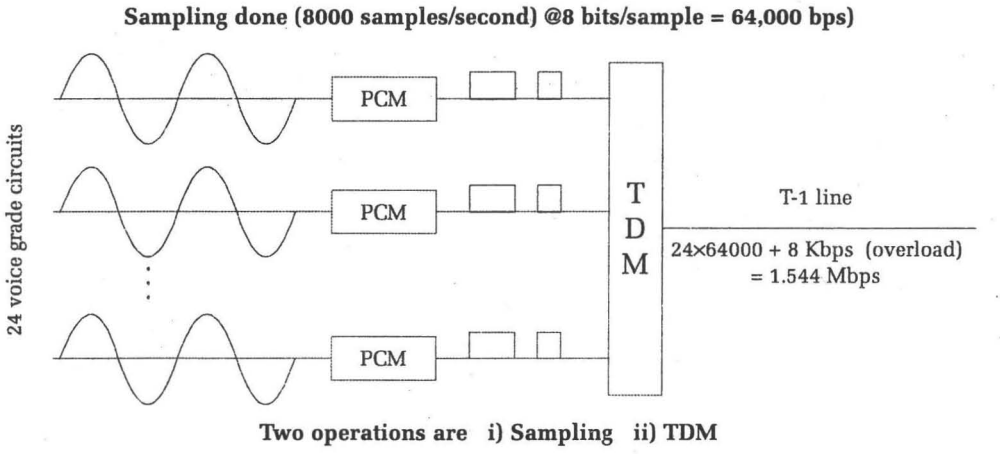


Fig. 8.20 DDS Service

T_1 Frame

Consists of 24 slots + 1 extra bit
(of 8 bits each) (for synchronisation)
24 x 8 + 1 = 193

For 8000 frames total in T_1 line

Data rate is 193 x 8000 = 1.544 Mbps

∴ capacity of the line = 1.544 Mbps

Note :

(i) Each slot contains 1 signal segment for each channel.

(ii) 24 segments are interleaved in one frame.

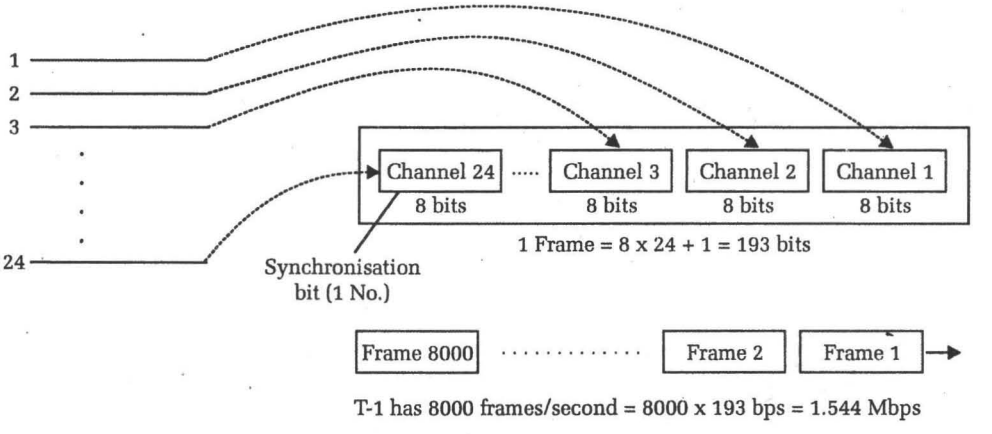


Fig. 8.21 T–1 Frame

The figure indicate above is self explanatory for a T_1 frame. If a small company needs only a small capacity of T_1 line, it can share by joining with other companies, a full T_1 line, in which case, the transmission is directed through a device known as data service unit/channel service unit (DSU or CSU).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

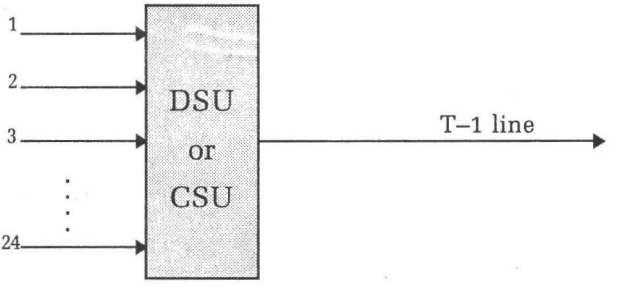


Fig. 8.22 Fractional T–1 line

E–lines

Europeans have their own version of T–lines called as E–lines. Though both the T–lines and E–lines are conceptually identical, their capacities differ.

Line	Rate (Mbps)	Voice channels	Line	Rate (Mbps)	Voice channels
T–1	1.544	24	E–1	2.048	30
T–2	6.312	96	E–2	8.448	120
T–3	44.736	672	E–3	34.368	480
T–4	274.176	4032	E–4	139.264	1920

Other multiplexing services

Hitherto, we discussed multiplexing over cable. Multiplexing is also important in the use of terrestrial and satellite micro wave transmission. Telephone service provides use powerful services like :

(i) SONET (Synchronous optical network)

(ii) ISDN (Integrated services digital network)

(iii) SMDS (Switched multimegabit data services)

(iv) ATM

POINTS TO REMEMBER

- Multiplexing is the process of combining signals from multiple sources for transmission across a single data link. It is usually done in multiples of 4, 8, 16 and 32 simultaneous transmissions over a single communication circuit.
- Two types of multiplexing are : Frequency Division Multiplexing (FDM), Time Division Multiplexing (TDM). Under FDM, we have two divisions, time domain and frequency domain. Under TDM, we have Synchronous TDM, Asynchronous TDM (known as statistical time division multiplexers – STDM).
- Frequency division multiplexing is dividing the circuit horizontally so that many signals travel a single communication circuit simultaneously. The guard bands are the unused portions of the circuit which separate the frequencies from each other to eliminate overlapping and interfering. In FDM, each signal modulates a different carrier frequency. The modulated carriers are then combined to form a new signal which is sent across the link.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

- Multiplexers modulate and combine signal whereas the demultiplexers do the reverse (decomposing and demodulating)
- In time division multiplexing, digital signals from n devices are interleaved with one another to form frame of data (bits, bytes, or any other data unit)
- In synchronous TDM, time slots, are grouped into frames. Each frame consists of one complete cycle of time slots, which includes one or more slots pertaining to each sending device plus framing bits. Further, the order in which each device sends its data to the frame is unvarying. If there is no data in the device to send, its time slot would be empty. A bit may be added at the beginning of each frame for synchronisation.
- In synchronous TDM, same time slot is allocated exactly to each device at all times, whether the device has to transmit or not. Time slot order is same and as such very little overhead information needs are to be included in each frame. The interleaving principle is adopted in the case of synchronous TDM.
- In a bit oriented protocol, addition of an extra bit (0) is to achieve data transparency. In synchronous TDM, the same means to equalize different data rates. This is known as bit stuffing.
- In asynchronous TDM, the purpose is to avoid waste. Asynchronous means flexible or not fixed. If the slot is empty, path is wasted. It is also called as statistical time division multiplexing (STDM). Asynchronous TDM adds device addresses to each time slot. STDM is known as statistical since selecting the transmission speed for the multiplexed circuit is based on a statistical analysis of the usage requirements of the circuits to be multiplexed. The benefits are (i) to provide more efficient use of the circuit (ii) saves money.
- STDM poses problems regarding addressing and time delays.
- Telephone services could be analog or digital. Analog switched service needs dialing, switching and a temporary dedicated link.
- Fast packet multiplexing (FPM) is the latest for of STDM that combines voice, video and data transmissions. This supports high data transmission rates (1 to 2 Mbps)
- In Analog services we have two types : switched and leased services. Analog switched service is a most common dial-up service encountered quite often when using a home telephone. It is a common public telephone service that connects two of the customers temporarily through the use of switches and switching stations. Dialing is required.
- Analog leased service is a permanent dedicated link between two customers. No dialing is necessary.
- Inverse multiplexing is used because of different data rates are required for data, voice and video. Voice needs a 64Kbps link; Data need a 128 Kbps link, Video needs a 1.544 Mbps link.
- Telephone carriers offer one more of service called 'conditioning' It is a means of improving the quality of a line by lessening attenuation and signal distortion or delay distortion.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

- Switched/56 service is a digital version of an analog switched line and allows data rates up to 56 Kbps. It needs a digital service unit (DSU) to ensure this data rate. Digital data service (DSU) is the digital equivalent for analog leased lined. DDS also needs a DSU.
- Digital data service (DDS) is the digital version of an analog line. It is a service featuring a digital leased line using a data rate of upto 56Kbps (same as switched/56).
- Telephone companies multiplexed signals from lower band widths on to a higher bandwidth lines to maximise the efficiency of the infrastructure. Switched or leased lines can be combined into a fewer or bigger channels.
- Digital system (DS) is a hierarchy of TDM signals. T–lines have 4 lines (T_1 to T_4) are the implementation of DS services. A T–1 line consists of 24 voice channels.
- Fractional T–1 known as FT_1 allows subscribers to share one line by multiplexing their signals. This offers portion of a 1.544 Mbps T–circuit for a fraction of its full cost.
- T–lines and E–lines are used in North America and Europe respectively. The European Standard defines a variation called E lines.

QUESTIONS

1. What do you mean by multiplexing? How does it work? Illustrate with a sketch.
2. What are the different types of multiplexing?
3. Of the different types of multiplexing, What distinguishes
   (i) Frequency division multiplexing (FDM)?
   (ii) Time division multiplexing (TDM)?
   (iii) Statistical time division multiplexing (STDM)?
   (iv) Wave length division multiplexing (WDM)?
4. Explain the function of FDM.
5. What are advantages of using guard bands?
6. Explain the FDM multiplexing process-time domain with a sketch.
7. Explain the FDM multiplexing process - frequency domain with a sketch.
8. Explain synchronous TDM and its working with a sketch.
9. What are the functions of TDM?
10. Compare and contrast TDM with FDM.
11. What are the functions of multiplexer and demultiplexer?
12. What is inverse multiplexing? Explain.
13. Explain asynchronous TDM (STDM) and its working with a sketch.
14. What is the reason of calling asynchronous TDM as statistical?
15. Explain the reasons why the number of slots for asynchronous TDM is less than the number of slots for synchronous TDM?
16. Compare and contrast modem with DSU.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

17. How does slot size affect synchronous TDM and asynchronous TDM?
18. In asynchronous TDM, how is the number of slots per frame is worked out?
19. What do you mean by conditioned lines?
20. Compare and contrast the analog hierarchy and the digital hierarchy.
21. What do you mean by fast packet multiplexing?
22. Compare and contrast analog switched service and analog leased service.
23. What are digital services?
24. What do you mean by switched/56? What are its components?
25. What do you mean by Adaptive differential pulse code modulation?
26. What is Fractional T–1? Explain T_1–lines used for analog transmission.
27. Compare and contrast T–lines with E–lines.
28. What are the other multiplexing services used in the use of terrestrial and microwave transmission?

FILL IN THE BLANKS

1. Multiplexing usually is done in multiples of _____.
2. In multiplexed system, number of devices share the capacity of one _____.
3. Multiplexer is denoted by _____ and demultiplexer is denoted by _____.
4. TDM is preferred to FDM because of _____ _____ _____ _____ and _____.
5. _____ is a sort of multiplexing dividing the entire circuit horizontally.
6. _____ is a sort of multiplexing dividing the entire circuit vertically.
7. _____ _____ multiplexing technique transmit, analog signals.
8. _____ _____ multiplexing technique transmits digital signals.
9. In FDM _____ _____ keep the modulated signals from overlapping and interfering with one another.
10. _____ is required in demultiplexing.
11. Multiplexing involves _____ path and _____ channels.
12. In the case of asynchronous TDM for n input devices, each frame contains m slots, were m is usually _____ _____ η.
13. In the case of synchronous TDM, for n signal sources, each frame contains ____ slots.
14. In the case of synchronous TDM demultiplexing process _____ _____ are added to the beginning of each frame.
15. _____ type of multiplexing is involved with multiple paths.
16. In asynchrons TDM, the transmission rate of the multiplexed path is usually _____ _____ the sum of the transmission rates of the signal sources.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

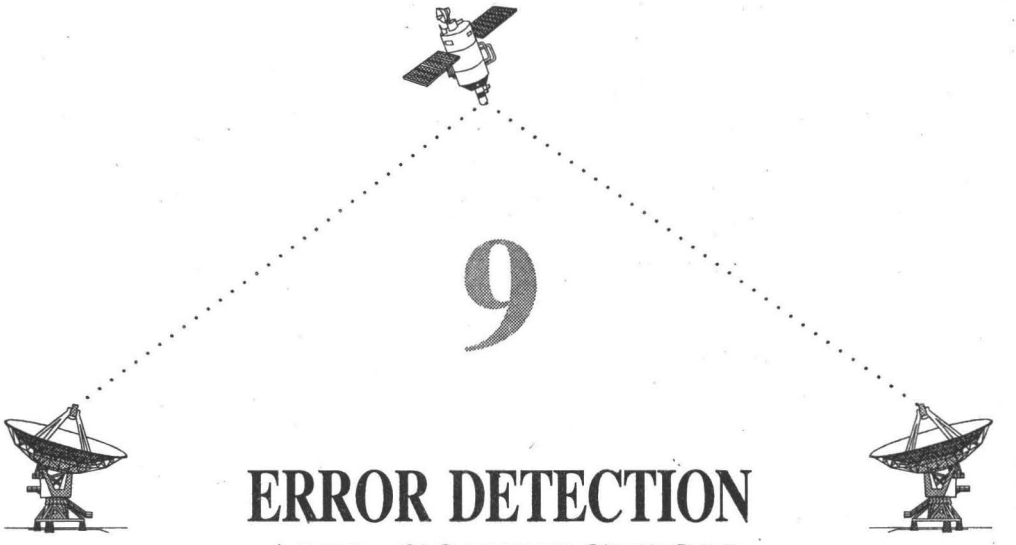
17. The purpose of designing asynchrons TDM is to avoid _____.
18. Asynchronous means _____ or ____ _____.
19. STDM poses problems about _____ and _____.
20. _____ _____ _____ type of telephone service is least expensive.
21. Guard bands increase the band width for _____.
22. In a T–1 line _____ interleaving occurs.
23. _____ _____ is used because of different data rates are required for data, voice and video.
24. Voice needs a _____ Kbps link; Data needs a _____ Kbps link; Video needs a _____ Mbps link.
25. Fast packet multiplexing supports high data transmission rates __ to __ Mbps.
26. T_1 circuit operates at a synchronous data rate of _____ Mbps.
27. Leased service means that connections between subscribers are with _____ _____.
28. To decrease attenuation and distortion of a signal a line should be _____.
29. In switched / 56 service, 56 means _____ _____.
30. DSU is needed in _____ service.
31. In switched service, the connection between subscribers must involve _____.

Answers

1. 4, 7, 16 and 32
2. link
3. MUX ;DEMUX
4. Higher data transmission speeds ; simplicity
5. FDM
6. TDM
7. Frequency division
8. Time division
9. guard bands
10. Filter
11. one ; multiple
12. less than
13. η
14. framing bits
15. Inverse
16. greater than
17. waste
18. flexible ; not fixed
19. addressing ; time delays
20. Analog switched line
21. FDM
22. byte
23. Inverse multiplexing
24. 64 ; 128 ; 1.544
25. 1 ; 2
26. 1.544
27. dedicated lines
28. conditioned
29. data rate
30. DDS
31. dialing

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.



9

ERROR DETECTION AND CORRECTION

9.1 INTRODUCTION

In order to protect a network from errors, two types of basic errors for implementation should be understood.

(i) Human errors

(ii) Network errors

Human errors are such as a mistake in typing a number, usually controlled through the application program.

Network errors are the errors which occur during transmission. Networks are supposed to transfer data from one device to another accurately. The data transmitted from source to destination sometimes get corrupted on the path. It is more likely that some part of a message will be altered in transit than that the entire contents will arrive intact e.g.. line noise etc. may alter or wipe out certain bits of a given data.

There should be a mechanism for detecting and correcting errors. For reliable communication, errors must be detected and corrected. Network errors are a fact of life in today's data communication network. No network can eliminate all errors. But most errors can be prevented or detected and corrected by properly designing. Interexchange carriers that lease data transmission circuits provide statistical measures indicating typical error rates and the pattern of errors that can be expected on the circuits.

Two categories of data errors in network are :

(i) corrupted data

(ii) lost data

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

The factors required to study when selecting an error control system are :

(i) Maximum error rate that can be tolerated.

(ii) Cost of increased accuracy compared with the cost of correcting errors.

(iii) Future cost of correcting errors (in the received data/information).

Error detection and correction are implemented at the data link layer or the transport layer to the OSI model.

9.2 TYPES OF ERRORS

It is a known fact that the flow of electromagnetic signal from point to point would result in unpredictable interference from heat, magnetism and other forms of electricity, which would change the shape or timing of the signal. Changes which occur may change over the meaning of the data by changing 0 to 1 or 1 to 0, in the signal carrying encoded binary data. Such changes might happen singly or in clumps. Even a slightest burst of impulse noise (say for 0.01 second) on a transmission with a data rate of 1200 bps might change 12 bits of information.

Errors normally appear in bursts. In a burst error, more than one data bit is changed by the error causing condition. This means errors are not uniformly distributed in time, inspite of common carriers usually list their error rates as the number of bits in error divided by the number of bits transmitted (without referring to their nonuniform distribution) eg. The error rate is given as 1 in 500, 000 means that there is 1 bit in error for every 500, 000 bits transmitted.

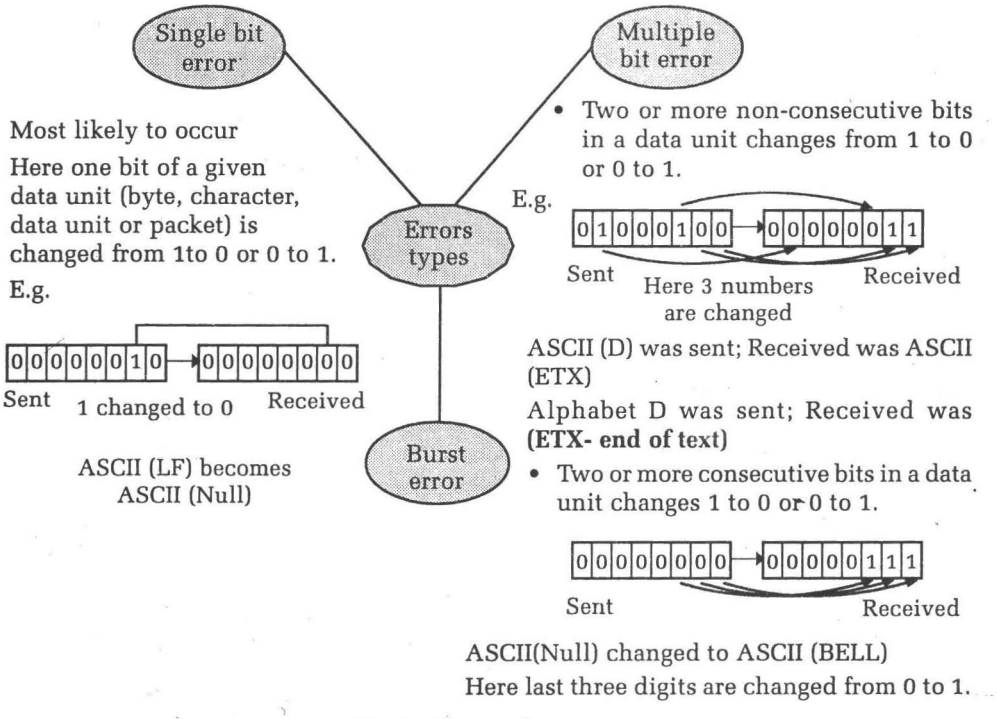


Fig. 9.1 Types of errors

The fact that errors tend to be clustered in bursts rather than evenly dispersed may be considered good and bad.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

If the errors were not clustered, an error rate of 1 bit in 500,000 would make it rare for two erroneous bits to occur in the same character. Hence simple character checking schemes would be effective at detecting errors.

E.g. If errors are #ore or less evenly distr#buted, it is easy to det#rmine the meaning, even the error rate is found high as it is in thi# s#ntence (1 chara#ter in 20)

Burst errors are the rule rather than the exception. Hundred or more bits at a time affected this makes it difficult to find the meaning. More reliance must be placed on knowledge of the message ####### (word is context) or on special logical or numerical error detection and correction methods.

Dial up lines are more prone to errors than private dedicated lines for the reason they have less stable transmission parameters.

The error rate in transmissions sent over the dial-up network (telephone company circuits) varies from one circuit to another. Higher transmission rate are more error prone.

The causes for errors are given in figure 9.2.

These are twelve in numbers and the causes are given in brief.

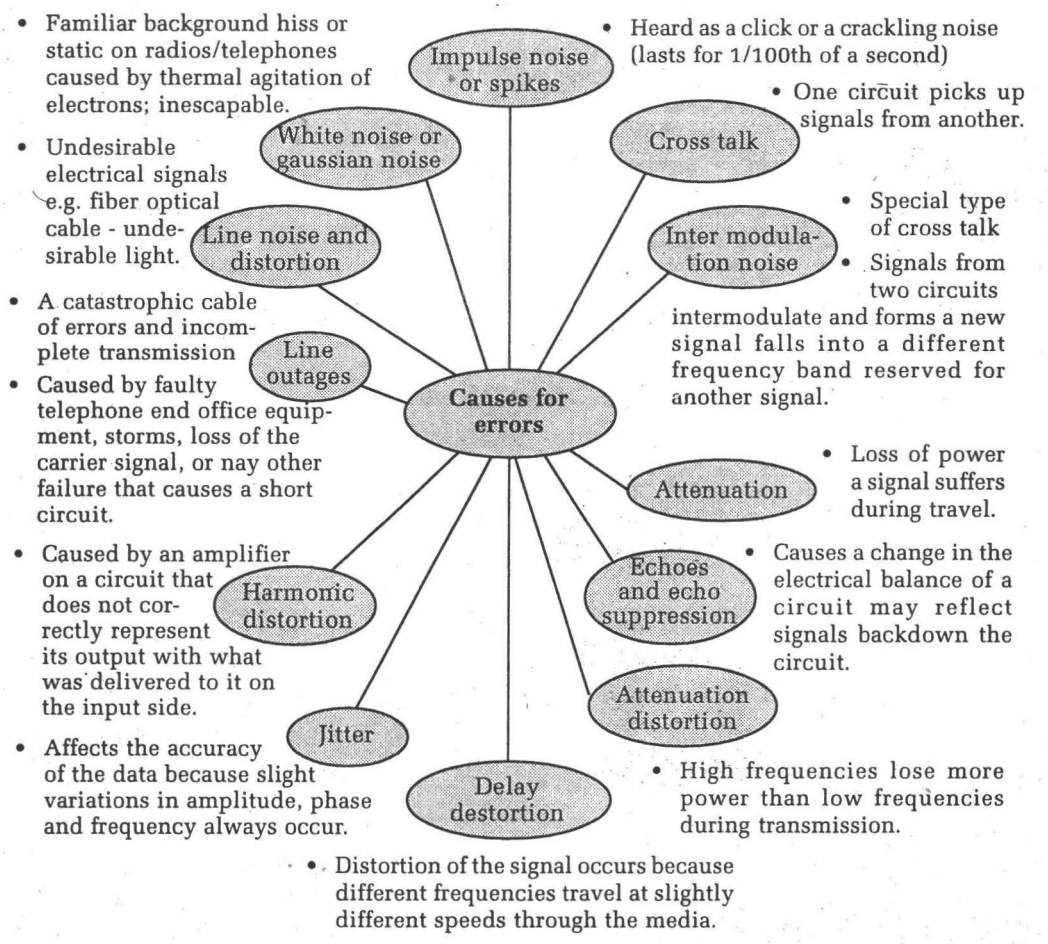


Fig. 9.2 Causes of errors

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

9.3 ERROR DETECTION METHODS

If once we know what types of errors occur, we could recognise the same. The only way to do error detection and correction is to send extra data with each message at the data link layer of the sender on the basis of some mathematical calculations performed on the message (It is also possible in some cases to build the error detection methods into the hardware itself). The receiver performs the mathematical calculations on the received message and matches the results against the error detection data that were transmitted with the message. If both tallies, the message is correct. Otherwise, error has occurred. What we need is a simple mechanism meeting the objective. It may be taken for granted that larger the amount of error detection data sent, the greater the error protection is achieved. But if the protection is increased, the throughput of useful data comes down, since the available capacity to a certain extent is used to transmit these error detection data and a small portion of it is only used to transmit the actual message itself.

Redundancy in one mechanism would satisfy the requirements by sending every data unit twice. The receiving data can compare both bit by bit. Any discrepancy would be shown as error, and an appropriate correction mechanism could be introduced in that place. This system though it is accurate it is slow since the transmission time is double and comparison time bit by bit is additional.

Error detection also uses the concept of redundancy by adding extra bits for detecting errors at the receiving end. Extra information in the transmission solely for the purposes of comparison is a good method. This technique is known as redundancy because the extra bits are redundant to the information and they will be discarded as soon as the accuracy of the transmission is known.

The mechanism is very simple. It performs the following steps. Let us assume, (i) The data as 1010100000000010 ; (ii) Redundancy check generated by generating function (after the data passes through the device and analysing the same, appropriate coded redundancy check added) as 11100111; (iii) Sender sends the data along with redundant bits to the checking function where it separates and redundancy bits. Data will be accepted and redundant bits are taken out or rejected.

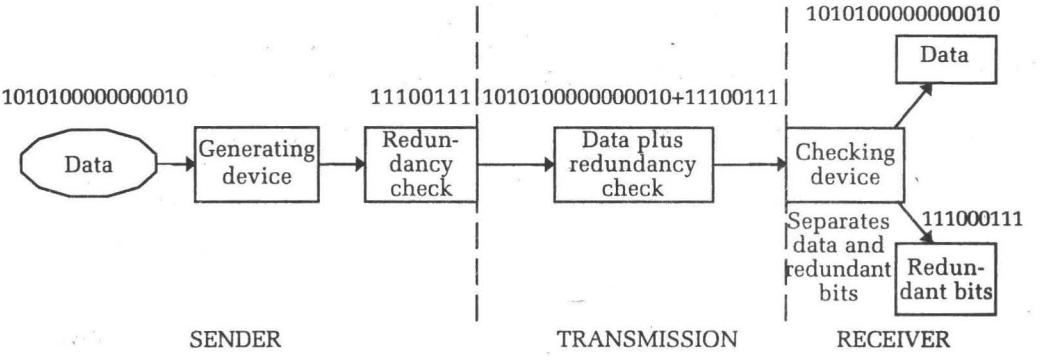


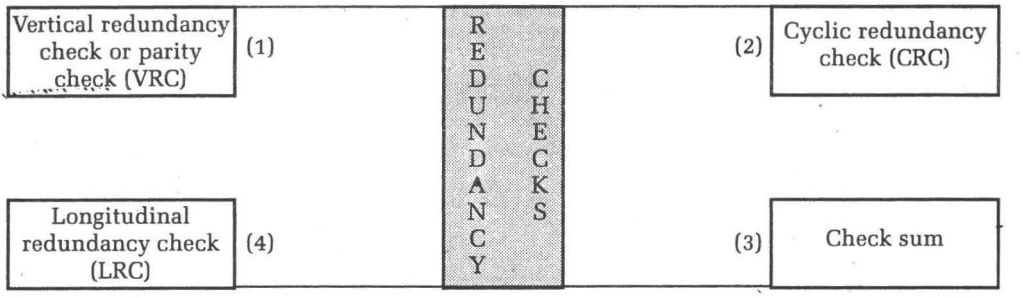
Fig. 9.3 Redundancy (Example)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Error detection methods

The four types are shown in figure 9.4 below.



Note :

(i) Check sum and cyclic redundancy are together known as polynomial checking.

(ii) Methods 1, 2, 4 shown above are implemented in the physical layer for use in the data link layer. Check sum 3 is used primarily by networks, including the Internet and is implemented in the transport layer.

Fig. 9.4 Error detection method types

The comparison of all the four are shown in tabular form (Table 1).

9.4 ERROR CORRECTION

Till now we discussed about error detection. Error corrections are indicated below. The types of errors have already been mentioned as three (a) Single bit error (b) Multiple bit error (c) Burst error. Any error once detected, it has to be corrected. A receiver which detects an error asks the sender to retransmit the entire message unit the message is received free of error. Alternatively, a receiver can use an error correcting code, which automatically corrects certain errors. Most error corrections are restricted to one two or at the most three bit errors for the reasons as under :

(i) It is possible to correct binary code errors automatically. However, error correcting codes are more complicated than error detection codes needing more redundancy bits.

(ii) The number of bits required to correct a multiple bit or burst error are very high. Further, it is inefficient to do so in a large number of cases.

Concept of error correction

As an example, let us take the simple one - single bit errors. In the case of VRC, single bit errors can be detected by the addition of a redundant (parity) bit to the data unit. A bit has two states 0 and 1 and this state is sufficient for detection. A single additional bit detects single bit errors in any sequence.

For detection and correction, two states are not enough. Error occurs when the receiver reads 1 to 0 or 0 to 1. For correction, the receiver has to reverse the value of the bit for which it should know which bit is in error (Location of the invalid bits is important). In ASCII character, you have to identify which of the seven bits is giving error? Is it in position 1 or 2 .. etc. In order to do this, this needs enough redundancy bits. Three bit redundancy code (000 to 111) can only

Copyright © 2009. Global Media. All rights reserved.

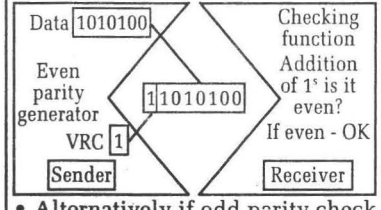
Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Vertical Redundancy Check (Parity check)

- Oldest and simplest error detection method - parity is used here.
- One additional bit is added to each byte of message (either 0 or 1)

  E.g. 7 bit ASCII for alphabet A is the data

  Letter A is 1010100 (Total number of 1s are 3) which is odd
- Transmit the data 1010100 through a parity generator to generate (0 or 1) a parity bit.
- Decide which parity check to be considered even parity or odd parity?
- Assume for the above example even parity check is required. 1010100 contains 3 – 1s and hence one more 1 is to be generated to make the total 4 – 1s which is an even parity.
- After generating 1 through the even parity generator, vertical redundancy check (VRC) becomes 1 – because of 4 – 1s
- Transmit the data now as under:



- **Alternatively if odd parity check is used VRC could be zero(0).**

Longitudinal redundancy check (LRC)

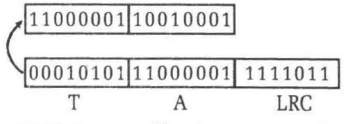
- An improvement on VRC to overcome the problems with parity's low probability of detection.
- LRC is VRC in two dimensions
- To detect multiple bits and burst errors, each bit is examined twice on the data.

eg.

LRC	A	T	A	D
1	1	1	1	1
1	0	0	0	0
0	0	1	0	0
1	0	0	0	0
1	0	1	0	1
1	0	0	0	0
1	1	0	1	0
1	1	0	1	1

LRC, BCC, Parity bit

- LRC adds one additional character, called the block check character (BCC) at the end of the entire message. The value of the BCC is determined in the same manner as the parity bit by counting longitudinally through the message using odd parity bit



- LRC is usually in conjunction with parity, producing an error detection rate above 98%.

Cyclic redundancy check (CRC)

- It adds 8, 16, 24 and 32 bits to the messages.
- A communication protocol with 16 bit CRC calculate a 16 bit number that is a function of all the data in the message. It is added at the end of the message block.
- The receiver recalculates its own 16 bit CRC when the block is received if the numbers are same, everything is acceptable. Vice-versa for error.
- Most powerful of the redundancy checking techniques. VRC and LRC based on addition. But CRC is based on binary division.
- Unlike a desired parity is obtained by adding in VRC and LRC, in CRC a sequence of redundant bits called CRC or CRC remainder is appended to the end of data unit. The resulting data unit becomes exactly divisible by a second; predetermined binary number.
- After reaching the receiver end, the incoming data unit is divided by the same number.
- If no remainder is found, the data is intact and accepted.
- The redundancy bits used by CRC are derived by dividing the (VI) same as (I) to (IV) as above

Check sum

- The technique here is a check sum (typically one byte) is added to the end of the message.

  The checksum is calculated by adding the decimal value of each character in the message and dividing the sum by 255. Use the remainder as the check sum that is transmitted to the receiver.
- The receiver calculates its own check sum in a similar way. It compares it with the transmitted check sum. If both are equal message not having any error. The checksum detects close to 95% of the errors.
- This method is used by the higher layer protocols and is based on the concept of redundancy
- At the sender end :

(i) Check sum generator divides the data unit into equal segments of n bits (say 16)

Section 1 (n bits)
2 (n bits)
:
:
m (n bits)

1+2+...m = (n bits) (Total)

(ii) Add the sum

(iii) Complement

(iv) Checksum (Minus of total)..(n bits)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

- The receiver end adds up all the ones including parity and it should even, if it is even parity check and it should be odd, if it is odd parity check.
- If the even parity checker counts 5,instead of 4, an error will be there somewhere and hence rejects the whole unit.
- VRC can detect all single bit errors. It can also detect multiple and burst errors when the total number of bits changed is odd eg. Even parity data unit (Total number of 1s including the parity bit is 6) 1100011011; change any 3 bits 1111111011, 1000001111 Total 9–1s, Total 5–1s.

  The VRC checker would return a result of 1 and the data would be rejected. This is applicable to any number of errors.

  Alternatively if two bits are changed, the number of 1s in the data unit is still even. The VRC checker will add them and return a parity of 0 even though the data unit contains 2 errors.

  Conclusion : VRC cannot detect errors if the total number of bits changed are even. The reasons being the changes cancel each other and the data unit will pass a parity check even though data unit is damaged. Same applies true for any even number of errors. Probability of detection is only 50%. Many networks do not use parity because of its low error detection rate.

- One pattern of errors that remains elusive. If two bits in one data unit are damaged and two bits in exactly the same positions in another data unit are also damaged, the LRC bit checker will not detect error.

e.g. **LRC**

0	(1)	(1)
	1	1
	0	1
	0	1
	0	0 → changed to 0,0
	0	0
	(1)	(0) → changed to 0,1
	1	0

change the 1st and last one bit in both

LRC does not effect because of changing

The combined errors of these two data units, leave both the longitudinal and vertical parties unchanged

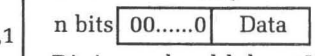
With no parity differences, an LRC checker will not show the damage.

- The above logic hold good for any even numbers of :
  - errors in corresponding position and
  - data units

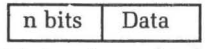
unit by the predetermined divisor. The remainder is CRC. The CRC should satisfy two conditions.

- one bit less than the divisor
- Appending it to the end of the data strong (makes the resulting bit sequence exactly divisible by the divisor)

- The major complexity is to arrive at CRC
- For this, a string of *n* 0s are put at the end of data unit.



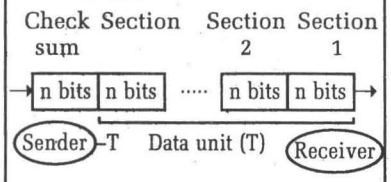
- Divisor should be nH bits (Divide using binary divisions)



Divisor (n + 1 bits)

- Remainder would be n bits which is CRC
- The CRC of n bits derived above replaces the appended 0s at end of data unit. If less than n bits, the missing left most bits are assumed to be 0s. If no reminder then the original data unit is divisible by the divisor, then n0s take the place of reminder as the CRC. The resulting bit pattern is exactly divisible.
- At the receiver end, the CRC checker yields a reminder of zero, the data unit passes. Otherwise vice versa.

(v) Transmit data as under to the receiver

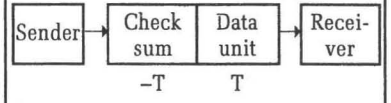


At the receiver end :

(vi) same as (i) to (iv) as above.

(vii) Add data unit section 1, section 2,.... section m) and check sum (all are of n bits)

(viii) If all are 1s in the sum, accept otherwise reject.



The receiver adds data unit and check sum. If result is all 1s, the data unit is accepted otherwise, reject.

Chec ksum detects all errors involving.

- odd number of units
- most errors involving even number of bits.

Check sum is used by the higher layer protocols (TCP/IP)

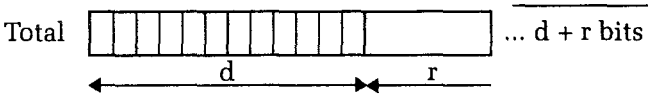
Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

show eight different states which is not enough since we have ASCII character – 7 bits plus three bits of redundancy; Total ten bits (Assuming that error might occur even in redundancy bits). Three bits are not enough to cover ten possibilities.

Assume that data bits to be transmitted are 'd' bits

and redundancy bits are '*r*' bits



There is one more state which is no error and hence d + r different states are not enough. We should have at least d + r + 1 different states to be discovered by r bits (2^r).

The formula is therefore $2^r \geq d + r + 1$. Minimum of 2 redundancy bits for any number of bits are to be considered.

For ASCII Code, d = 7
$2^4 \geq 7 + 4 + 1 \geq 13$
4 redundancy bits are required.

Hamming code

A technique was developed by R.W. Hamming for an error correction code wherein the redundant bits are inserted at predefined positions.

Example : 7 bit ASCII code (As already said, four redundancy bits can be added to the end of the data unit or mixed with the original data bits); Total bits are 11.

11	10	9	8	7	6	5	4	3	2	1
d	d	d	r_8	d	d	d	r_4	d	r_2	r_1
.	.	.	2^8	.	.	.	2^3	.	2^2	2^1

Note : r_1, r_2, r_4, r_8 are redundancy bits placed in 1,2,4 and 8 positions.

In hamming code :

r_1 bits are a combination of various data bits for 1, 3, 5, 7, 9, 11 positions

r_2 bits are a combination of various data bits for 2, 3, 6, 7, 10, 11 positions

r_4 bits are a combination of various data bits for 4, 5, 6, 7 positions

r_8 bits are a combination of various data bits for 8, 9, 10, 11 positions

(Each r bit is the VRC bit for one combination of data bits)

E.g. 1, 3, 5, 7, 9, 11 have binary numbers 0001, 0011, 0101, 0111, 1001, 1011 respectively (all have 1 at the right most position)

Similarly 2,3,6,7,10 11 have binary numbers 0010, 0011, 0110, 0111, 1010, 1011 respectively (all have 1 at the second positions)

4, 5, 6, 7 binary number 0100, 0101, 0110, 0111 respectively (all have 1 at the third position)

8, 9, 10, 11 have binary number 1000, 1001, 1010, 1011 respectively (all have 1 at the fourth position)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

The parity value for each combination is the value of the corresponding r bit.

The value of r_1 is calculated to provide even parity for a combination of bits 3, 5, 7, 9 & 11

Similarly r_2 is calculated for 2, 3, 6, 7, 10 and 11 and so on.

The final 11 bit code is sent through the transmission line

Error detection and correction

Let us take the data transmission is as under from sender to the receiver

Data sent

1	0	0	1	0	1	0	1	0	1	1

Data received

1	0	0	1	1	1	0	1	0	1	1

Error has occurred 0 to 1 at the 7th bit (may be due to line noise)

Error has occurred 0 to 1 at the 7th bit (may be due to line noise) By the time the above transmission is received at the receiver end, the number 7 bit has been changed from 0 to 1. The receiver recalculates four new VRCs using the same set of bits and the relevant parity sent by the sender. It converts the parity values into binary number in the r positions (r_1, r_2, r_4 and r_8). In the seventh position that is r_1 – 7th position, it gives 0111 (7 is decimal), which happens to be the precise location of the bit in error once the bit is identified as wrong, the receiver can reverse its value and then correct the error.

Multiple bit correction

As already said in the beginning of para 9.3, the redundancy bits to make corrections in this case will be very high as compared to single bit errors. But here also it is possible to calculate redundancy bits on overlapping sets of data bits in the same way as used for single bit errors. To correct double bit errors it is to be considered that the two bits can be a combination of any two bits in the entire sequence. Similarly for three bits correction, the combination would be three bits in the entire sequence and so on. The situation becomes complicated. More sophisticated schemes to tackle these have been worked out and are not dealt in this book.

CRC generator

For the data unit, we are appending n bits of 0s. The divisor is n +1 bits. The divisor is n + 1 bits.

As an example we will take, data unit as XXXXXX. Divisor should be YYYY (4 bits).

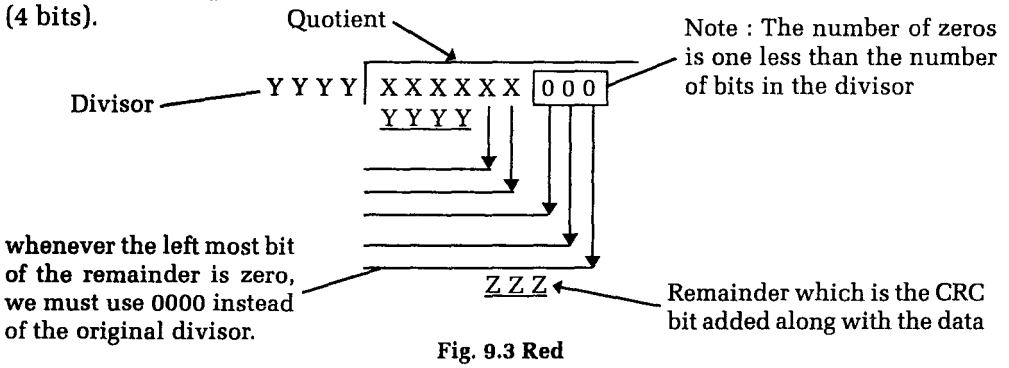


Fig. 9.3 Red

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

The CRC generator (divisor) is representation an algebraic polynomial but not as a string of 1s and 0s, because of the latters usefulness as shortness and the ability to prove the concept mathematically.

The standard polynomials are 12, 16 and 32 (refer to the size of the CRC remainder) for CRC generation with divisors 13, 17 and 33 bits respectively
CRC 12 is $x^{12} + x^{11} + x^3 + x + 1$ CRC ITU is $x^{16} + x^{12} + x^5 + 1$
CRC 16 is $x^{16} + x^{15} + x^2 + 1$
CRC 32 is $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

The relationship between polynomial to binary

This is as shown below :

A polynominal of CRC 12 is $x^{12} + x^{11} + x^3 + x + 1$. A divisor for this would be

	x^{12}	x^{11}	x^{10}	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x	1
Divisor	1	1	0	0	0	0	0	0	0	1	0	1	0

These are not in the polynomial.
Hence 0.

POINTS TO REMEMBER

- Two types of basic errors which are to be implemented to protect a network from errors are human errors and network errors. Network errors occurs during transmission.
- Two types of data errors in the network found are : corrupted data, lost data the various type of errors found during transmission are single bit error, multiple bit error and burst error. There are various causes for errors.
- Transmission errors are usually detected and corrected at the physical layer and the data link layer of the OSI model. Redundancy is one mechanism would satisfy the requirements by sending every data unit twice.
- Four common methods of error detection are (i) Vertical Redundancy Check (VRC) or Parity Check (ii) Longitudinal Parity Check (iii) Cyclic Redundancy Check (CRC) and (iv) Check Sum
- VRC adds extrabit known as parity bit to each byte of the message. It can detect only an odd number of errors and cannot detect an even number of errors.
- LRC is VRC in two dimensions. LRC error detection groups a predetermined number of data units, each already containing a VRC parity bit together into a block. On the other hand CRC is the most powerful than the other two techniques is based on binary division.
- Check sum is worked out in the following steps : (1) Whole data is divided into equal sections (2) Add the sections together by using one's complement arithmetic (3) Complement the final sum which would be the checksum.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

Repetition occurs at the receiver end to calculate the checksum; the data and checksum should add upto 0 for no errors.

- The Hamming code is a single bit error correction code. It associates parity bits with unique combination of data bits. The redundant bits are inserted at predefined positions. The formula used here is $2^r \geq d + r + 1$ where d is data unit of d bits, r is number of redundant bits. With this formula, r can be worked out.

QUESTIONS

1. What are the two basic types of errors which occur in a network?
2. What are the two categories of data errors found in a network?
3. What are the factors to be studied while selecting an error control system?
4. What are the different types of errors found during transmission? Explain them.
5. What do you mean by single bit error? Explain.
6. What do you mean by multiple bit error? Explain.
7. What do you mean by burst error? Explain.
8. What are the different causes for errors? Explain in brief.
9. What is error detection? How is it achieved?
10. What are the different methods of error detection? Explain in brief.
11. What do you mean by redundancy check? What are the different types of redundancy checks?
12. Compare and contrast Vertical redundancy check with Horizontal redundancy check?
13. What is parity check? Explain.
14. What is longitudinal redundancy check? Explain
15. What do you mean by cyclic redundancy check? Explain.
16. Compare and contrast VRC, LRC and CRC.
17. What do you mean by check sum? Explain the technique.
18. Explain a CRC Generator.
19. What are polynomials? Explain the relationship of a polynominal to its corresponding binary representation with a sketch.
20. What are the standard polynomials used by popular protocols for CRC generation?
21. What is check sum generator? Explain its function.
22. Compare and contrast error detection with error correction.
23. Explain how a single bit error correction is effected?
24. What is Hamming code? Where it used? How does it function?
25. Why multiple bit error correction is more complex single bit error correction?

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

FILL IN THE BLANKS

1. Network errors are the errors which occur during _____.
2. Transmission error detection is usually done in the _____ layer and error correction is usually done at the _____ _____ layer of the OSI model.
3. Two categories of data errors in the network are _____ data and _____ data.
4. The error detection method using parity bit is _____ _____ _____ method.
5. _____ is a mechanism which sends every data unit twice.
6. _____ uses one's complement arithmetic.
7. Character D is sent, C is received in ASCII character, the type of error is _____. Similarly H to I is _____ bit.
8. Polynomials are used in _____ error detection method.
9. The Hamming code is a method of error _____ and _____.
10. In CRC the quotient at the sender is _____.
11. In CRC the remainder at the CRC is _____.
12. In cyclic redundancy checking the CRC is the _____.
13. _____ is the error detection method consists of just one redundant bit per data unit.
14. LRC is _____ in two dimensions.
15. In VRC additional bit is added to each _____ of the message. VRC can detect only an _____ number of errors.
16. _____ redundancy check is based on binary division.
17. _____ and ____ redundancy checks are based on addition.
18. In checksum, one _____ is added to the end of the message.
19. In _____ the receiver end adds up all the 1s and should be even for the even parity check.
20. CRC should satisfy two conditions ____ ____ less than the divisor; appending it to the end of the _____ _____.
21. Error correcting codes needs more _____ _____ than error detection codes.
22. A Hamming code is a technique where _____ _____ are inserted at predefined positions.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

23. The standard polynomials are ____; ____ and ____ for CRC generation with divisors _____, _____ and _____ bits respectively.

Answers

1. transmission
2. data link or transport
3. corrupted ; lost
4. vertical redundancy check
5. Redundancy
6. Checksum
7. single bit ; burst
8. CRC
9. detection ; correction
10. discarded
11. zero
12. remainder
13. VRC
14. VRC
15. byte ; odd
16. Cyclic
17. Vertical ; longitudinal
18. byte
19. VRC
20. one bit ; data string
21. redundancy bits
22. Redundant bits
23. 12 ; 16 ; 32 ; 13 ; 17 ; 33

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 15:06:37.

UNIT 3

CHAPTER 10
DATA LINK CONTROL

CHAPTER 11
DATA LINK PROTOCOLS

CHAPTER 12
LOCAL AREA NETWORKS

CHAPTER 13
METROPOLITAN AREA NETWORKS (MAN)

CHAPTER 14
SWITCHING

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

10

DATA LINK CONTROL

Communication needs two devices minimum for working.

(i) To send the message

(ii) To receive the message.

We have observed that in half duplex transmission, only one device would transmit at a time. If both ends of the link transmits simultaneously, they collide resulting only in noise. Hence a line discipline is needed. This is one of the important functions of the data link layer. It takes the message generated by the network layer and performs the following three functions before passing the message to the physical layer.

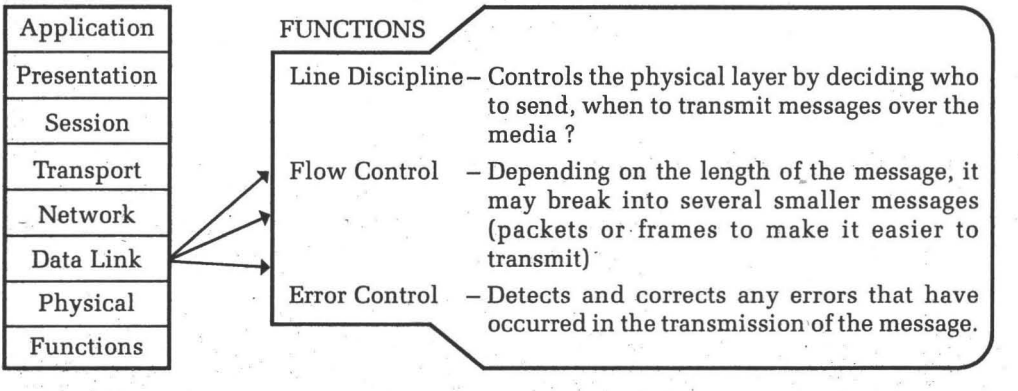


Fig. 10.1 Data link layer functions

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

A data link protocol determines :	
(i) Who should transmit at what time?	– LINE DISCIPLINE
(ii) Where a message begins and ends? How much data may be sent?	– FLOW CONTROL
(iii) How a receiver recognises and corrects a transmission error?	– ERROR CONTROL

10.1 LINE DISCIPLINE

It is a data link layer procedure defining which device has the right to send data at a given time also referred to as access control. It oversees the establishment of links and the right of a particular device in the above context. It is performed in two ways :

(i) Enquiry / Acknowledgement ENQ/ACK (used in peer - peer communication)

(ii) Poll / Select (used in primary - secondary communication)

ENQ/ACK

The systems are to be so set that there is no question of the wrong receiver getting the transmission, when there is a dedicated link between the two devices. The receiver should receive the transmission as intended. ENQ/ACK coordinates two aspects :

(i) Which device should start a transmission?

(ii) Whether the intended recipient is ready or not? How to make sure?

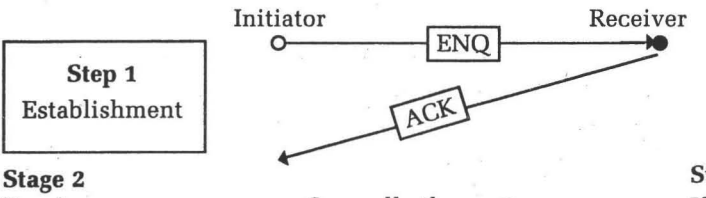
ENQ/ACK enables a session which can be initiated by either station – on a link, if they are of equal rank. The initiating device establishes the session which is possible in half duplex and full duplex transmission,

In half duplex { Initiator sends data → Responder waits } ↓

(Initiator Waits ← Responder takes over and sends data (after the initiator finishes)

In full duplex Both devices can transmit simultaneously (after the session is established).

Working of ENQ/ACK



Stage 1
Initiator transmits a frame enquiry (ENQ), wants to know whether the receiver is ready to receive the data.

Stage 2
Receiver answers either with an acknowledge (ACK) or negative acknowledge (NAK) frame if not ready

Generally three attemps made to establish a link before completely withdrawn. Attempt will be made again after sometime.

Stage 3
If no ACK or NAK received within a specified time, the initiator assumes that ENQ frame was lost in transition, disconnects and sends a replacement.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

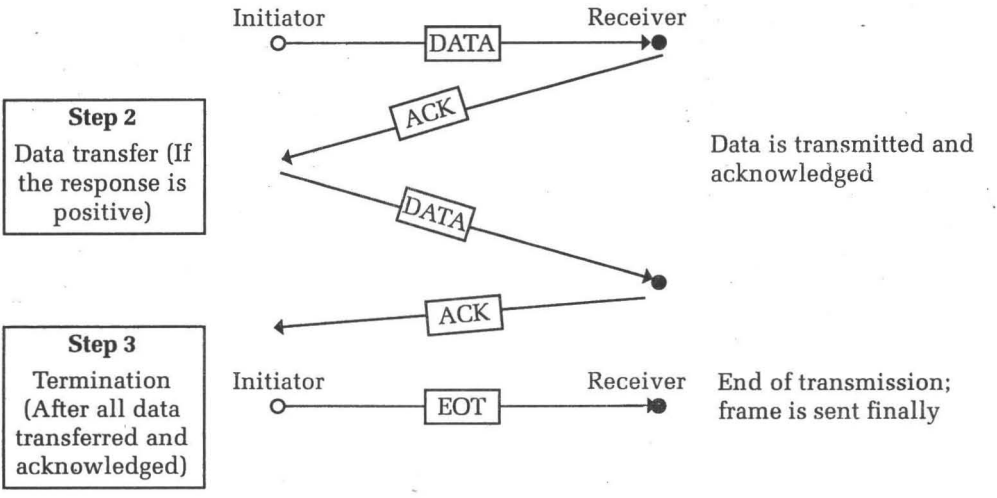


Fig. 10.2 ENQ/ACK line discipline

Poll / Select

This method of line discipline works where one device is a primary and the other devices are secondary. Multipoint systems must coordinate number of nodes which of the nodes have the right to use the channel is the question ?

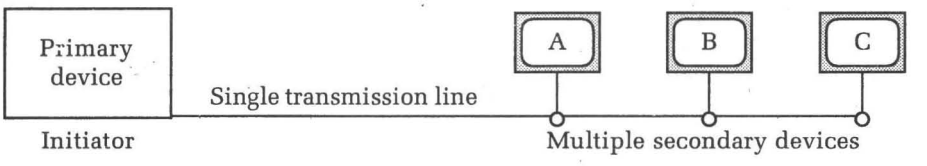


Fig. 10.3 Discipline in multipoint devices

Multiple secondary devices using a single transmission line if connected to the primary devices, all exchanges are made through the latter. The primary device controls the link and the secondary device follows the primary device instructions. Primary device decides which secondary device is to be allowed to use the channel at a given time. The primary acts as an initiator of the session.

On the contrary, if the primary wants to receive the data, it questions the secondaries if they have anything to send. In this sort of primary/secondary access method, a procedure in which the primary station asks a secondary station if it has any data to transmit.

In primary/secondary access method, where the primary device has to identify and communicate with a specific secondary device in a multipoint technology, the secondary device has to be named. Otherwise, without identification it could be difficult to identify the device. This is known as addressing. No addressing is required in the case of point to point configuration. The select mode is used when the primary device has something to send to the certain secondary device. The primary being the controller of the link, sometimes do not send or receive if the link is not available. The primary alerts the secondary to the upcoming transmission and wait for an acknowledgement if the secondary is ready to send. So also while sending data, the primary creates and transmits a

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

select (SEL) frame. It addresses the intended secondary by including one field. The secondary checks the address field when the frame is sent down the link by the primary the concerned secondary checking the address opens the frame and reads the data. The working of poll/select method is as shown below.

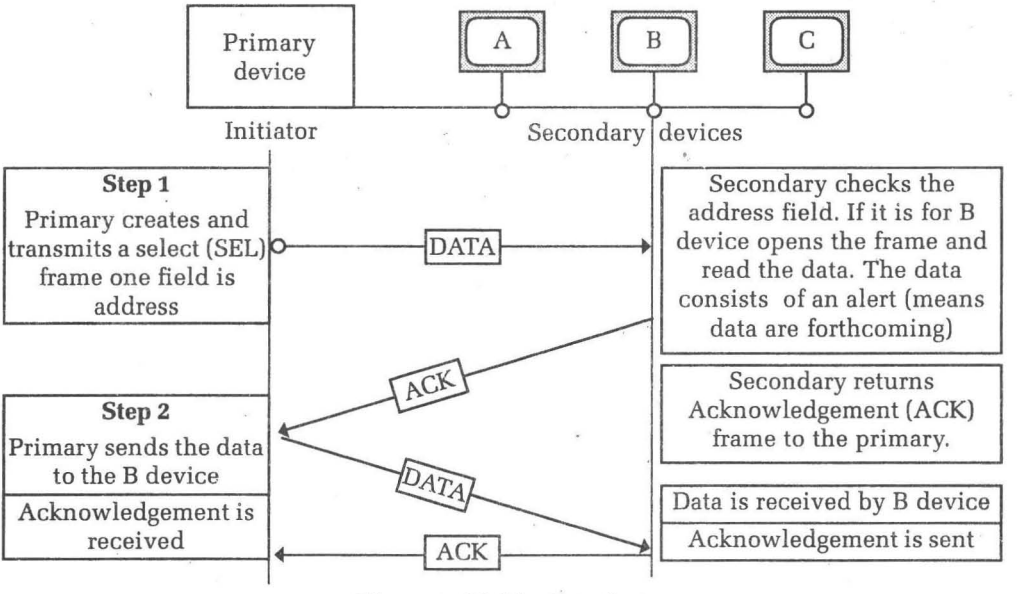


Fig. 10.4 Multipoint select

The multipoint guarantees that only one transmission can occur at a time; to ensure no collisions of signal takes place without requiring elaborate procedure protocols.

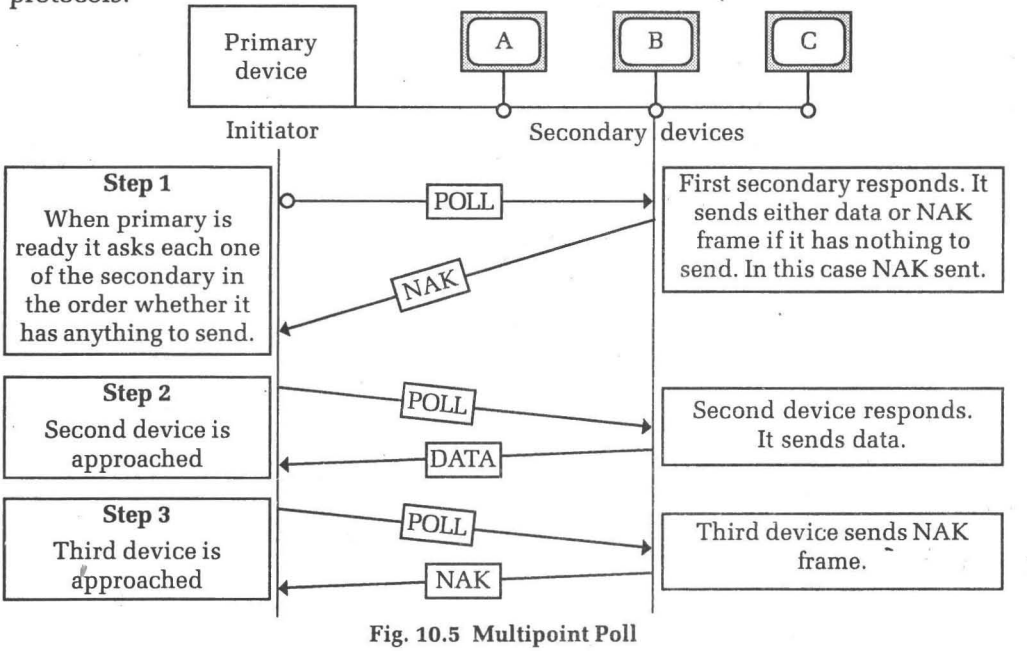


Fig. 10.5 Multipoint Poll

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Two possibilities of terminating the exchange are :

- Secondary completes all its data by sending; Finally sends an end of transmission (EOT) frame or
- Primary stops saying 'Time is over'

The above takes place depending on the protocol and length of the message. After this, the primary can poll the remaining devices.

10.2 FLOW CONTROL

As already said earlier, flow control is a set of procedures in most protocols which informs the sender the amount of data it can transmit before it must wait for an acknowledgement from the receiver. Following points need attention.

(i) The receiving device has its own limitations :

- It has a limited speed at which processing of incoming data is carried out. Incoming data must be checked and processed before they can be used.
- Limited amount of memory to store incoming data.
- Rate of processing at the receiving end is slower than the rate of transmission. Hence the receiving device is to inform the sending device its limitations when it is reached and to request the sending device to send fewer frames or to stop temporarily. Each receiving device has a block of memory known as buffer reserved for storing incoming data till they are processed. If buffer gets filled in, receiver should tell the sender to stop transmission for some time.

(ii) Frames received are acknowledged individually or in groups at a time. If frame arrives not properly, the receiver sends an error message through an NAK frame.

To control the flow of data through communication links, two popular methods have been adopted.

- Stop and wait
- Sliding window

Stop and wait method (sending only one frame at a time)

In stop and wait control, each frame is acknowledged by the receiver before the next frame is sent by the sender. In sliding window flow control, the sending of data is constrained with the help of an imaginary window based on the acknowledgements received by the sender. These windows may either expand or contract. Similarly the receiving data also have an imaginary window which constraints. These windows expand and contract according to the data received.

The working of this as shown in figure 10.6 :

Advantage of stop and wait :

(i) Simplicity

(ii) Every frame is checked and acknowledged before next frame is sent.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Disadvantages :

(i) Inefficiency

(ii) Slow because of the waiting time

(iii) If distances are more between devices, time spent of ACKs will be long.

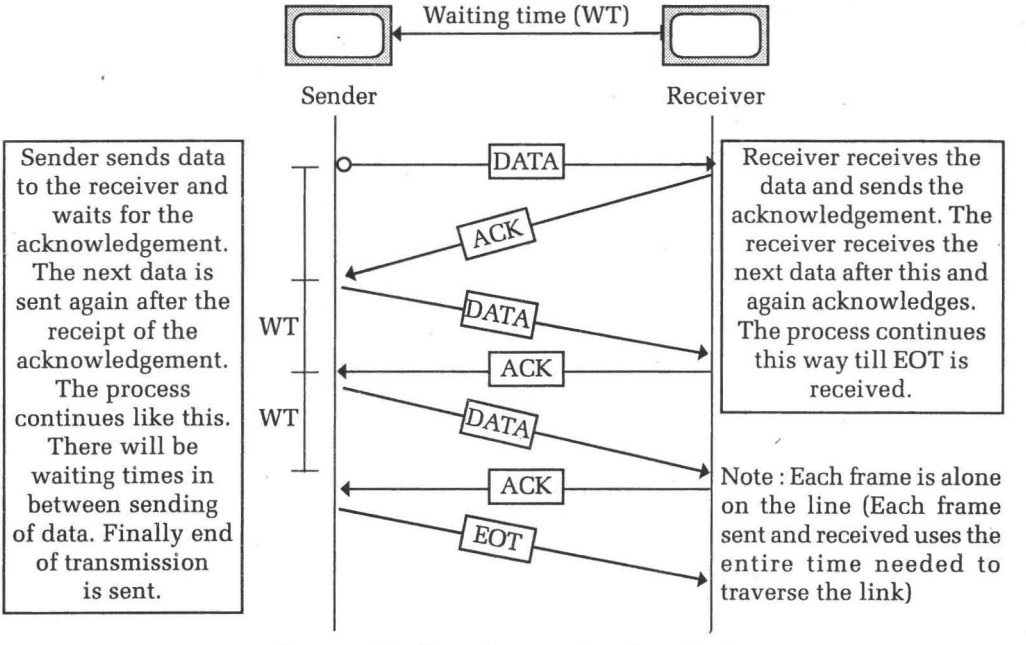


Fig. 10.6 Working of stop and wait method

Sliding window (Sending several frames at a time)

Here the sender transmits several frames before needing an acknowledgement. The link carry several frames at once (sent one right after another) and hence capacity is used efficiently. The receiver acknowledges to receipt of only some of the frames.

Window here is sliding window referring to an extra buffer created at both the ends (sender as well as receiver). The windows can hold frames at either ends and upper limit on the number of frames that can be transmitted could be worked out (before requiring an acknowledgement). The receiver acknowledges at any point, without waiting for the windows to fill up (though not full). Sliding window to keep a track of which frames have been transmitted and received, introduces an identification scheme.

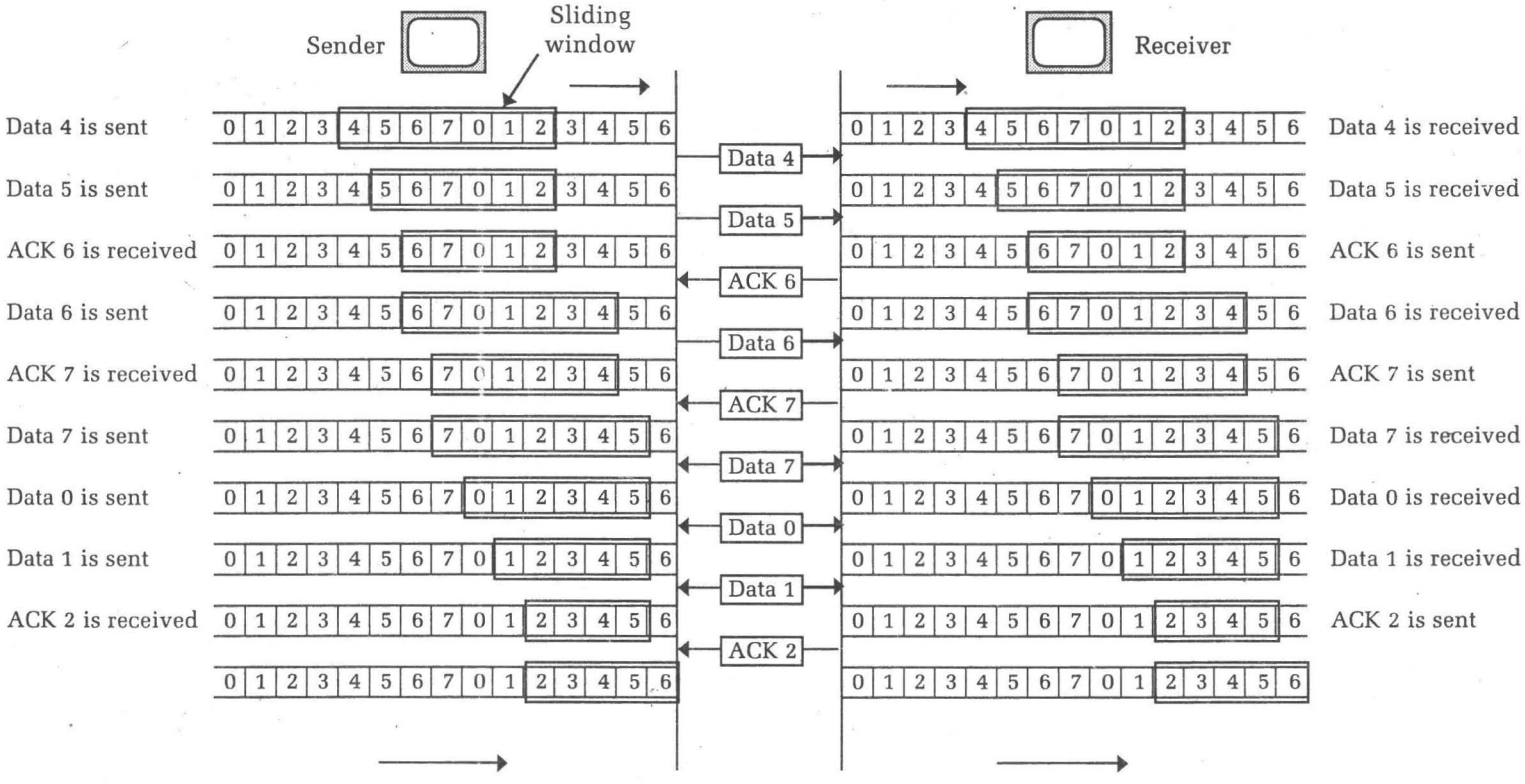
Eg. Frame with modulo-n numbering will have numbers 0 to n-1. If 8 frames are in a module, the size of the window will be 7. That is, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, ...

When the receiver sends an acknowledgement, it is expecting the next frame number it has to receive. Acknowledgement for the receipt of a string of frames ending is 4, the receiver sends an ACK containing the number 5. It is understood by the sender from this that all frames up through number 5 have been received.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

The working of sliding window is as follows :



Note : In the example shown above 4,5, 6, 7, 0, 1, 2 the sliding window acknowledgement 6 means, data upto 5 have been received.

Fig. 10.7 Working of Sliding Window

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

10.3 ERROR CONTROL

The most commonly used method for error correction is retransmission. Using this, a receiver detects an error and asks the sender to retransmit the message until it is received without error. This is often called Automatic Repeat Request (ARQ). This happens in three cases – damaged frame, lost frame, and lost acknowledgement. The frame is so damaged by noise during transmission that the receiver do not recognise the complete frame.

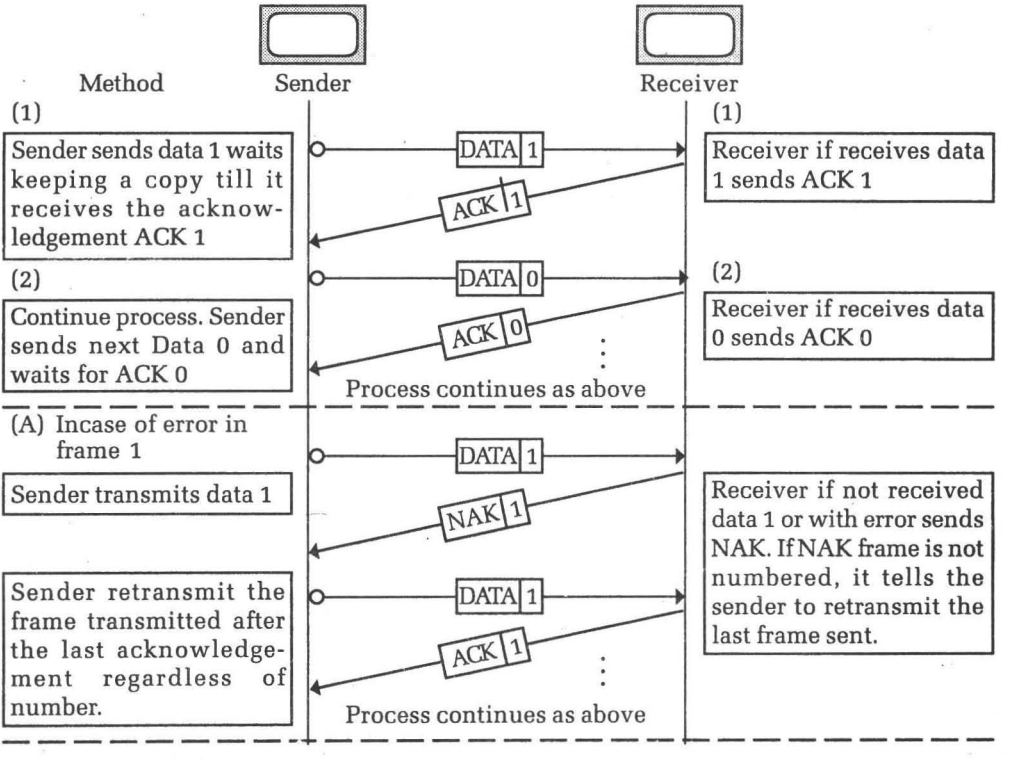
	Retransmission required incase of:	Effect	
(i)	Damaged frame due to noise	Frame has been completely lost	ARQ allows us to say that the frame has been lost
(ii)	Lost frames and lost acknowledgement	Frames are lost (including lost ACK and NAK frames)	

Two categories of error control are :

- Stop and wait ARQ (Half duplex transmission technique)
- Sliding window ARQ (Continuous ARQ) — Selective - reject / Go back - n
  (A fullduplex transmission technique)

Stop and wait ARQ

It is nothing but stop and wait flow chart + including retransmission of data in case of lost or damaged frames. The working is as under :-



Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

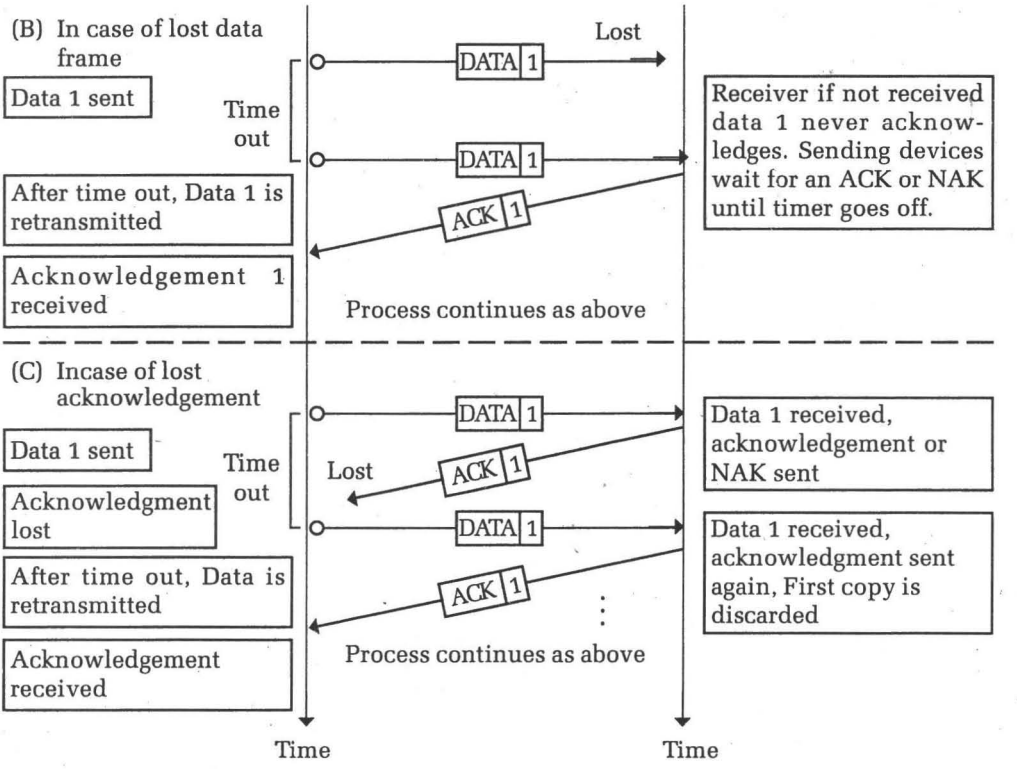


Fig. 10.8 Stop and Wait ARQ

With stop and wait ARQ, the sender stops and waits for a response from the receiver after each message or packet of data. The sending device is equipped with a timer to handle lost acknowledgements.

Sliding window ARQ or continuous ARQ

Under this, two protocols are most popular :-

- Go–back–n ARQ
- Selective – reject ARQ

Both are based on sliding window flow control.

Go-back-n ARQ

In a sliding window go-back-n-ARQ method if one frame is lost or damaged, all frames sent until the last frame acknowledged are retransmitted.

E.g. Assume that 0, 1, 2, 3, 4 frames transmitted 1st Acknowledgement is NAK 4 This shows that data frames 0, 1, 2 and 3 were received in good condition. Only frame 4 is to be resent.

If frames 0, 1, 2, 3 have been transmitted and NAK is received for frame 2. The receiver do not accept subsequent frames until the damaged frame is replaced correctly. Data 2 arrives damage and so is discarded. So also data 3 though may be intact and already sent, it has to be retransmitted again after frame 2.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

See the example below for damaged data frame :

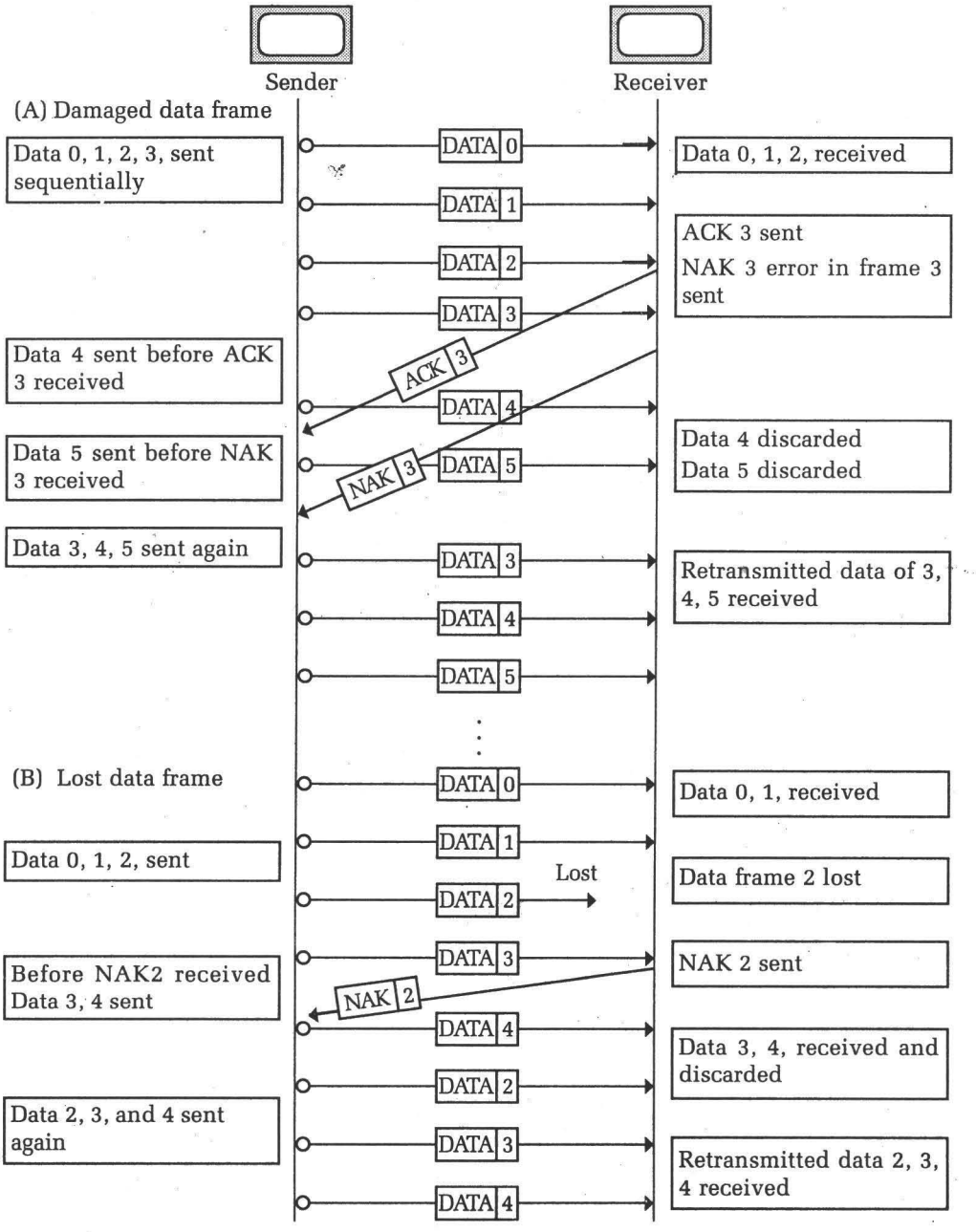


Fig. 10.9

NAK2 received here indicates that 0 and 1 have been accepted; but 2 is in error (lost). The sender in between has already transmitted 3 and 4 before receiving NAK2, data 4 arrives at the destination out of sequence and hence data 3 and 4 are discarded. Hence retransmission of data 2, 3 and 4 done again.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

The lost acknowledgement under go-back-n is as shown below :

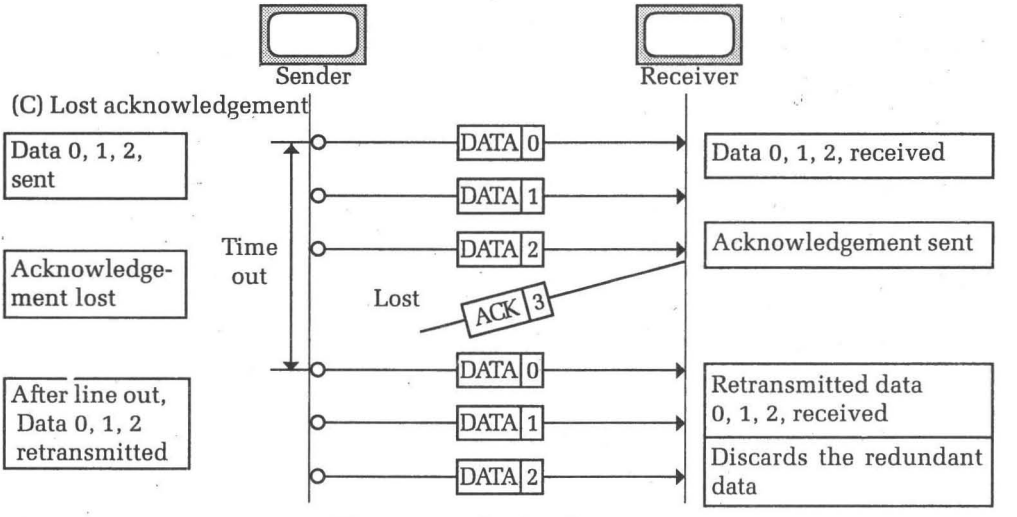


Fig. 10.10 Go-back-n, lost ACK

If the ACK or NAK sent by the receiver has been lost, the sender could wait for ever. To avoid tying up both devices, the sender is equipped with a timer that begins counting as soon as the window capacity is reached. If an acknowledgement has not been received within the time limit, the sender retransmits all the frame transmitted since the last ACK/NCK.

Selective - Reject ARQ

In this case, only the specific damaged or lost frame is retransmitted. If any frame is corrupted during transmission, a NAK is returned and this frame can be sent again, out of sequence also. The receiving device would be able to sort out the frames and insert the corrected frame into its proper place in the sequence. The working of selective – reject ARQ is as under :

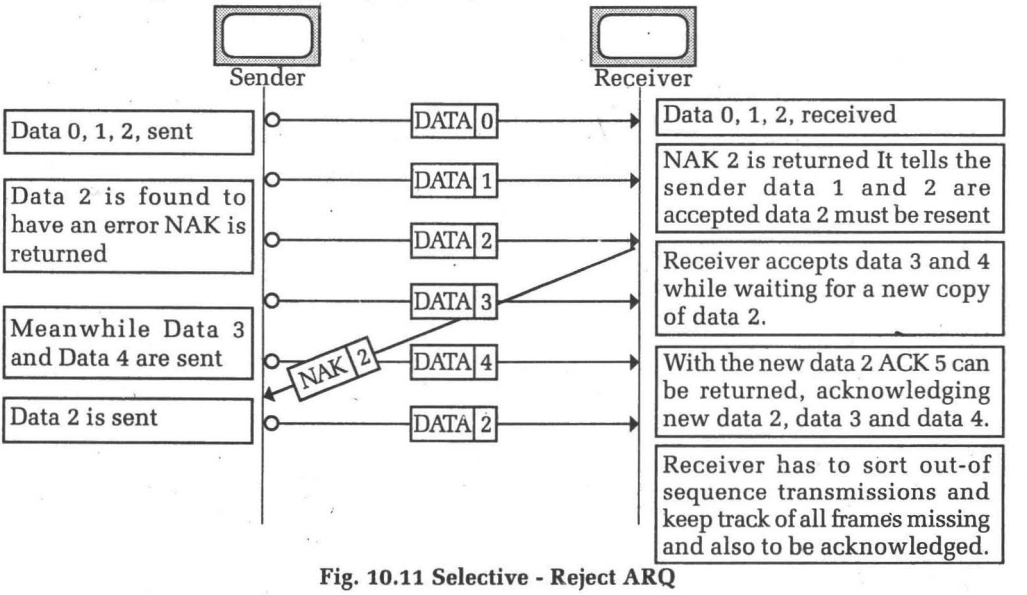


Fig. 10.11 Selective - Reject ARQ

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Go–back–n	Selective-reject
Involves retransmission of several un-damaged frames, if a damage takes place.	Retransmitting only specific damaged or lost frames. Efficiency looks high but in reality it is no so.
Simplicity of implementation	Complexity of the sorting & storage by the receiver; Extra logic needed by the sender to select specific frames for transmission;
Less expensive	The above makes selective reject expensive and not used.
This method is preferred	Gives better performance; But still this method is discarded.

Table comparison between Go-back-n and selective-reject

POINTS TO REMEMBER

- Communication needs two devices minimum for working (i) to send the message (ii) to receive the message. The second layer in the OSI model, which is the data link layer has three main functions; line discipline, flow control, and error control.
- Line discipline is a data link layer procedure defining which device has the right to send data at a given time also referred to as access control. It is performed in two ways. Enquiry / Acknowledgement (ENQ/ACK) used in peer–peer communication or point to point connections.
- The receiver using ENQ/ACK line discipline responds by sending an acknowledgement either as ACK if it is ready to receive data or as NAK (Negative Acknowledge) if it is not ready.
- Poll/select is a method of line discipline works where one device is a primary and the other devices are secondary. Multipoint system must coordinate number of nodes. The primary device initiates communication with either a poll or select (SEL) frame. The primary device controls the link and the secondary device follows the instructions. In the primary/secondary access method, a procedure in which the primary station asks a secondary station if it has any data to transmit. This is known as poll. The secondary can respond by sending a NAK (no data to send) or a data frame.
- Flow control is a set of procedures in most protocol which informs the sender the amount of data it can transmit before it must wait for an acknowledgement from the receiver. It is a regulation of data transmission to ensure that the receiver buffer does not become overwhelmed with data.
- Two popular methods adopted in controlling the flow of data are
  - Stop and Wait (only one frame at a time)
  - Sliding window (several frames at a time)

  In stop and wait control, each frame is acknowledged by the receiver before the next frame is sent by the sender. In sliding window flow control, the

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

sending of data is constrained with the help of an imaginary window based on the acknowledgements received by the sender. These windows may either expand or contract. Similarly the receiving data also have an imaginary window which constraints. These windows expand and contract according to the data received.

- The most commonly used method for error correction is retransmission. The receiver detects an error and asks the sender to retransmit the message until it is received without any error. This is often called Automatic Repeat Request (ARQ) Retransmission of data is initiated by ARQ.
- Two categories of error control are :
  - Stop and wait ARQ
  - Sliding window ARQ or continuous ARQ

  In continuous ARQ, there are two subdivisions :
  - Go-back-n ARQ
  - Selective-reject ARQ
- With stop and wait ARQ, the sender stops and waits for a response from the receiver after each message or packet of data. After the receipt of a message or packet, the receiver sends an ACK or NAK (negative acknowledgement) if the message received is without error or with error respectively. It is a half duplex transmission technique.
- With continuous ARQ, the sender does not wait for an acknowledgment after sending a message; it immediately sends the next one. While messages are being sent, the sender examines the stream of returning acknowledgements. If NAK received, the sender retransmits the needed messages.
- Three types of errors on ARQ are :
  - A damaged frame
  - A lost frame
  - A lost acknowledgement
- The method used to handle error control depends on the methods of flow control; for stop–and–wait flow control, stop–and–wait ARQ is used. Go–back–n ARQ is for sliding flow control, wherein retransmission begins with the last unacknowledged frame even if subsequent frames have reached correctly. Here duplicate frames are discarded. In selective reject ARQ, only the unacknowledged frame is retransmitted.

QUESTIONS

1. Which are the two devices needed for communication?
2. What are the functions of data link?
3. What is line discipline? How is it performed?
4. Explain ENQ/ACK and its working.
5. Explain poll/select. How does it work?

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

6. What do you mean by multipoint select?
7. Why and where is flow control needed? Explain its parameters.
8. Explain stop-and-wait flow control with special reference to the handling of (i) a damaged frame (ii) a lost frame.
9. In stop and wait ARQ, what happens if NAK is lost? Explain the reason why there is no necessity to number NAK?
10. What are the advantages of stop and wait method?
11. Explain sliding window method's working? Which sliding window ARQ is more popular ? Why?
12. Compare and contrast Go-back-n ARQ with selective–reject ARQ.
13. The frames are discarded in all the three ARQ methods in a particular situation. When?
14. What do you mean by error control? How it happens?
15. Explain selective–reject ARQ with a sketch.

FILL IN THE BLANKS

1. Flow control is needed to present _____ of the receiver buffer.
2. _____ _____ is the transmission of damaged or lost frames in the data link layer.
3. In sliding window the sender transmits several frames before needing an _____.
4. With _____ ____ _____ _____, the sender stops and waits for a response from the receiver after each message of data.
5. In sliding window flow control, if the window size is 16, the range of the sequence numbers is 0 to ____.
6. In sliding window flow control, the frames to the left of the receiver window are frames received and _____.
7. In go-back-n ARQ if frames 'n' are received successfully, the receiver may send an ACK _____ to the sender.
8. For a sliding window of buffer size 'n', there can be a maximum of ___ frames sent unacknowledged.
9. _____ decides the sender's role of device on a network.
10. ENQ/ACK is used in _____ – _____ communication in where as poll/select is used in _____ – _____ communication.
11. The expansion of ARQ is _____ _____ _____.
12. In stop and wait ARQ, if data 5 has an error, the receiver sends _____ frame.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

13. In sliding window flow control (window size 16) ACK 3 means that the frame ____ is next expected by the receiver.
14. In _____ ARQ the sender does not wait for an acknowledgement after sending a message.
15. _____ ARQ is by definition, a half duplex transmission technique where as _____ ARQ is full duplex transmission technique.

Answers

1. overflow
2. error control
3. acknowledgement
4. stop and wait ARQ
5. 16
6. acknowledged
7. n + 1
8. n
9. Line discipline
10. peer, peer ; primary, secondary
11. Automatic Repeat Request
12. NAK
13. 3
14. continuous
15. stop and wait ; continuous

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

11

DATA LINK PROTOCOLS

In simple words *protocols* means rules for communication. A *protocol* in data communications is set of rules or specifications for implementing one or more layers of the OSI Model.

E.g. EIA 232–D interface which is a protocol used at the physical layer of the OSI model.

The sets of specifications used to implement the data link layer are known as data link protocols, containing rules for line discipline, flow control and error handling etc.

The two categories of data link protocol are :

- Asynchronous protocols – Treat each character in a bit stream independently.
- Synchronous protocols – Takes the whole bit stream and chop into characters of equal size.

Asynchronous protocols

Asynchronous transmission is referred to as start – stop transmission because the transmitting device can transmit a character whenever it is convenient and at the time the receiving device will accept that character. This is used on point to point full duplex circuits.

The different types of asynchronous data link protocols developed in the last few decades are shown in figure 11.1.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

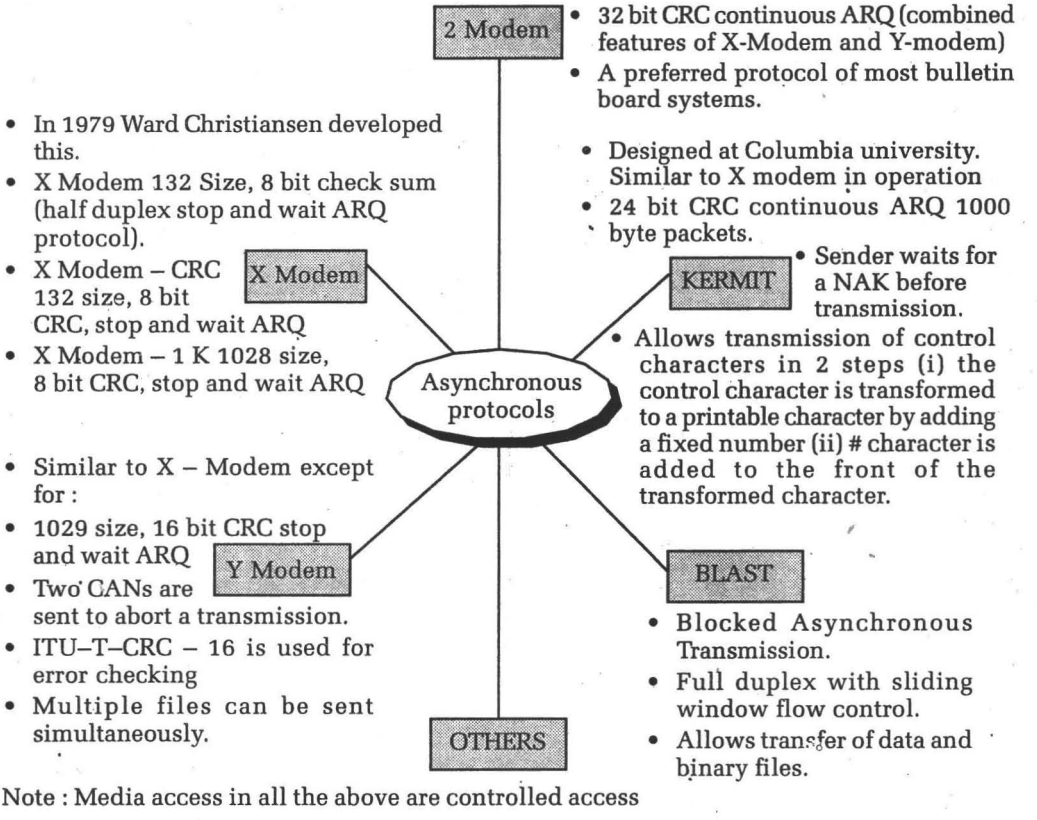


Fig. 11.1 Asynchronous protocols

X - Modem

The frame, fields of X - Modem are shown below :

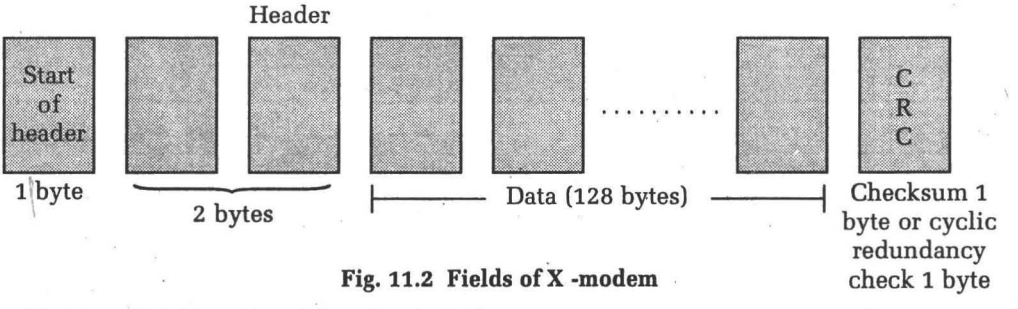


Fig. 11.2 Fields of X -modem

(i) First field is start of header (SOH)
(ii) First header byte – sequence number carries the frame number
(iii) Second header byte – to check the validity of the sequence number
(iv) Data field holds 128 bytes of data (binary, ASCII, Boolean, text etc)
(v) Last field CRC checks for errors in the data field.

It may be noted that each character contains start and stop bits. Characters are separated from each other by gaps. The header consists of two bytes : as detailed above.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

In this protocol, the sender sends a frame and waits for acknowledgement (ACK) before next frame is sent. If NAK is received alternatively, the previously sent frame is sent again. Besides a NAK or an ACK, the sender may also receive a CANcel (CAN) signal, which aborts the transmission.

Kermit is an extremely flexible protocol (Named after the Frog of sesame street fame); adjusted to support a variety of different packet sizes and error detection methods. It is suited to micro to mainframe connections, but works well with micro to micro or mainframe to mainframe connections.

Synchronous Protocols

Speed of Synchronous transmission gives this advantage over a synchronous transmission especially for LAN, MAN and WAN technology. The types of protocols in this are :

- Character oriented protocols (byte-oriented protocols)
- Bit oriented protocols
- Byte-count protocols

Character oriented protocols interpret a transmission frame or packet as a succession of characters (usually composed of one byte – 8 bits). All control information is in the form of an existing character encoding systems (ASCII characters). Here the frame or packet is interpreted as a series of characters. These protocols are not efficient and are not used much eg. BSC. In a bit oriented protocol, the frame or packet is interpreted as a series of bits.

Character oriented protocols are easy to understand and uses the same logic and organisation as the bit oriented protocols.

Control information is inserted into the data stream in data link protocols either as :

- Separate control frames
- Additions to existing data frames.

The same in the case of character-oriented protocols, it will be in the form of code words taken from existing character sets (ASCII or EBCDIC)

These multi bit characters carry information about:

- Line discipline
- Flow control and
- Error control

Binary synchronous communication (BSC) - Byte oriented protocol

This protocol is primarily a main frame protocol also popular character oriented data link protocol developed of IBM in the period 1964–1967. It is still in use in many organisations who do not have funds to up grade to newer protocols such as SDLC and HDLC. It uses special one byte characters (8 bits) to mark the start and end of the message.

All characters in the message are also 8 bits in length. It supports half duplex transmission using stop and wait ARQ flow control and error correction and usable in both point-to-point as well as in multipoint configurations. It does not support full–duplex transmission or sliding window protocol. It uses a controlled access media access protocol.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

The BSC format will be as under.

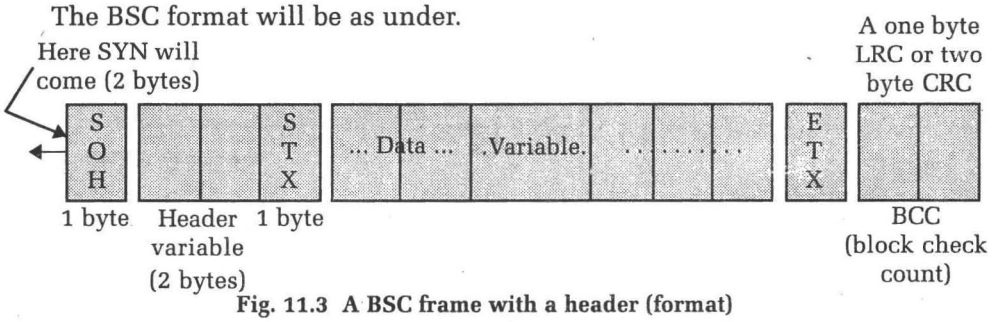


Fig. 11.3 A BSC frame with a header (format)

The message begins with SYN characters which are fixed 8 bit characters. The SOH (start of heading) is again an 8 bit character, which is the start of the message or data packet. It is followed by other header control characters that address the message to a specific device or for other control purposes such as ACK, NCK. The header ranges from one to seven bytes. The header may be one or more bytes defining address and / or other information nonstandardised.

STX, the start of text is another special eight bit character, which is the actual start of the message to be processed by the sender.

ETX is the end of text compresses the text characters so that they can be identified easily. Lastly there is a block character BCC which is a one byte LRC or two byte CRC used for error detection.

As we all know the probability of error occurring depends on the block of text increase (length of the frame). More bits leads to more corruption in transit – greater chances for error – detection becomes difficult. Hence text will be always divided into several convenient blocks. Each block (leaving the last) starts with an STX character, but ends with an ITB known as intermediate text block. Last block starts with STX but ends with ETX (not ITB). After ETX is reached, a BCC field is sent. Thus, the receiver can check each block separately for errors. The detection efficiency is increased. If any block is having an error, the entire frame is to be retransmitted. Otherwise, if OK, receiver sends an acknowledgement for the entire frame. The figure shows the structure of a multi–block frame.

Some of the standard control characters for BSC are shown below :

SYN	Alerts receiver to incoming frame	ACK O	ASCII Code DLE and 0	Good even frame received; ready to receive
STX	Text begins	ACK 1	DLE and 1	Good odd frame received
ENQ	Request for a response	ITB	US	End of Intermediate block
EOT	End of termination	NUL	NULL	Filler character
ETB	End of transmission block	RVI	DLE and <	Urgent message from receiver
ETX	End of text in a message	WACK	DLE and ;	Good frame received, but not ready to receive more
NAK	Bad frame received; nothing to send	TTD	STX and ENQ	Sender in pausing but not relinquishing the line
SOH	Start of heading	Note :	RVI is reverse interrupt WACK is wait and acknowledge	
DLE	Data Transparency Marker			
This is same in ASCII code				

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Problems with BSC

The problems are

- The use of a special character to mark the end of the message ETX. ETX is a pattern of bits like others and is a reserved character. One that is impossible to type on a terminal because no key can generate that bit pattern. Earlier, BSC was designed to transmit only text characters. Today it is used to transmit nontext binary data files, wherein there is a possibility of one of the bytes in the data file has the same bit pattern as ETX. The data byte would be wrongly interpreted as ETX. Receives presumes that the packet has ended losing all the data which follows.
- Transparency problem because the protocol is not transparent. It cannot automatically send all types of data with any bit pattern. BSC's solution to the problem is cumbersome. For transmission of packets with binary data, all control characters (STX, ETX etc) are preceded by a second control character called Data Link Escape (DLE) i.e. 00000100. Any data byte in the binary file that has the same bit pattern as the DLE has a second DLE character stuffed in front of it. If the receiver finds two DLE bytes in a row, it automatically deletes one of them and treats the second DLE as data. The character that follows a DLE is treated as a control character.

BSC Frames

BSC protocol bifurcate the transmission into two types of frames

- Control frames – Strictly for control purposes; to exchange information between communicating devices (to establish the initial connection to control the flow of transmission, to request error corrections, to disconnect the device at the end of a session).
- Data frames – For transmitting information (also contains control information applicable to that information); contains part or all of the message data itself.

A simple data frame format is shown below in figure 11.4

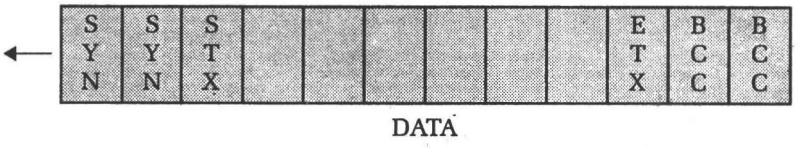


Fig. 11.4 Simple data frame format

(i) The frame begins with SYN (two or more synchronisation characters). These would alert the receiver on the arrival of a new frame and provide a bit pattern used by the receiving device to synchronise its timing with that of the sending device. ASCII code for SYN is 0010110. Two SYN are (0001011000010110).

(ii) Next is STX character which is used to signal to the receiver that the control information is ending. The next byte will be data, consisting of varying numbers of characters.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

(iii) ETX is end of character indicates the transit in between text and more control characters.

(iv) Last is BCC – one or two characters called block check count are included for error detection. A BCC can be one character for LRC or two characters for CRC.

Header fields

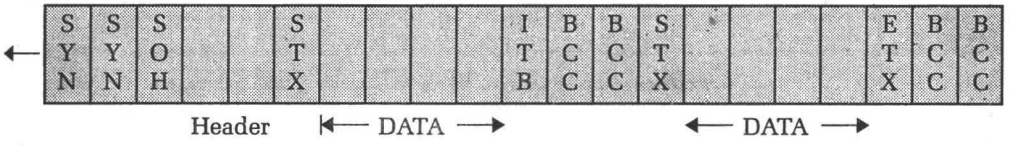
Here address of the receiving device, the address of the sending device, identifying number of the frame (0 or 1) for stop and wait ARQ are included. Header provides the above which begins with SOH (Start of header) character. The header is in between SOH and STX.

Multiframe transmission

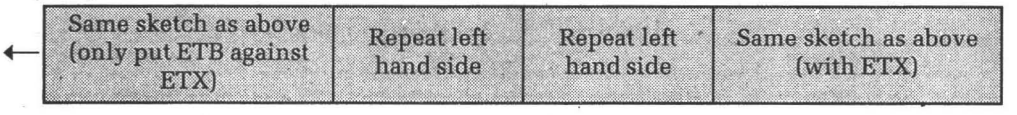
A BSC frame with a header is shown in figure 11.3. Here a single frame carries an entire message. The message is complete at the end of the frame and control of the line passes to the secondary device. In some cases, if the messages are long, it may not fit in to the format of a single frame. Hence the sender splits the message either (i) among blocks (ii) among frames.

Several frames can carry continuations of a single message. At the end of the frame (at the end of transmission) an ETB is put. The receiver acknowledges each frame separately but cannot take over control of the link unless it sees ETX finally.

A Multiblock frame

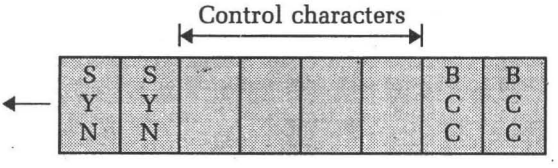


A Multiframe transmission



BSC Control frame

A *control frame* is used by one device to send commands to or solicit information from, another device. It contains control characters but not data. The basic format is as under:



Three purposes of control frames are :

(i) Establishing connections

(ii) Maintaining flow and error control (during data transmission)

(iii) Terminating connections.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Data Transparency

The transparency has already been explained under problems with BSC. Today use would like to send binary sequences that contain nontextual information and commands like programs and graphics. This creates problems for BSC transmission. Confusion between control information and data is called a lack of data transparency. In data transparency, we must be in a position to send any combination bits as data.

Data transparency of BCC is achieved by byte stuffing involving :

- Defining the transparent text region with data link escape (DLE) characters.
- Preceding DLE character within the transparent region by an extra DLE character.

If we insert one DLE character just before the STX character at the beginning of the text field and another before ETX (or ITB or ETB) character at the end of the text field, the first DLE tells the receiver that the text may contain control characters & to ignore them. Second DLE tells the receiver that the transparent region has ended. If the text contains DLE character, problem may arise.

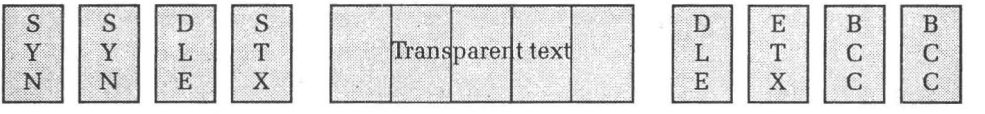


Fig. 11.5 Byte stuffing

11.4 BIT ORIENTED PROTOCOLS

Bit oriented protocol is a protocol where in a frame is seen as a bit stream. Each bit or group of bits have meaning. In character oriented protocols, the frame is interpreted as a series of characters. Here bits are grouped into predefined patterns forming characters. Bit oriented protocols can pack more information into shorter frames and avoid the transparency problem, what has been seen in character-oriented protocols.

In the recent days, many different bit oriented protocols have been developed, all competing for the standard as the most are proprietary designed by manufacturers. (Refer figure 10.6)

SDLC

SDLC is a main frame bit oriented protocol because the control fields and the data do not have to be in 8 bit bytes. Each SDLC frame begins and ends.

With a special bit pattern (01111110) known as the flag. The beginning flag indicates (i) the position of the address (ii) control frame elements and (iii) initiates error checking procedures.

The ending flag terminates the error checking procedures :

The address field identifies the destination.

The control field identifies kind of frame that is being transmitted, either information or supervisory. The information frame is used for the transfer and reception of messages, frame numbering of contiguous frames and the like. The supervisory frame is sued to transmit acknowledgements (ACKs and NCKs). The message field is of variable length containing the users message. The frame check

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

sequence of field is a 16 bit or 32 bit CRC code. SDLC suffers from similar transparency problems like BSC. The binary data to be transmitted may also contain the same bit pattern as the flag, which if not corrected will cause the premature end of the frame and loss of data in the same way as an uncorrected ETX as in BSC. The solution is stuffing an extra DLE into the message. If the sender at any time encounters five 1s in a row in the data to be transmitted, the sender stuffs one extra bit, a 0, into the message and continues to transmit. Similarly, the receiver encounters five 1's and a 0 (111110), the receiver automatically deletes the 0 and continues to process. This technique is called 'bit stuffing' is little more efficient than the character stuffing used by BSC, but is cumbersome.

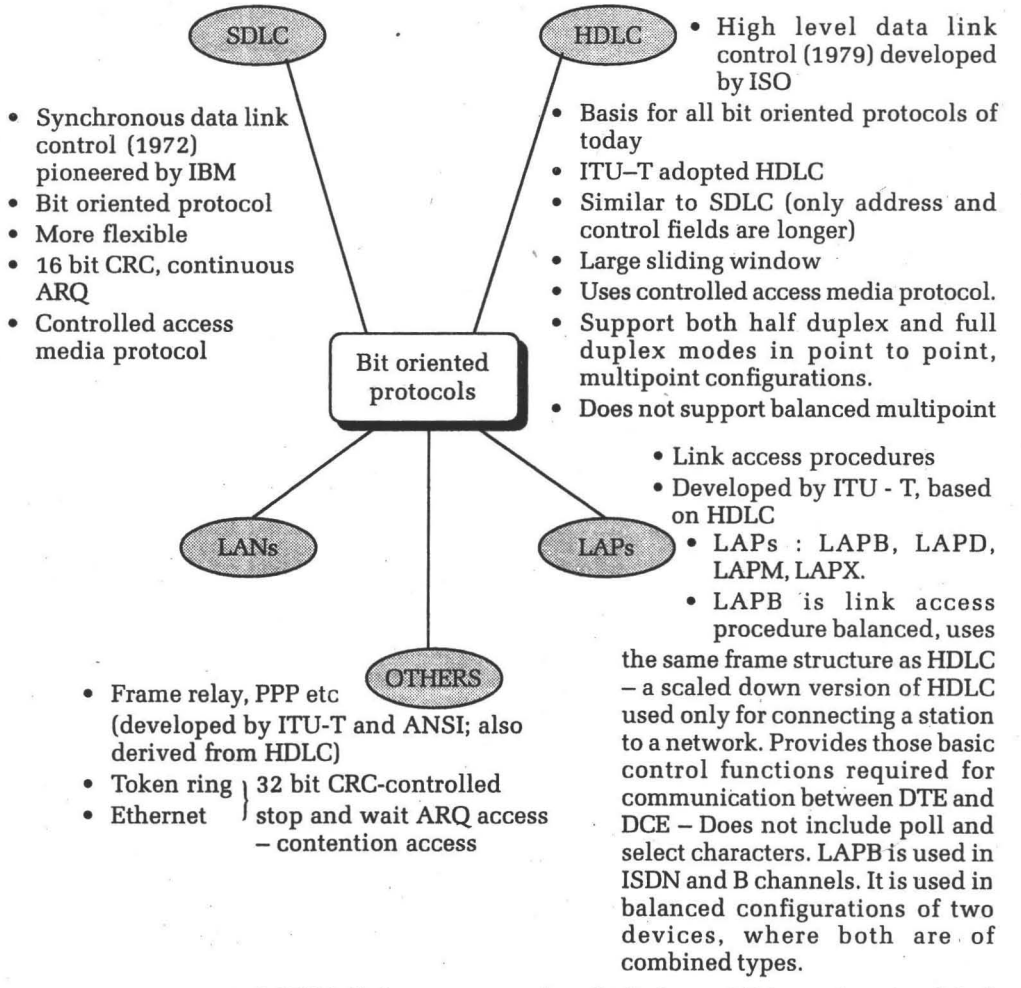


Fig. 11.6 Bit oriented protocols

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

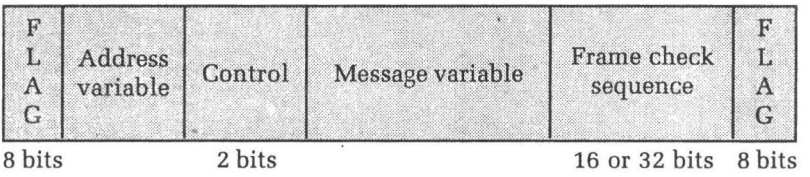


Fig. 11.7 SDLC Format

HDLC

HDLC and its features are already shown in figure .... It differentiates between three different types of stations. Primary, Secondary and Combined.

(i) A primary station sends commands to the secondary eg. Computer to terminal.

(ii) A secondary station issues responses

(iii) A combined station can both command and respond

The hardware devices on a link may be :

(i) Primary (ii) Secondary (iii) Peers

Peer devices can act as both primary and secondary (depending on the mode). Primary, secondary and combined stations can be configured in three ways: Balanced, unbalanced and symmetrical and these can support both half duplex and full duplex transmission.

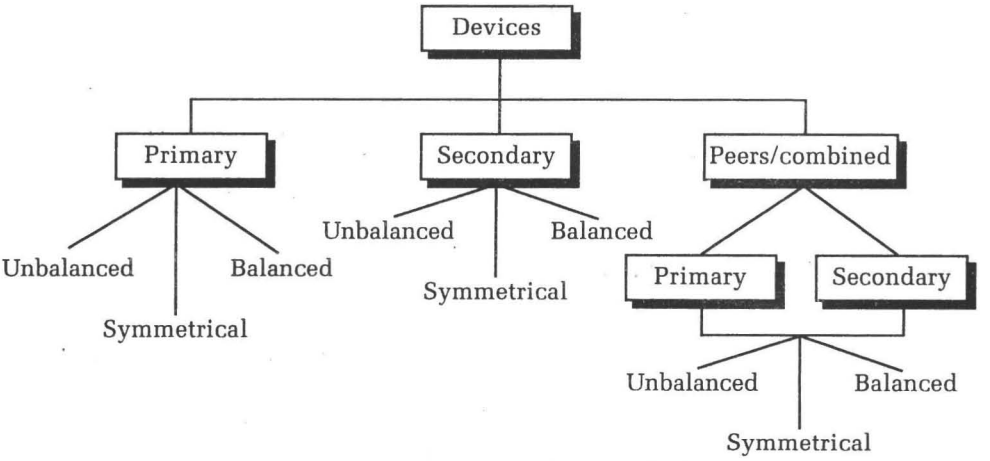


Fig. 11.8 Hardware devices on a link

(i) An *unbalanced* configuration (master/slave configuration) – one device is primary & others are secondary; it can be point to point, if two devices are involved. Many a times, they are multipoint. One computer controlling several peripherals. (eg. one computer and one or more terminals).

(ii) A *symmetrical* configuration is one wherein each physical station on a link consists of two logical stations (one primary and the other secondary). Separate lines link the primary aspect of one physical station to the secondary aspect of another physical station. It behaves like an unbalanced configuration except that control of the link can shift between the two stations.

(iii) A *balanced* configuration wherein the stations are linked by a single line that can be controlled by either station.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

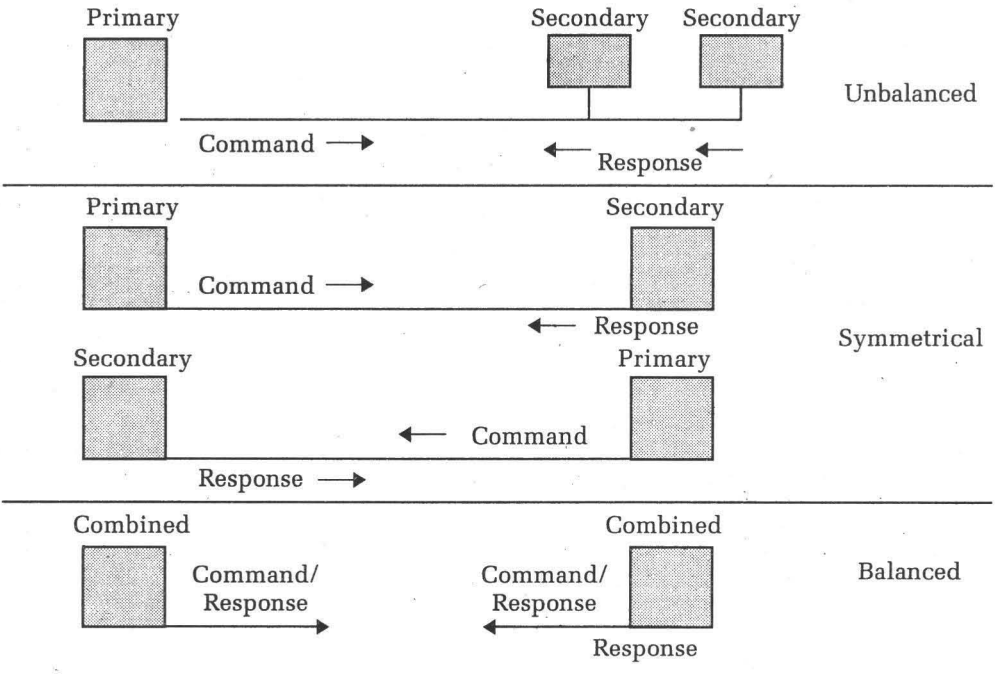


Fig. 11.9 HDLC configurations

Three modes of communications in HDLC are :

- Normal response mode (NRM) – standard primary – secondary relationship
- Asynchronous response mode (ARM) – standard primary – secondary relationship
- Asynchronous balanced mode (ABM) – All stations are equal; combined stations connected in point to point are used.

NRM initiator is primary

ARM initiator is either

ABM initiator is any

HDLC defines three types of frames :

- Information frames (I frames) – To transport user data and control information relating to user data.
- Supervisory frames (S frames) – To transport control information, primarily data link layer flow and error controls.
- Unnumbered frames (U frames) – Referred for system management information carried by U-frame is intended for managing the link itself.

Total 6 fields (Flag (bit pattern is 01111110) Six ones enclosed in two 0s The ending flag of 1 frame can be used as the beginning flag of the next frame.

Flag	Address	Control	Information	FCS	Flag
8-bit			I - Frame		8-bit

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Flag	Address	Control	FCS	Flag

S - Frame

Management information used for managing the network (may or may not be present).

Flag	Address	Control	Information	FCS	Flag

U - Frame

Flag field

The flag field may pose potential cause of transparency problems in HDLC. When a station finds a flag on the line, it determines that the frame is addressed to it and begins reading the transmission. It would watch for the next flag that signifies the end of the frame. In a bit sequence, control information or data might contain the pattern 01111110. If this happens, the receiver finds it and assume that the end of the frame had been reached resulting in disastrous results.

HDLC also to overcome this uses a process called *bit stuffing*. Every time a sender wants to transmit a bit sequence of more than five consecutive 1s, it stuffs one redundant 0 after the fifth one. The sequence 0111110 becomes 011111010, irrespective of the sixth bit whether there is another 1 or not. This would tell the receiver that it is not a flag. Once the receiver comes to know that it is a stuffed 0, it is dropped from the data to retain the original bit stream.

Under three exceptions, bit stuffing is required. These are :

- Bit sequence is really a flat
- The transmission is being aborted (14 consecutive 1s)
- Channel is being put into idle (15 or more 1s)

Address field

Flag	Address	Control	Information	FCS	Flag

- Address is one byte (8 bits) or a multiple of bytes depending on the needs of the network. One byte can identify upto 128 stations.

						1

One byte address will always have 1 at the right end

- Second field
- Contains the address of the secondary station which is either the originator or destination of the frame (to or from address)

						0						0						1

In multibyte address, all bytes will end with 0 except the last one (which is 1)

Control field

It is a one or two byte segment of the frame used for flow management it differ depending on the type of the frame. If the first bit of the control field is 0, the frame is an I frame, First and second bits are 1 and 0 respectively then it is an S frame. If both first and second bits are 1s it is a U-Frame. The control fields of all three types of frames will have a bit called the poll/final (P/F) bit.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

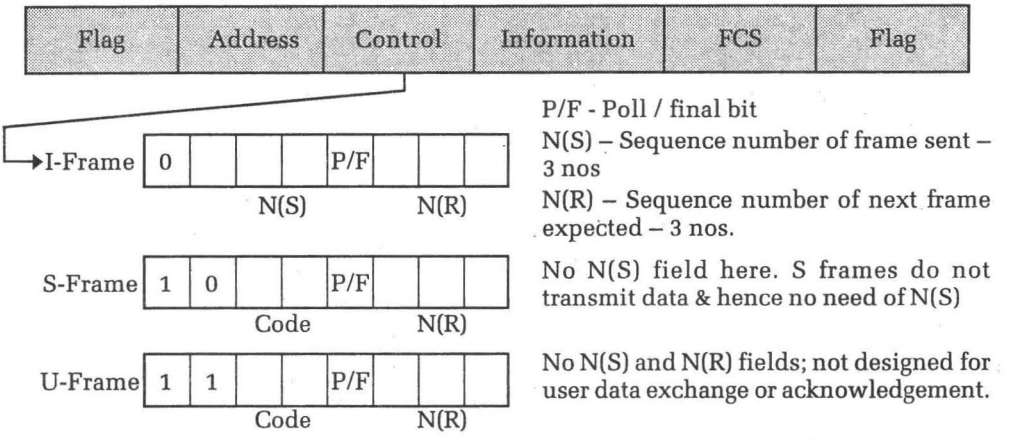


Fig. 11.10 HDRC control fields

In I frame, N(S) and N(R) both 3 bit flow flank the P/F bit.

N(S) specifies the number of the frame being sent

N(R) indicate the number of the frame expected in return in a two way exchange.

It is the acknowledgement field. If the last frame received was error free, the N(R) number will be that of the next frame in the sequence. If the last frame was with error, the N(R) number will be the number of the damaged frame, indicating the need for its retransmission.

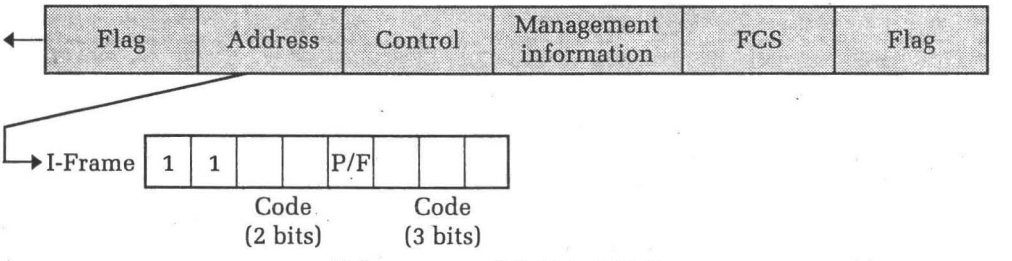
In S-Frame

No N(S) here. The two bits preceding the P/F bit are used to carry coded flow and error control information. S frames are used to return N (R) when the received does not have data of its own to send. Otherwise, the acknowledgement is contained in the control field of an I frame.

In U-Frame

U frame have two code fields (one with 2 bits and other with 3 bits) flanking the P/F bit. These codes are used to recognise the U Frame and its function.

If the control field is of two bytes long instead of one, the modes (extended) are called NRME, ARME and ABME instead of NRM, ARM and ABM.



U-frame control field in HDLC

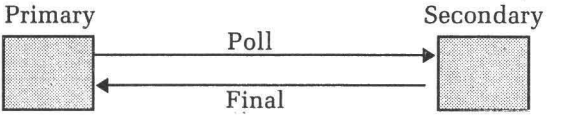
P/F field

It is a single bit with double purpose and can mean poll or final. It means poll when the frame is sent by primary station to secondary. Otherwise, final (when the address field contain the address of the sender)

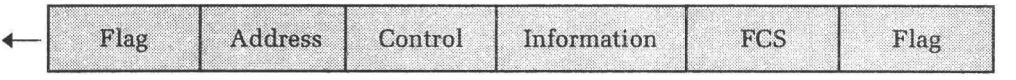
Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Information field



It is user's data in I frame and network management information in a U frame. It does not exist in S frame. The length can vary from one network to another but is fixed within each network.



It is possible to include flow, error and other control information in an I frame that contains data. In either half or full duplex (two way exchange of data), station 2 can acknowledge receipt of data from station 1 in the control field of its own data frame instead of sending a separate frame only for acknowledgement. Thus, combining data to be sent with control information is called *piggy-backing*. *Piggy-backing* is combining data to be sent and acknowledgement of the frame received in one single frame.

The frame check sequence (FSC) is HDLC's error detection field, which can be of a two or 4 byte CRC.

The comparison of three frames I, S & U are given below.

I-Frame	S-Frame	U-Frame
• Designed for user information transport, piggy backed acknowledgements. • Range of variation in I frames small • Contains two 3 bit flow and error control sequences called N(S) & N(R) flanking the P/F bit no codes. • All differences relate either to the data (content & CRC) Identifying number of the frame, or to the acknowledgement of received frames (ACK or NAK) • The details of I frame are already explained (regarding all fields)	• Contain subfields within their control fields which carry codes that alter the meaning of the frame. • Do not contain N(S) field. Contains N(R) field P/F bit is in between 2 bit code and 3 bit N/R. • S frame coded for selective reject (SREJ) cannot be used like S frame coded for receive ready (RR). • Used for acknowledgement, flow control and error control whenever piggy backing that information on to an I frame is impossible / inappropriate • Do not have information fields (yet each one carries message to the receiving station based on the type of S - Frame and the context of the transmission). • The type of S frame is determined by a two bit	• Same as S frame (Sub fields) • Unnumbered frames are used to exchange session management and control information between connected devices. • U frame contains an information field, unlike S frame, but one used for system management information not user data. • Much of the information carried by US frames is contained in codes included in the control field. • U frame codes are decided into 2 sections. a 2 - bit before P/F bit and 3-bit after the P/F bit. These 5 bits can create upto 32 different U frame times. • The commands and responses can be divided into five basic categories – Mode setting – Unnumbered exchange – Disconnection – Initialisation – Miscellaneous • SNRM – Set normal response mode SNRME – Set normal response mode (Extended) SNRM – Set asynchronous response mode

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

	code sent into its control field before P/F bit. Four types of S frames: Code Command 00 RR (Receive ready) 01 REJ (Reject) 10 RNR (Receive not ready) 11 SREJ (Selective - Reject)	SNRME – Set asynchronous response mode (Extended) SABM – Set asynchronous balance mode SABME – —"— (Extended) UP – Unnumbered pole information UI – Unnumbered information UA – Unnumbered acknowledgement DISC – Disconnect mode DM – Disconnect mode RD – Request disconnect RIM – Request information mode SIM – Set initialisation mode RSET – Reset

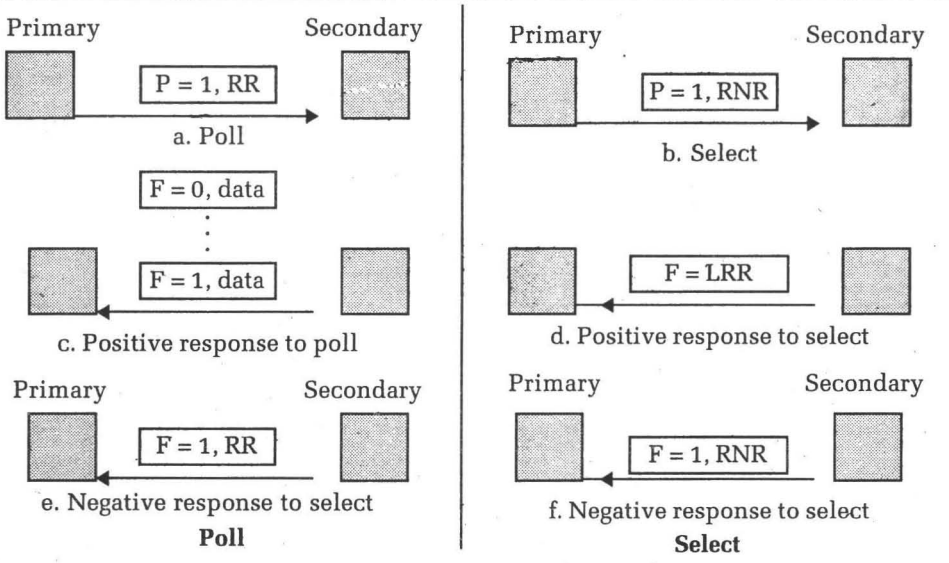


Fig. 11.11 P/F bits in polling and selecting

Mode-setting in U-Frame

These are sent by the primary or combined stations using to control an exchange to establish the mode of the session. A mode setting U frame tells the receiving station what format the transmission would take. If temporary primary to secondary relationship is to be established it contains code 00001 (Normal response mode). The addressed station understands and adjusts itself accordingly. The table of codes & Commands are given below.

Code	Command	Code	Command
00 001	SNRM	00 000	UI
11 011	SNRME	00 010	DISC
11 000	SARM	10 000	SIM
11 010	SARME	00 100	UP
11 100	SABM	11 001	RSET
11 110	SABME	11 101	XID
		00 110	UA

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Unnumbered exchange codes are used to send specific pieces of data link information between devices. The numbered poll (UP) code is 00 100 is transmitted by primary station or a combined station (acting as primary) on a link to establish the send / receive status of the addressed station. The unnumbered information UI code (00 000) is used for transmission of specific pieces of information such as time/date for synchronisation UI frame can be sent as commands or as responses. The unnumbered acknowledgement UA code (00 110) is returned by the addressed station is replied to an UP to acknowledge one of the unnumbered request frames.

Disconnecting codes

Three disconnect codes are :

- from the acting primary/ combined station
  - Disconnect (DISC 00110) is sent by first to the 2nd station to terminate the connection.
- two responses from the receiving station
  - (i) Request disconnect (R 00010) by the second station to the first that a DISC be issued.
  - (ii) Disconnect mode (DM 11000) by the addressed station to the initiating station as a negative response to a mode setting command.

Initialisation mode 2

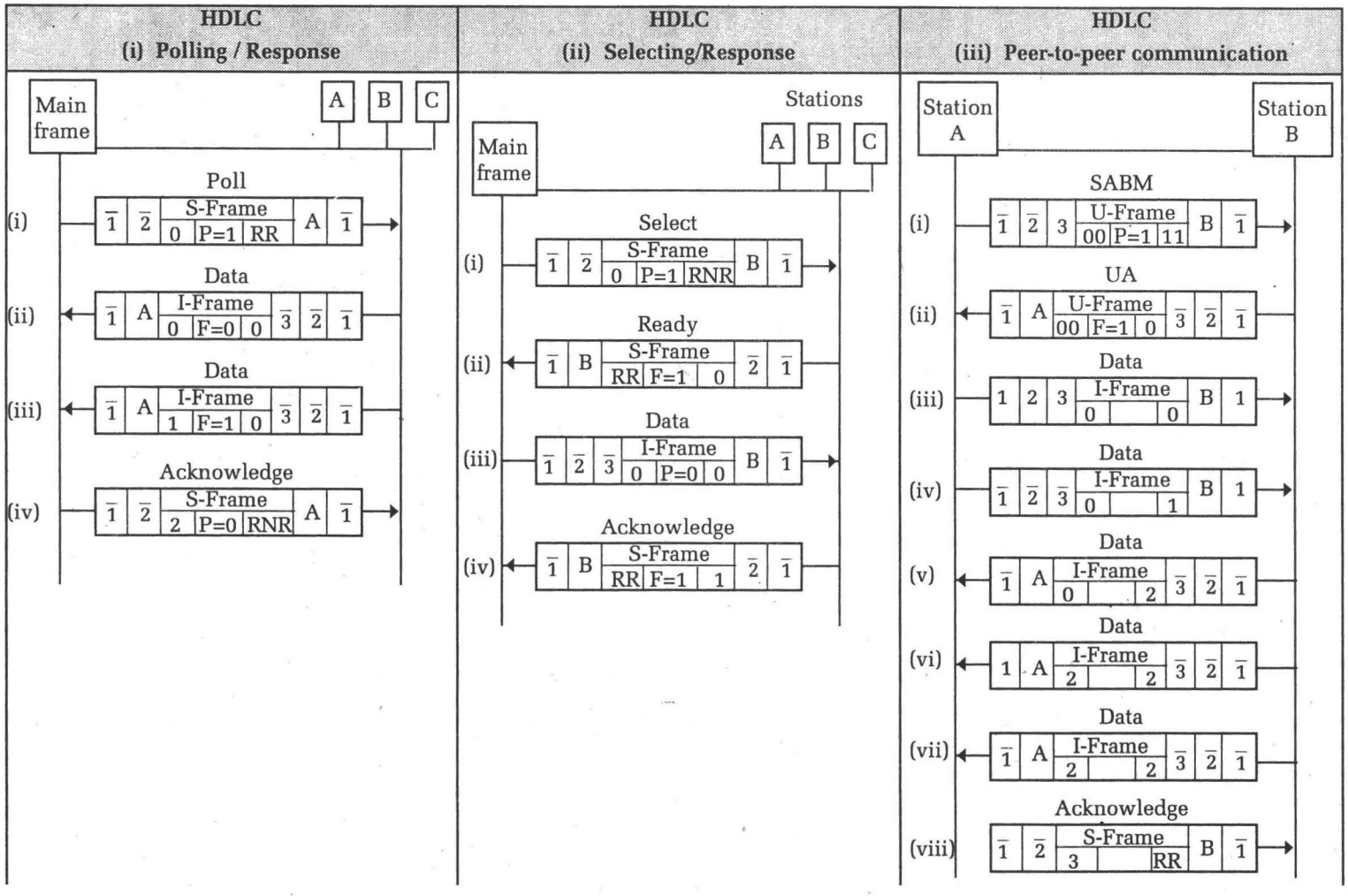
SIM i.e. set initialisation mode (code 10 000) is used as a command. It prepares the addressed station to initialise its data link control functions. SIM command is followed by UI frames (contains a new frame or a new parameter set). Same code 10 000 is used as a response (second to the first system), means request initialisation mode (RIM) and solicits a SIM command for the first station. It is used to respond to a mode setting command when a second station cannot act upon the command without receiving SIM.

The last three commands are :

R SET (11 001) XID (11 101) (Exchange ID)	From the initiating system to the addressed system in both RSET and XID. RSET informs second station that the first station is resetting its send sequence numbering and instructs to do the same or like wise (like all issued in response to an FRMR). XID requests an exchange of identifying data from the 2nd station (Address?)
FRMR (10 001) (Frame Reject)	Tells the first system that a U frame received by the second system contains a syntax error.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.



Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

(i) The primary device (mainframe) on a multipoint link polls the secondary device with an S - Frame containing the codes for poll

Firs is flag field

Second is address of the secondary being polled

Third is code identifying the frame (P/F bit set to poll) NR = 0 field; fourth is FCS; Fifth is flag

(ii) (iii) and (iv)

Station A has data to send. It responds with two I - frames numbered F = 0 and F= 1. The second has the P/F bit for final to indicate the end of data. The primary acknowledges both frames at once with an S - Frame containing the number 2 in its N(R) field to tell station A that frames 0 & 1 has been received.

Abbreviations used :

$\overline{1}$ is the Flag

A is the address

RR is receive ready

$\overline{2}$ is FCS error detection code

UA unnumbered acknowledgement

$\overline{3}$ is Data

SABM – Set asynchronised balance mode.

RNR – Receive not ready

(i) & (ii)

The same multipoint configuration using primary device and selecting station B in the secondary device to receive a transmission is shown

The primary sends out an S - Frame to B that contains the codes for select. The select frame is identical to the poll frame except RR is RNR. Station B responds with another S Frame addressed from B, that contains the code for RR as well as the final bit set, to indicate that the station is ready to receive and that this frame is the last.

(iii) Primary sends an I-frame containing its data. The frame is addressed to B, the N(S) field identifies it as frame number 0, to P-bit is not sent to indicate that the frame is not a poll and the N/R field indicates that if an I frame is returned, it is expected also to be number 0.

(iv) Station B responds with an RR frame (a) the set final bit tells the primary that B does not have anything to send and (b) 1 in the N(R) field acknowledges the receipt of frame 0 and indicates that B next expects to receive frame 1.

An exchange in asynchronous balanced mode (ABM) using piggy band acknowledgements. Two stations A and B are of equal status (connected by a point to point link) – peer to peer.

(i) Station A issues a U-frame code for SABM to establish link. The P-bit is set to indicate that station A expects to control the session and to transmit first.

(ii) Station B accepts the request by returning the code for UA with the F bit set. The P/F bit can be ignored in the frames that follow because of peer to peer type.

(iii) & (iv) Station A beings the exchange of information with an I frame numbered 1. Station B piggy backs its acknowledgement of both frames onto an I frame of its own.

(v) Station B's first I frame is numbered (0) in N(S) field and contain a (2) in its N(R) field, acknowledging the receipt of A'S frames 1 and 0 and indicating that it expects frame 2 to arrive next.

(vi) & (vii) Station B transmits its second and third I frames (numbers 1 & 2) before accepting further frames from station A. Its N(R) information has not changed. B frames 1 & 2 indicate that station B is still expecting A frame 2 to arrive next.

(viii) Station a has sent all its data. It cannot piggy back an acknowledgement on to an I frame and sends as S frame. The RR code indicates that A is still ready to receive. The number 3 in the N(R) field tells B that frames 0, 1 & 2 have all been accepted and A is now expecting frame 3.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

POINTS TO REMEMBER

- Protocol is rules for communication. A protocol in data communications is set of rules or specifications for implementing one or more layers of the OSI model.
- The two categories of data link protocols are (i) Asynchronous and Synchronous.
- Asynchronous protocols are X MODEM, Y MODEM, Z MODEM, BLAST, Kermit, and others. Asynchronous transmission is referred to as start – stop transmission and used on point to point full duplex circuits.
- The types of synchronous protocols are :
  - Character oriented protocols (byte – oriented protocols)
  - Bit oriented protocols
  - Byte-count protocols
- Character oriented protocols interpret a transmission frame or packet as a succession of characters. In bit oriented protocols, each bit or groups of bits can have meaning.
- Binary synchronous communication (BSC) – Byte oriented protocol is the most well known character oriented protocol developed by IBM. It operates in half duplex mode with stop and wait ARQ in a point to point or multipoint configuration. Two types of BSC frames are control frames and data frames.
- Three purposes of BSC control frames are : Establishing connections, maintaining flow and error control, terminating connections.
- The problems with BSC are the use of the special character to mark the end of the message ETX. BSC was originally designed to transmit only text characters. Today, it is used to transmit non – text binary data file wherein there is a possibility of one of the bytes in the data file has the same bit pattern as ETX. Transparency problem exists because the protocol is not transparent. It is the ability to send any bit pattern as data without it being mistaken for control bits. A bit pattern that resembles a BSC control character in the data field must not be recognised as a control character; it must be made transparent. Data transparency is achieved by a process called byte stuffing.
- Any data byte in the binary file that has the same bit pattern as the control character as the data link escape (DLE) has a second DLE character stuffed in front of it. If the receiver finds two DLE in a row, it automatically deletes one of them and treats the second DLE as data. Byte stuffing includes : Demarcation of the transparent region, Addition of DLE (in the transparent region) before every DLE character.
- Most of the bit oriented protocols are generally coming under HDLC high level data link control. Bit oriented protocol is a protocol where in a frame is seen as a bit stream and each bit or group of bits have meaning.
- Bit oriented protocols have the following popular types : SDLC – Synchronous data link control developed by IBM in 1972, HDLC – High level data link

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

control developed by ISO in 1979. It supports both half duplex and full duplex modes in point to point multipoint configurations – It is a versatile and a very popular protocol.

LAP Link access procedures developed by ITU–T ; Its constituents are LAPB, LAPD, LAPM, LAPX. Others are frame relay, ppp etc developed by ITU – T and ANSI.

- HDLC stations are categorised as (i) primary station (sends commands), secondary station (sends responses); combined station (sends commands and responses). HDLC are configured as 3 types (i) Unbalanced (one primary – one or more secondaries) (ii) symmetrical (two physical stations – each capable of switching from primary to secondary) (iii) Balanced – two combined stations, each of equal stations.
- HDLC stations communicate in 3 modes : Normal response mode (NRM) – Asynchronous response mode (ARM), Asynchronous balanced mode (Secondary station needs permission, does not need permission to transmit, combined stations may initiate transmission respectively). HDLC defines three types of frames : Information frame (for data transmission and control), supervisory frame (S-Frame purely for control), unnumbered frame (U–Frame for control and management)
- HDLC handles data transparency by adding one zero whenever these are the consecutive 1s following a 0, which is known as bit stuffing.

QUESTIONS

1. What do you mean by protocol?
2. What are the two categories of data link protocol?
3. Explain Asynchronous protocol.
4. Explain synchronous protocol. Which are the two groups coming under it?
5. What are the different types of Asynchronous protocol ? Briefly explain them?
6. What do you mean by Binary Synchronous communication (BSC)?
7. What are the different problems with BSC?
8. What are the two types of BSC frames ?
9. Which is the most important character oriented protocol?
10. What is data transparency in BSC?
11. When would a DLE pattern occur in BSC?
12. Compare and contrast HDLC I –Frame, HDLC U–Frame and HDLC S–Frame.
13. Explain BSC control frame. What are the functions of control frames?
14. What do you mean by bit oriented protocols? What are the categories under this?
15. What is byte stuffing? Give an example.
16. Compare and contrast SDLC with HDLC.
17. What is Piggy backing?

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

18. Explain HDLC. What are the categories of HDLC stations?
19. What is the configuration and modes of HDLC?
20. What are the three different types of frames defined in HDFC protocol?
21. What are LAPs? What are the different categories coming under LAPs?
22. Write down all the HDFC configurations and modes with the help of figures.
23. Write down the sketches for polling, selecting, peer to peer communication using HDLC and explain.
24. What is the expansion of DLE, ETX, SYN, ACK, NAK, WACK, BSC, SDLC, HDLC, FCS, LAPB, LAPD, LAPM, RR, RNR, SIM, SNRM, SNRME, SARM, SARME, SABM, SABME, RIM?

FILL IN THE BLANKS

1. _____ means rules for communication.
2. Two categories of _____ _____ protocol are Asynchronous and Synchronous.
3. Asynchronous transmission is referred to as _____ transmission.
4. BSC stands for _____ _____ _____.
5. HDLC _____ field defined the beginning and end of a frame.
6. BSC is a _____ _____ protocol.
7. _____ is supports both half duplex and full duplex modes in point to point, multipoint configurations.
8. HDLC is known as _____ _____ _____ _____ _____.
9. In BSC protocol _____ terminates a transaction.
10. BSC frames are of two types _____ frames and data frames.
11. A negative response in BSC for select is _____.
12. ____ Frame do not transmit data and hence no need of N(S).
13. When data and acknowledgement are sent on the same frame it is known as _____.
14. HDLC protocol's shortest frame is usually _____ frame.
15. BSC protocol uses _____ _____ mode.
16. BSC protocol a _____ field follows after ETB, ETX or ITB.
17. HDLC ____ frames are to transport user data and control information relating to user data.
18. HDLC ____ frames are to transport control information.
19. HDLC ____ frame is reserved for system management information.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

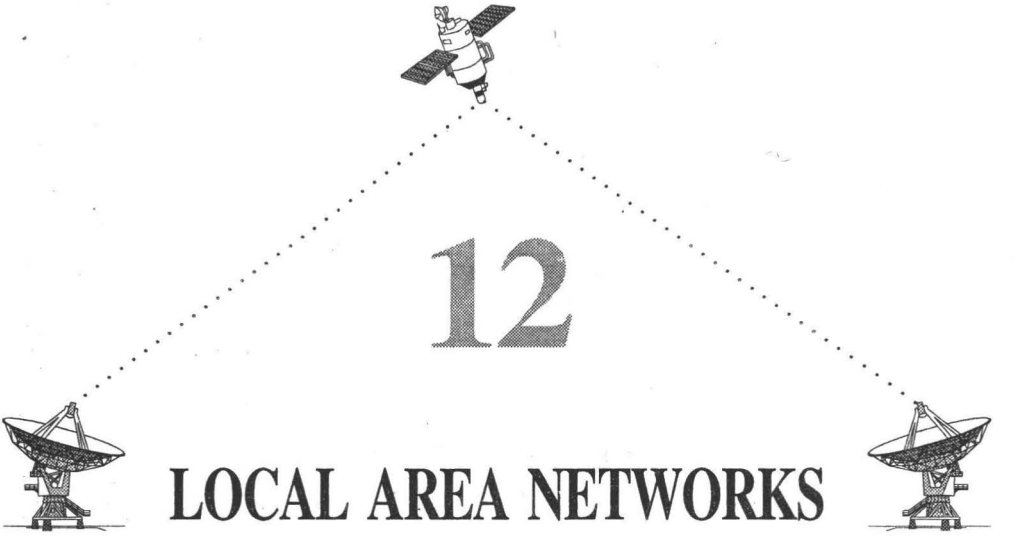
20. _____ _____ is carried out in bit oriented protocol, an extra bit 0 is added to achieve data transparency.
21. _____ _____ is carried out in character oriented protocols, an additional control character (s) is added to achieve data transparency.
22. All HDLC control fields have _____ _____.

Answers

1. Protocol
2. data link
3. start-stop
4. binary synchronous communication
5. Flag
6. character oriented
7. HDLC
8. high level data link control
9. EOT
10. control
11. NAK
12. S
13. piggy-backing
14. supervisory
15. half duplex
16. BCC
17. I
18. S
19. U
20. Bit stuffing
21. Byte stuffing
22. P/F bit

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.



12

LOCAL AREA NETWORKS

Local area network links the computers into a network that provide the standard office functions like :

- Word processing
- File transfer
- Electronic mail
- Printer sharing
- File sharing
- Internet access

It is a data communication system with a network communicating devices inside a single building or inside buildings close to each other. Large organisations have numerous LANs connected by backbone networks.

These LANs provide access to organisations host main frame computers. We shall now deal with certain fundamentals of LAN and types of LAN.

LANs are developed for two purposes :

- Information sharing – Users access the same data files, exchange information via electronic mail or search the Internet for information. Benefit is for improved decision making.
- Resource sharing – One computer sharing a hardware device (printer etc) or software package with other computers on the network to save costs.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

LANs are having four architectures :

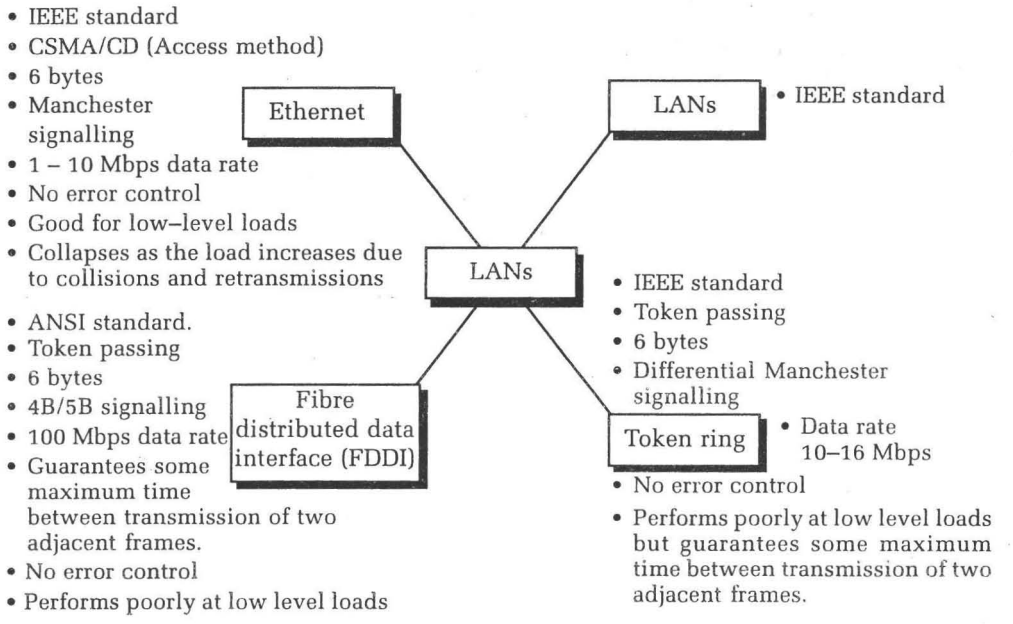


Fig. 12.1 Architecture of LAN and comparison

There are many ways to classify LANs. One way is

- Dedicated server LANs (Accounts for nearly 70% of all installed LANs)
- Peer to Peer LANs (Many issues are common with dedicated server LANs)
- Zero slot LANs.

A dedicated server, LAN connects with almost any other network, can handle very large data bases, has a dedicated network server and uses sophisticated LAN software. The different types of dedicated server LANs are : file servers, database servers, Print servers and Communication servers. With dedicated server LANs, the network has one or more computers, supporting the network by providing access to the files and other network resources.

Peer-to-peer network do not require a dedicated server. Any computer can function as both a user and server, share its hard disk and printer with any other computer on the run work. All the computers run special network software, enabling to run as a client and as a server. Peer to peer network is slower with less capability, supports a more limited number of computers, provides less sophisticated software, more appropriate in having resources in smaller LANs as compared to dedicated server networks. E.g. Artisofts' LANtastic, Novell's Netware lite and windows for work groups.

Zero slot LANs have the lowest level of capability for a LAN, inexpensive. Zero slot LAN, so called because they do not need a network interface circuit card, provides limited capabilities such as file transfer, file sharing, printer sharing and e-mail. The zero slot LAN adapter plug can be plugged into a serial or parallel port instead of taking up on of the computer's expansion slots. It costs 1/10 to 1/2 of the amount of more powerful dedicated server LANs.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Project 802

IEEE developed a project 802 by its computer society in 1985. It covers the first two layers of the OSI model and also a portion of the third layer (physical layer, data link layer - full and a part of the network layer to the extent of allowing interconnectivity of major LAN protocols. Project 802 is to set standards to enable intercommunication between equipment from a variety of manufacturers. IEEE has divided the data link layer into two sub layers LLC and MAC as shown below.

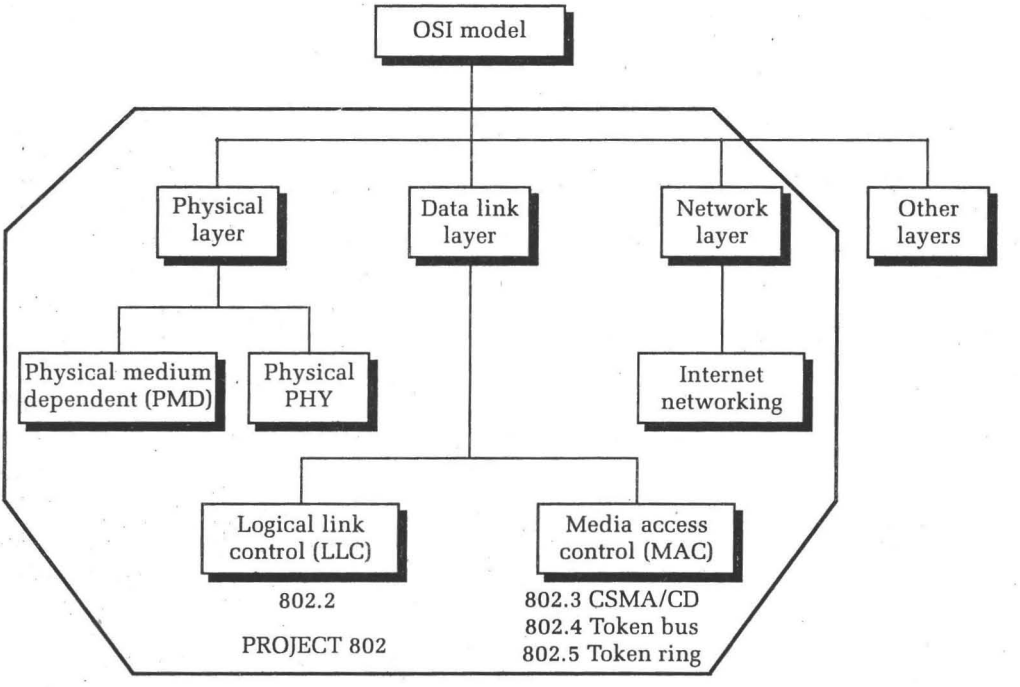


Fig. 12.2 OSI model

In addition to two sub layers LLC & MAC, project 802 contains a section governing internet working (assuring the compatibility of different LANs and MANs across protocols and allows data to be exchanged across otherwise incompatible networks.

Project 802 works on the strength of modularity. The functions required by LAN management has been subdivided and the designers have standardised of those that can be generalised and to isolate special ones. Each sub division is identified by a number e.g. Internet working 802.1, LLC, 802.2 etc.

IEEE 802.1

It is a subdivision of project 802 devoted exclusively to internet working issues in LANs and MANs. It seeks to resolve the incompatabilities between network architectures, without needing modifications in addressing, accessing, and error recovery mechanisms. It is an internet working standard for LANs.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Logical link control (LLC)

Protocol 802.2 and Media Access Control (MAC(802.3 to 802.5)

IEEE Project 802 model takes the structure of an HDLC frame and divides it into two sets of functions; one set contains end user portions of the frame (logical addresses, control information and data) handled by logical link control protocol. LLC is the upper layer of the IEEE 802 data - link layer and is common to all LAN protocols. The second set of functions, the MAC sub layer resolves the continuation of the shared media, containing :

- Synchronisation
- Flag
- Flow
- Error control specifications

(to move information from one place to another)

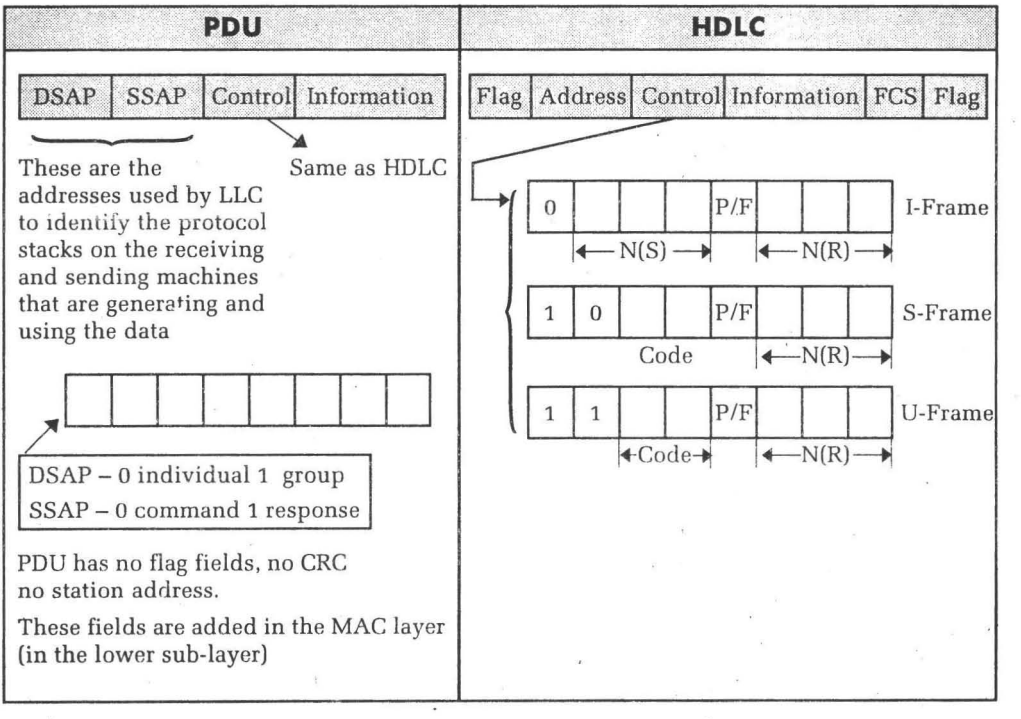
- Physical address of the next station

(to receive and to route a packet MAC are specific to the LAN using them and forms the lower sub layer of the data link layer (Ethernet, token ring, token bus etc.))

Protocol data unit (PDU) format

The data unit in the LLC level is known as protocol data unit (PDU)

PDU contains
- DSAP (Destination service access point)
- SSAP (Source service access point)
- A control field
- Information



Copyright © 2009. Global Media. All rights reserved.

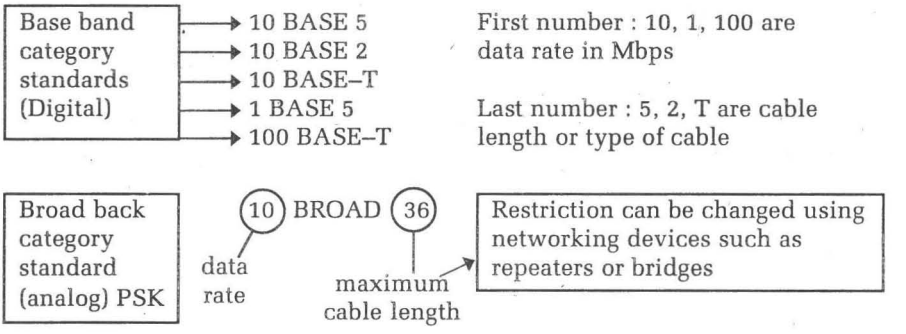
Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Ethernet

It is a local area network using CSMA/CD access method. IEEE 802.3 supports a LAN standard (developed first by Xerox, extended by a joint venture between DEC, Intel and Xerox. This is known as *Ethernet*. There are many different types of ethernet, classified either as *base band* or *broad band*.

Base specifies a digital signalling (Manchester encoding). It treats the cable as one single channel and carry only a single transmission at any one moment.

Brand specifies a analog signalling (PSK encoding). It splits the cable into many channels (using frequent division multiplexing) so more than one transmission can occupy the LAN cable at the same time. We can intermix voice, data and image signals on the same network. It is less complex, less expensive (does not need modulation devices) built in the NICs.



The original ethernet specification was a 10 Mbps data rate using and signalling on thin coaxial cable, called 10 base 5 or thick ethernet.

10 Base 5 – Thick ethernet or Thick net.

10 Base 2 – Thin coaxial cable today rapidly replacing the original thick coax. Easier to work with (though it is limited to 185 meters between hubs) hence known as *thin ethernet or cheaper net*.

1 Base 5 – (1 Mbps to a maximum distance of 500 meters using star topology) called Star lan after the AT&T product that introduced it. Rarely used because of its low data transmission rate.

10 Base T – Most commonly used type of Ethernet (10 Mbps, base band) T means it uses twisted pair wiring unshielded. This revolutionised Ethernet and made it most popular type of LAN in the world. Extremely low cost to its foremost competitor IEEE 802.5 Token ring.

10 Broad 36 – Broad based Ethernet (10 Mbps, broad band, 3600 meters most commonly used in the backbone networks.

100 Mbps ethernet, transmission is also available.

Access Method : CSMA/CD

Carrier sense multiple access with collision detection 802.3.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Collisions occur whenever overlaps occur which make the signal into unusable noise. Such signals overlap occur whenever multiple users have unregulated access to a signal line. Signals overlap destroy each other. As traffic increases on a multiple access link, so do collisions. In order to coordinate traffic and minimise the number of collisions that take place and to maximise the number of frames that are developed successfully, a LAN needs a mechanism. The access mechanism used in an Ethernet is called *carrier sense multiple access with collision detection (CSMA/CD).* standardised in IEEE 802.3. Originally the design started with a multiple access (MA) method in which every work station had equal access to a link. Here there was no provision for traffic coordination and access to the line was open to any node at any time. The assumption was that the odds of two devices competing for access at the same time were small enough to be unimportant.

CSMA carrier sense multiple access was the development from MA. CSMA/CD is the result of an evolution from CSMA and uses a contention based media access control technique.

In CSMA system, any work station wishing to transmit must first listen for existing traffic on that line. A device listens by checking for a voltage if it is not detected, the line is taken for granted as idle and transmitter starts. CSMA cuts down on the number of collisions but cannot eliminate all. If another station has transmitted recently for its signal to have reached the listening station, the listener assumes the line is idle and introduces its own signal onto the line.

If two computers are on the same circuit, it is necessary to control their access to the media. E.g. If two computers on the same circuit transmit at the same time, their transmissions are garbled. Such collisions must be prevented. If they are permitted to occur, there must be a way to recover from them which is known as *media access control.*

Ethernet's CSMA/CD protocol is very simple in concept; waits until the bus is free and then transmits. Computers wait until no other devices are transmitting and then transmit their data.

CSMA/CD protocol is termed as ordered chaos. As long as no other computer attempts to transmit at the same time, everything is fine. If two computers located at some distance from each other can both listen to the circuit and finds empty and begin to transmit simultaneously. This is called a *collision*. The two messages then collide and destroy each other. The solution is to listen while transmitting, better known as *collision detection* (CD). In CSMA/CD the station wishing to transmit first listens to make certain the link is free, then transmit its data, then listens again. During the data transmission also, the station checks the line for the extremely high voltages that indicate a collision. Once collision is detected, the station waits a predetermined amount of time for the line to clear, then sends its data again. Chances are both computers will choose a different random amount of time and one will begin to transmit before the other.

NIC

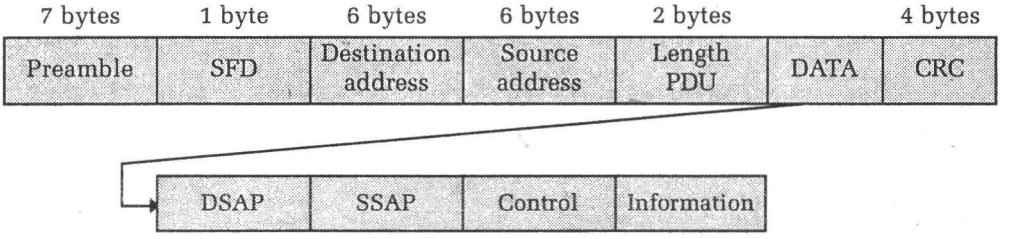
NIC is network interface card and each stations on an Ethernet work has its own NIC. This usually fits inside the station and provides the station with a six byte physical address. The number on the NIC is unique Ethernet LANs can support data between 1 and 100 Mbps.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Format of the MAC frame in CSMA/CD

The frame specified by IEEE 802.3 contains 7 fields



Ethernet do not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgements are implemented at the higher layers.

Preamble –

- First field of 802.3 frame with seven bytes (7 X 8 = 56 bits) of alternating 0s and 1s (alerts the receiving system to the coming frame, and enable it to synchronise its input timing).
- Pattern 1010101 provides an alert and timing pulse.
- HDLC combined the alert, timing and start synchronisation into a single field. IEEE 802.3 divides these three functions between the preamble and the second field, the start frame delimiter (SFD).

SFD –

- Second field; one byte 10101011 of the 802.3 frame signals the beginning of the frame.
- It tells the receiver that everything follows is data, starting with the addresses.

Destination address (DA) –

- Field is allotted six bytes; contains the physical address of the packets next destination.
- Physical address is a bit pattern encoded on its, network interface card (NIC). Every NIC has a unique address that distinguishes from other NICs.
- DA field contains the physical address of the router connecting the current LAN to the next one if the packet must cross frame one LAN to another to reach the destination; also to make the packet to reach the target network. DA field contains the physical address of the destination device.

Source address –

- As shown above, it is allotted 6 bytes and contains the physical address of the last device to forward the packet. The device can be the sending station or the most recent router to receive/forward the packet.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

PDU length/type –
- 2 bytes indicating the number of bytes in the coming PDU.
- Field can be used to indicate type or as a base for other protocols if the length is fixed eg. Novell and Internet use it to identify the network layer protocol.

802.2 frame (PDU)–
- It contains the entire 802.2 frame as a modular removable unit.
- 46 to 1500 bytes long (depends on the type of frame and length of information field)
- Generated by the upper LLC sub layer (and linked to the 802.3 frame)

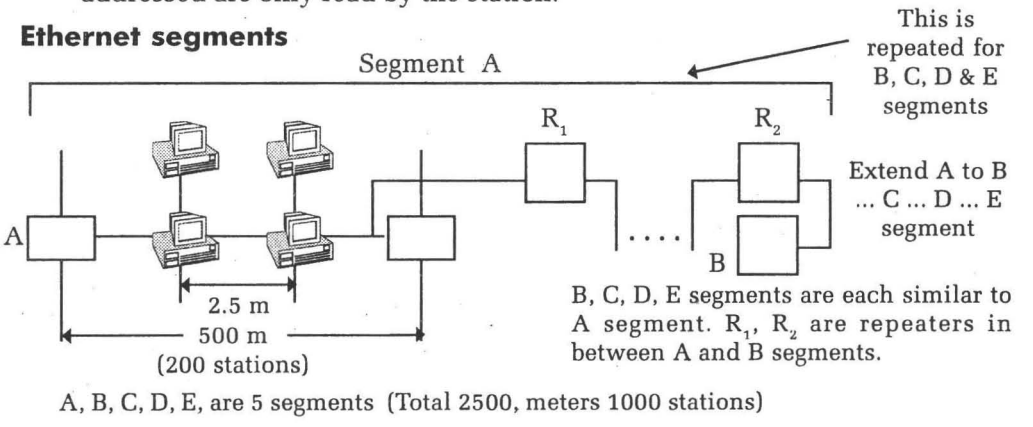
CRC –
- Error detection information (CRC–32) 4 bytes.

Implementation

- 802 model defines some of the physical specifications for each of the protocols defined in the MAC layer (though Bulk of the IEEE project 802 standard is connected on the data link layer of the OSI model).
- In 802.3 standard, IEEE defines :
  – the types of cable
  – connections and
  – signals

  The above are to be used in each of the five different Ethernet implementations.
- All Ethernet LANs are configured as logical buses (though they may be physically implemented in bus or star topologies)
- Each frame is transmitted to every station on the link, but the ones which are addressed are only read by the station.

Ethernet segments



A, B, C, D, E, are 5 segments (Total 2500, meters 1000 stations)

Fig. 12.3 Ethernet segments

RG - 8 Cable : Radio government cable is a thick co axial cable, provides the backbone of IEEE 802.3 standard.

Transceivers : Each station is connected by an AUI cable to an intermediary device called a medium attachment unit

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

(MAU) or more commonly known as a *transceiver* (transmitter - receiver). This performs the CSMA/CD function of checking for voltages & collisions on the line (a small buffer is present); Also serves as a connector that attaches a station to the thick coaxial cable via a tap.

AUI cables : Every station is linked to the corresponding transceiver by an attachment *unit interface* (AUI). It is a 15 wire cable with plugs that perform the physical layer interface functions between the station and the transceiver. Each end terminates in a DB–15 (15 pin) connector. One connector plugs into a port on the NIC, the other into a port on the transceiver. AUIs are restricted to a maximum of 50 meters length (allows some flexibility in placement of stations relative to the 10 base 5 back bone cable).

Transceiver tap or (Vampire tap) : Each transceiver contains a connecting mechanism called a *tap* since it allows the transceiver to tap into the line at any point (*Tap* is a thick cable sized well with a metal spike at the center. The spike is attached to the wires inside the transceiver. When cable is pressed into the well, the spike pierces the jacket and sheathing layers and makes electrical connection between receiver and the cable. *Vampire tap* is the another name because it bites the cable.

NIC : A thin ethernet similar to thick Internet system plus the functions of the transceivers eg. 10 Base 2 NIC not only provides the station with address but also checks for voltage.

Refer Table 13.1

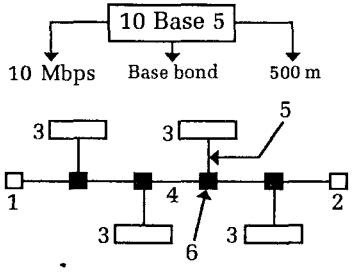
12.3 TOKEN BUS

LANs are needed in factory automation and process control, whereas nodes are computers controlling the manufacturing processes. Real time processing with least delay is needed. Processing should take place in line parallel with the jobs moving along the assembly line. IEEE 802.3 is not the right protocol for this, since the number of collisions cannot be predicted and the delay in sending data from the control place to the computers along the assembly line do not have a fixed value. Further, Token ring is also not a suitable protocol because generally an assembly line needs a bus topology and not a ring. Token bus combines features of Ethernet and token ring and combines the physical configuration of Ethernet (a bus topology) and the collision free (predictable delay) feature of token ring. Token bus is considered as a physical bus that operates as a logical ring using tokens. This is limited to factory automation and process control and has no commercial application in data communication. Here stations are logically organised into a ring. A token is passed among stations. If a station wants to send data, it must wait and capture the token. Like Ethernet, stations communicate via a common bus.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

10 Base 5 Thick Ethernet or thick net

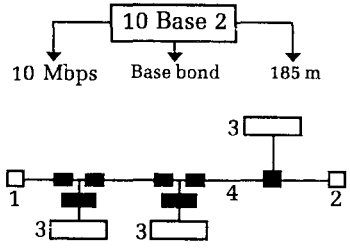


1. Cable Starter
2. Cable Terminator
3. NIC (4 Nos in the above figure)
4. Thick coaxial cable 500 meters
5. Attachment unit interface (AUI) Transceivers cable 50 meters Max.
6. Medium attachment unit (MAU) Transceivers

10 Base 5

- First of the physical standards defined in the IEEE 802.3 model.
- Name got from the size of the cable as thick net (Size of the

10 Base 2 Thin Ethernet or cheaper net

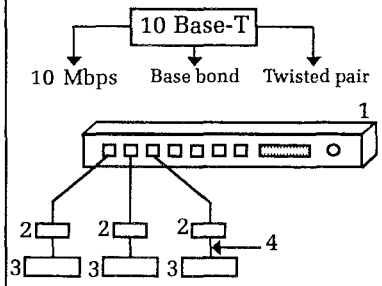


1. Cable starter
2. Cable terminator
3. NIC (3 Nos. in the above figure)
4. Thin coaxial cable 185 meters maximum
5. BNC – T connector

10 Base 2

- Second ethernet implementation defined in the IEEE 802 series.
- Called as also thin net, cheaper net, thin wire ethernet.
- Inexpensive with the same data rate.
- Bus topology LAN

10 Base-T Twisted pair Ethernet

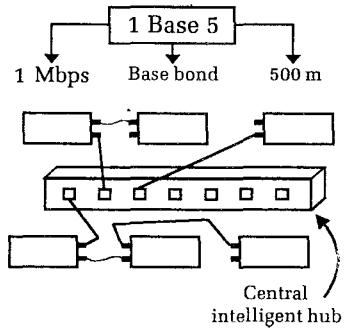


1. 10 Base –T Hub
2. RJ 45 Jack
3. NIC (3 Nos in the above figure)
4. 4–pair UTP unshielded twisted-pair cable

10 Base T

- Most popular standard defined in IEEE 802.3 series
- A start topology LAN using unshielded twisted pair (UTP) cable instead of coaxial cable.
- Supports a data rate of 10 Mbps and has a maximum length of hub to station of 100 meters.

1 Base 5 Star LAN (AT&T product)



1 Base 5

- Not used much because of low speed; only 1 Mbps, 10 times slower than the other three standards.
- Range can be increased by a mechanism called daisy chaining.
- Twisted pair cable to connect stations to a central intelligent hub.
- It allows as many as 10 stations to be linked each to the next in a chain in which the lead device only connects to the hub.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

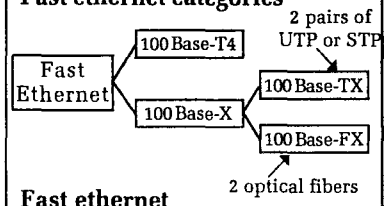
garden hose, stiff, difficult to bend with hands)

- Bus topology LAN uses base band signalling
- Maximum segment length of 500 meters
- LAN can be divided into segments by connecting devices. The length of each segment is limited to 500 meters. To reduce collisions, the total length of the bus should not exceed 2500 meters (5 segments).
- Standard demands that each station be separated from each neighbour by 2.5 meters (200 stations per segment and 1000 stations total).
- Physical connectors and cables utilised are coaxial cable, network interface cards, transceivers and AUI cables.

- Reduced cost, ease of installation (cable is lighter weight, more flexible than that used in thick Ethernet).
- Disadvantages are shorter range (185 meters) smaller capacity (accomodates fewer stations).
- Better choice if cost and small number of users are there eg. UNIX based mini computers or network of PCs and work stations.
- Connectors and cables utilised are : NICs, thin coaxial cable, BNC–T connectors
- The transceiver circuity has moved into the NIC, transceiver tap has been replaced by a connector that splices the station directly into the cable, eliminating the need for AUI cables.
- The cable required to implement is RG58. These cables are easy to instal and move around (inside existing buildings through walls and ceilings).
- BNC–T connector is a T–shaped device with 3 points: For NIC, For input, For output ends of the cable.

- Instead of individual transceivers, 10 Base–T ethernet places all of its networking operations in an intelligent hub with a port for each station.
- Stations are linked into the hubby four–pair RJ 45 cable (eight wire unshielded twisted pair cable) terminating at each end in a male type connector much like a telephone jack.
- Hub fans out any transmitted frame to all of its connected stations.
- Here logic with NIC ensures that the only station to open and read a given frame is the station to which that frame is addressed.
- Each station contains an NIC. Four pair UTP (Not more than 100 meters) connects the NIC in the station to appropriate port in the 10 Base – T hub.
- Weight and flexibility of the cable and the convenience of the RJ–45 jack and the plug make this 10 Base–T as the easiest of the 802.3 LANs to install and reinstall.

Fast ethernet categories



Fast ethernet

- IEEE developed a set of specifications providing a low cost ethernet. Operating 100 Mbps.
- Uses star topology and MCA protocol, Frame format as 10 Base–T. Encoding system has been changed to accomodate 100 Mbps data rate.
- Two different links between the computer and the hub are specified (one link transmission and the other reception).
- Two different standards for physical medium exists 100 base T4 and 100 base X.
- 100 Base T4 allows the use of 4 pairs of category 3 or 5 UTP between a computer and the hub (Two pairs for transmission and two for reception)
- 100 Base X allows the use of 2 pairs of high quality category 5 UTP, two pairs of STP (100 Base – TX) or two optical fibres (100 Base –FX).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

12.4 TOKEN RING (IEEE 802.5)

This is second most popular type of LAN. Nearly 40 percent of all LANs worldwide are token ring LANs. Originally it was developed by IBM and has since been standardised by IEEE as IEEE 802.5. The network access mechanism used by Ethernet (CSMA/CD) is not infallible and may result in collisions. Stations may attempt to send data multiple times before a transmission makes it onto the link. This redundancy may create delays of indeterminable length if the traffic is heavy. It is not possible to predict either the occurrence of collisions or the delays produced by multiple stations attempting to capture the link at the same time.

Access method

Token passing is shown in figure 12.4 whenever the network is unoccupied, it circulates a three byte token. From outside, token ring and ethernet LANs appears to be identical with same physical topology (a star) but internally uses a different topology. All computer in a token ring LAN share the same common circuit. Hence it is essential that access to the media be controlled by the data link layer. Token ring uses a controlled access technique called *token passing*. This can be compared to relay race in the athletics where the track belongs to you so long as you have the baton. In a token passing network, the baton is the token, a short electronic message that is generated when the network is started. The token is passed from NIC to NIC is sequence unit it encounters a station with data to send. That station waits for a while for the token to enter its network board. If the token is free, the station sends a data frame.

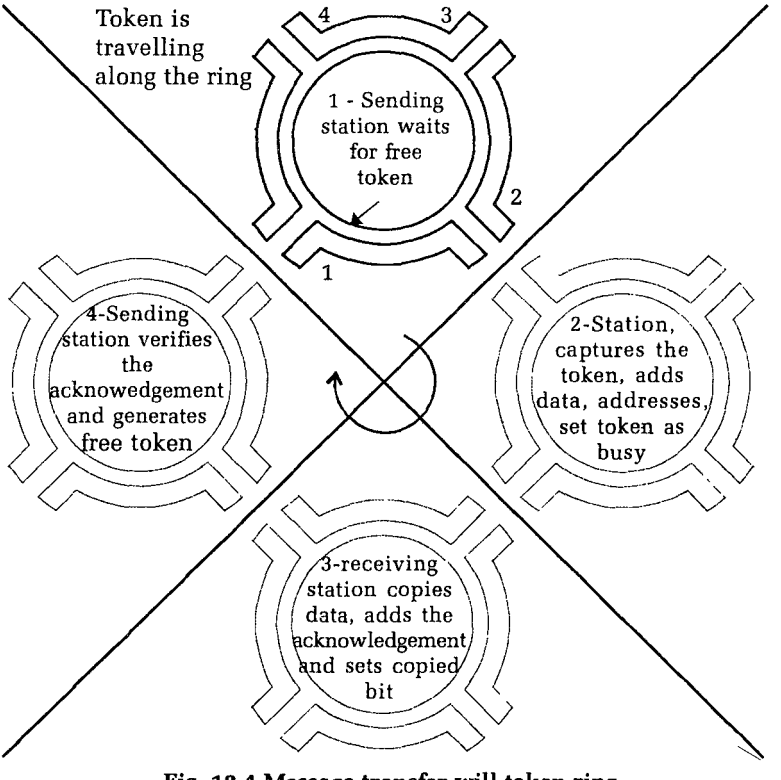


Fig. 12.4 Message transfer will token ring

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

The token moves between the computers on the network in a predetermined sequence (e.g. roll call polling). A computer with a message to transmit waits until it receives what is called a free token (a token available for use). The computer then changes the free token into a busy token, attaches its message to it and retransmits it on the circuit to the next computer in the sequence.

The data frame proceeds around the ring being regenerated by each station. Each intermediate station examines the destination address. If it finds the frame is addressed to another station, it relays to its neighbour. The intended recipient recognises its own address, copies the message, checks for errors and after changing the four bits in the last byte of the frame to indicate address recognised and frame copied at the destination computer sets the acknowledgement (ACR) bit (or NAK if there was an error in transmission) and the message continues around the ring making a complete round trip back to the transmitting computer. The transmitting computer then removes the message and inserts a new free token on the ring. Most token passing methods restrict the maximum number of messages, which a computer can transmit before issuing a free token. It should permit other computers to send messages so that monopoly from one computer should not occur.

Problem also occurs with this protocol about dealing of 'lost' tokens. If the computer having token crashes before it can retransmit it, or a computer with busy token has just transmitted a message crashes before receiving an acknowledgement and create a free token. Here the token is 'lost' because no other computer on the network can use the token. If no action on this taken, the entire network will cease to function. The solution is to designate one computer in the network to be the token monitor. If no token is circulated through the network for a certain length of time or if a busy taken circulates too often, the token monitor will create a new free token and destroy the busy token. The problem is complicated however, because the computer that crashed (causing the lost token) could be the token monitor itself, in which case there should be a backup token monitor.

If once is token is released, the next station in the ring where the data is to be sent has the right to take charge of the ring. In IEEE 802.5, another option is that the busy token can be reserved by a station waiting to transmit, regardless of that station's location in the ring.

Every station has a priority code. As a frame passes by, a station waiting to transmit may reserve the next open token by entering its priority code in the access control (AC) field of the token or data frame. Higher priority station may have a better control over lower priority station. If stations are with equal priority, first come will be first served.

In order to make the token travelling, token ring imposes a time limit on any station wanting to use the ring. A starting delimiter reaches each station within a specified interval (10 milli seconds). This shows that each station would expect to receive frames within regular time intervals. (If it receives a frame now, it expects, to receive the next frame again within a specified period).

As already said, many problems occur to disrupt the operation of a token ring network.

- A station may neglect to retransmit a token or token may be destroyed by noise (there will be no token on the ring and no station sends data).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

- A sending station may neglect to remove its used data frame from the ring or may not release the token when its turn has ended.

Under these circumstances, one station on the ring acts as a monitor. It sets a timer each time the token passes.

If token does not reappear in the allotted time, it presumes the token is lost and the monitor generates a new token and introduces it to the ring. The monitor also guards against perpetually recirculating data frames by setting a bit in the AC field of each frame. As the frame passes, the monitor checks the status field. If the status bit has been set, it knows that the packet has been around the ring. The monitor then destroys the frame and puts a token on to the ring. If the monitor fails a second station designated as back up takes over.

Token ring uses a six byte address, which is printed on the NIC card in a way similar to Ethernet addresses.

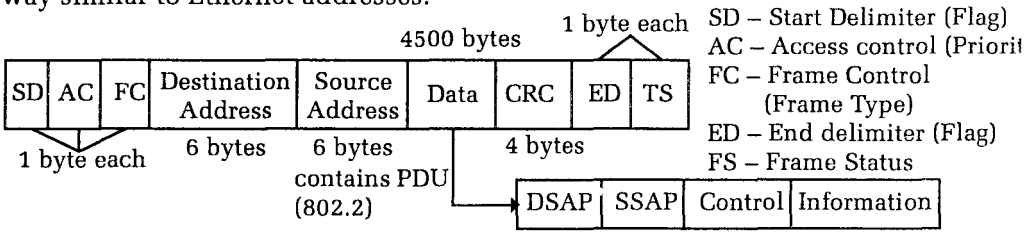


Fig. 12.5 Token ring frame

Start delimiter (SD)

- First field of the data/command frame
- One byte long
- Used to alert the receiving station to the arrival of the frame as well as to allow it to synchronise its retrieval timing.
- Equivalent to the flag held in HDLC
- J & K violations are created at the physical layer and included in all start delimiter to ensure transparency in the data field.
- An SD Bit pattern that appears in the data field cannot be taken for the start of a new frame.

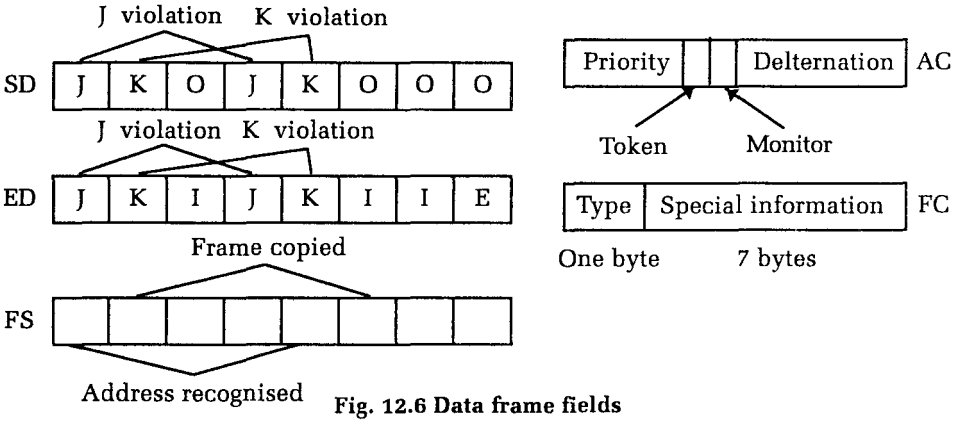


Fig. 12.6 Data frame fields

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

In differential Manchester, each bit have two transitions.

One at the beginning and another at the middle
- In I violation both gets cancelled
- In K violation middle transition is cancelled

AC field

- One byte long
- Includes four sub fields
- First three bits – priority field.
- Fourth bit – token bit (set to indicate that the frame is a data frame rather than a token or an abort frame)
- Token bit – followed by a monitor bit (fifth bit)
- Last three bits – Reservation field that can be set by stations wishing to receive access to the ring.

Destination address (DA)

- Six byte DA field contains the physical address of the frames next destination.
- If its ultimate destination is another network, DA is the address of the router to the next LAN. If same is on the current LAN, DA is the physical address of the next station.

Frame Control (FC)

- One byte long
- Contains two field

  (First is one bit field used to indicate the type of information contained in the PDU (may be control information or data. Second uses seven bits of the byte and contains information used by the token ring logic.

Source address (SA)

- Six byte 9 A field contains the physical address of the sending station.
- If its ultimate destination is another network as the originating station, SA is that of the originating station. If packet has be routed from another LAN, SA is the physical address of the most recent router.

Data is the sixth field. A PDU length or type field is not included in a token ring frame.

CRC is the seventh field; 4 bytes long and contain a CRC–32 error detection sequence. End delimeter (ED) – second flag field of one byte and indicates the end of the sender's data and control information. It is changed at the physical layer like SD and includes J & K violation which are necessary to ensure that a bit sequence in the data field cannot be mistaken for an ED by the receiver.

Frame status (FS)

- Last byte of the frame in the FS field.
- Set by the receiver indicate that the frame has been read
- By the monitor to indicate that the frame has already been around the ring.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

- This field is not an acknowledgement.
- Only tells the sender that the receiving station has copied the frame, which can be discarded.
- It contains two 1–bit pieces of information (address recognised and frame copied). These come at the beginning of the field and are repeated in the fifth and sixth bits. This repetition is for the purposes of preventing errors and is required because the field contains information inserted after the frame leaves the sending station. It cannot therefore be included in the CRC and so has no error checking performed on it.

Token frame

- Token is a place holder and reservation frame
- Includes three fields: SD, AC and ED.
- SD indicates that the frame is coming
- AC indicates that the frame is token and includes the priority and reservation fields.
- ED indicates the end of the frame.

Abort frame

- No information is carried – just starting and ending delimiters.
- Can be generated either by the sender to stop its own transmission or by monitor to purge an old transmission from the line.

Token ring

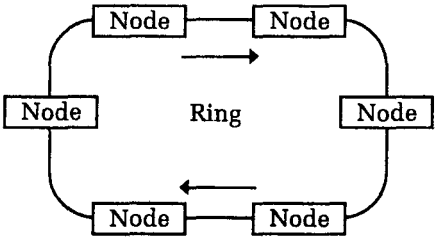


Fig. 12.7 Token ring

- Consists of a series of 150 Ω , shielded twisted pair sections linking each station to its immediate neighbours.
- Each section connects an output port one side and an input port on the other port one side and an input port on the other side of the station.
- Thus it creates a ring with an unidirectional traffic flow.
- Output from the final station becomes the input of the first station to complete the ring.
- Frame is passed to each station in the order for : Examination, Regeneration and Sending it to the next station.

Switch

- Configuring the network as a ring gives rise to a potential problem : Even one disabled or disconnected note could stop the flow of traffic all around.
- To overcome this, each station would have an automatic switch to by pass an inactive action.
- If a station is disabled, the switch closes the ring without it.
- If the station comes one, a signal sent by the NIC moves the switch and brings the station into the ring.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

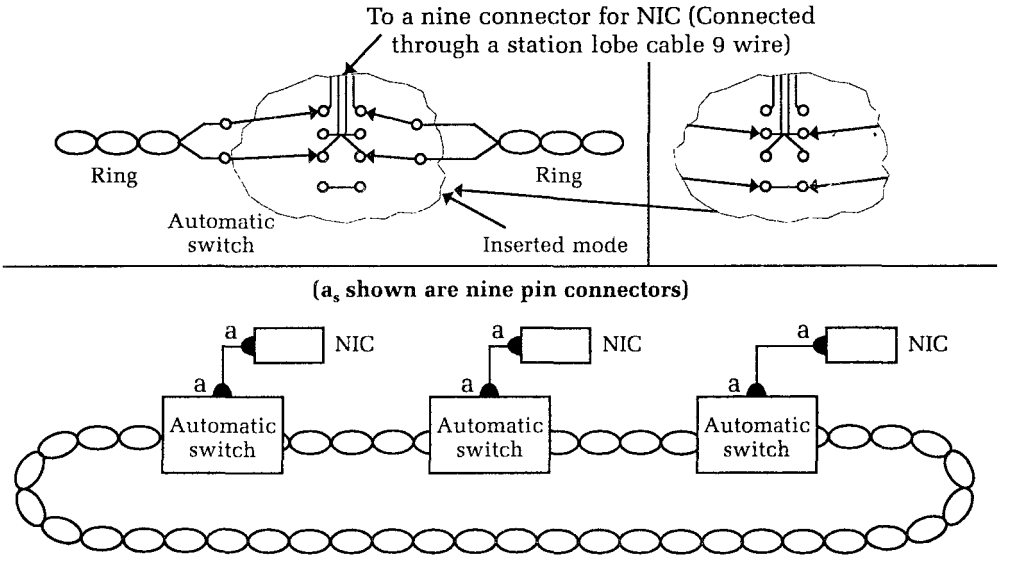


Fig. 12.8 Multistation access unit (MAU)

Multistation access unit (MAU)

This is as shown in figure 12.8. Individual automatic switches are combined into a hub called MAU. One MAU can support eight stations maximum. This system appears like a star with the MAU at the middle.

12.5 FDDI – FIBER DISTRIBUTED DATA INTERFACE

It is a set of standards originally design for use in MANs but has since made its way into backbone networks. It is a token passing ring network operating at 100 Mbps over a fiber optic cable. FDDI standard assumes :

(i) A maximum of 1000 stations

(ii) 200 KM (120 miles) path & needs a repeater every 2 KMS

(iii) Uses two counter rotating rings
- Primary ring where data traffic usually travels.
- Secondary ring mainly serves as a back up transmission circuit.

FDDI is a LAN protocol standardised by ANSI and ITU–U (ITU–TX.3), when FDDI was designed, speeds of 100 Mbps required fiber optic cable. Today comparable speeds are also available with copper cable. The copper version of FDDI is termed as CDDI. (Copper distributed data interface). It uses the same topology and media access protocol as FDDI. It uses two pairs of either shielded or unshielded category 5 twisted paper cable instead of fiber optic cable.

FDDI
- FDDI–C or CDDI (copper distributed data interface)
- FDDI–II It permits the transmission of voice and video over the same cable as the normal FDDI token passing data. FDDI–II functions like FDDI; It adds the ability to divide the 100 Mbps circuit between the standard FDII token passing data circuit and one or more circuit switched circuits for voice/and/or video.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

FDDI – II uses time division multiplexing to break up the available 100 Mbps into 17 separate channels, one channel at 768 Kbps and 16 wide band channels at 6.144 Mbps each. Token passing circuit will have the 768 Kbps channel. The 16 wide band channels can be allocated either to the token passing data circuit or to separate connection–oriented circuits used for the transmission of voice and video (or alternatively more data).

Soon the network begins to operate, all 16 wide band channels are allocated to the token – passing data circuit. Media access is controlled using the standard FDDI protocol. Allocation of these wide band channels from the token passing circuit to a new voice/video circuit is controlled by a computer called the *cycle master.*

Token passing – (Access method)

In a token ring network, a station can send only one frame each time it captures the token. But in the case of FDDI, access is limited by time. A station may send a number of frames within its allotted access period, with the provision of time sensitive frame, are sent first.

FDDI differentiates between two types of data frames : Synchronous and asynchronous while implementing this access mechanism. Synchronous refers to information that is time sensitive; asynchronous refers to information that is not. Both are called S–frames and A–frame respectively. Which ever station that captures the token is required to send S frames first though its time allotment has run out or not. The remaining time is then used to send A frames. It is necessary to understand the FDDI time registers and timers to understand and ensure fair and timely link access's mechanism.

Time registers

FDII has three registers to control circulation of the token and distribute link–access opportunities among the nodes equitably as under : Every station has three registers. These are :

(i) Synchrous allocation (SA)

- Indicates the length of time allowed by each station for sending synchronous data.
- Values are different for each station; negotiated during initialisation of the ring.

(ii) Target token rotation time (TTRT)

- Indicates the average time required for a token to circulate around the ring exactly once (elapsed time between a token's arrival at a given station and its next arrival at the same station).
- Value is same for all stations; negotiated during the initialisation of the ring (Since average taken, the actual time of any rotation may be less or greater).

(iii) Absolute maximum time (AMT)

- Holds a value equal to twice TTRT.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

- Token may not take longer than this time to make one rotation of the ring (If found more, some stations are monopolising the network, ring must be reinitialised).

The time values held by the above three registers control the operation of the ring. These values are set when the ring is initialised and do not vary in the course of operation.

Timers

Every station will have a set of times. The purpose is to compare actual timings with the values contained in the registers. Timers can be set and reset; their values decremented at a rate sent by the system clock. Two timers used by FDDI are :

(i) Token rotation timer (TRT)

- Runs continuously and measures the actual time taken by the token to complete a cycle. After the token is returned, the station records the time removing on its TRT into its THT. The station resets its TRT based on the TTRT value.
- TRT is set, it begins counting down. The time indicated by the TRT at any given point is the Actual time that has elapsed minus expected or allowed time (TTRT time).
- The token completes a rotation and returns to the station. The time indicated by TRT = Amount of time remaining for that rotation (TTRT–Actual elapsed time).
- The remaining time is then available to the station to send its frames.

(ii) Token holding timer (THT)

- As soon as the token is received, THT commences.
- Shows how much time remains for sending asynchronous frames once the synchronous frames have been sent.
- When the station receives the token every time, TRT value is copied to THT.
- Then THT start its own countdown. Any waiting synchronous frames must be sent as soon as the token is received.
- THT indicates how much time remains for sending asynchronous frames. The station may send only as many A–frames based on the THT credit. If THT is positive the station can send asynchronous data. If the value of this reaches or falls below zero, the station would release the token. THT may be considered as the station's bank account.
- S-Frames are bills which are to be paid immediately (even if the station has to go into debt to do so)
- A frames are expenditures that can be put off of for a while. The station can wait until its bank account can cover the expense.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

FDDI operation

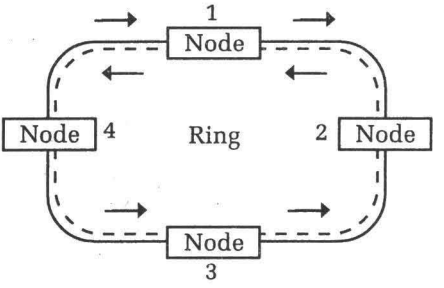


Fig. 12.9 FDDI Operation

An example is as shown below :

Assumptions made :

(i) 4 stations considered
(ii) TTRT – 40 time units
(iii) Time required to send each frame–1 time unit
(iv) Each station sends 5 synchronous data units per turn.
(v) Each station has asynchronous data to send plenty waiting in buffers.
(vi) System completely free of all types of delays
(vii) At time zero all stations start together

First round

Station 1	Station 2	Station 3	Station 4
• Receives the token • Transfers the value of TRT to THT countdown • Copies the value of TTRT to TRT (Say 40 time units) • Restarts the TRT countdown • Sends S–frame. • By the time TRT sends its allotted 5S frames, its TRT and THT are 35. THT is able to send 35 A frames. • After the TRT and THT are 0, Station releases the token	• TRT becomes 0 after arrive time of 40 • The station sends its five S–frames. It keeps the token for five time units After sending this, THT becomes –5. • Value is negative. • Station is deprived of the right to send A-frames. • It should pass on the token immediately.	• TRT becomes –5 after sending 5S frames in station 2 • The station sends five S Frames It keeps the token for five time units. After sending this. THT becomes – 10. • Value is negative • Station is deprived of the right to send A frames. • It should pass on the token immediately.	• TRT becomes – 10 after sending 5 S – frames in station 3 • The station sends five S frames it keeps the token for five time units. After sending this THT become – 10. • Value is negative • Station is deprived of the right to send A frames.
Arrival time : 0	Arrive time : 40	Arrive time : 45	Arrive time : 50
TRT 40, THT 35	TRT 0, THT –5	TRT –5, THT –10	TRT –10, THT –15
SYN 5 ASYN 35 → sent	SYN 5 ASYN 0 → not sent	SYN 5 ASYN 0 → not sent	SYN 5 ASYN 0 → not sent

The same process step by step through a number of rounds can be followed.

FDDI is both fair and self adjusting

FDDI uses a six byte address similar to Ethernet addresses on the NIC card.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Signalling (Physical layer)

A special encoding mechanism is used on FDDI called four bits five bits (4B/5B). Here each four bit of segment of data is replaced by five bit code before being encoded in NRZ–1, which inverts on the 1.

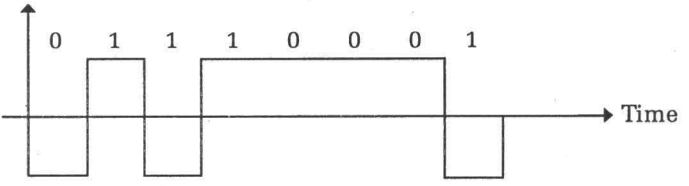


Fig. 12.10 Encoding

Extra encoding step is because sender and receiver may go out of synchronisation any time the data includes a long sequence of 0s (though NRZ–1 provides adequate synchronization under average circumstances).

- 4B/5B encoding transforms each four bit data segment into a five bit unit .
- This contains no more than two consecutive zeros.
- Each of the 16 possible four bit patterns is assigned a five bit pattern to represent it.
- The five bit patterns have been selected in such a way that even sequential data units cannot result in sequences of more than three 0s.
- None of the five bit patterns start with more than one 0 or end with more than two 0s.

Data sequence	Encoded sequence	Data sequence	Encoded sequence	Data sequence	Encoded sequence
0000	11110	0110	01110	1100	11010
0001	01001	0111	01111	1101	11011
0010	10100	1000	10010	1110	11100
0011	10101	1001	10011	1111	11101
0100	01010	1010	10110		
0101	01011	1011	10111		

Table 12.1 4B/5B Encoding

- While giving the control symbols for 4B/5B, care is taken not to assign any five number which is present above in the table 12.1 to represent a four bit counter part.
- SD field contains J and K codes
- ED field contains the symbols TT.
- To guarantee that control codes do not endanger synchronisation or transparency the designers specify bit patterns that never occur in the data field.
- Their order is controlled to limit the number of sequential bit patterns possible
- K always follows a J; H is never followed by an R.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Control symbol α	Encoded sequence	Control symbol start	Encoded sequence
Q (Quiet)	00000	K (used in start delimiter)	10001
I (Idle)	11111	T (used in end delimiter)	11101
H (Halt)	00100	S (Set)	11001
J (used in start delimiter)	11000	R (Reset)	00111

FDDI supports data rates up to 100 Mbps

Frame format

The FDDI standard divide transmission functions into four protocols. Figure 12.2 is the OSI model. The standard specifies a fifth protocol (used for station management)

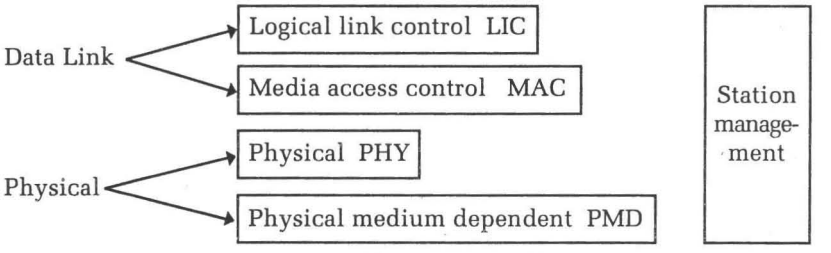


Fig. 12.11 FDDI layers

Media access control

FDDI MAC layer is similar to that defined for token ring. FDDI MAC frame itself is different enough to warrant an independent discussion of each field.

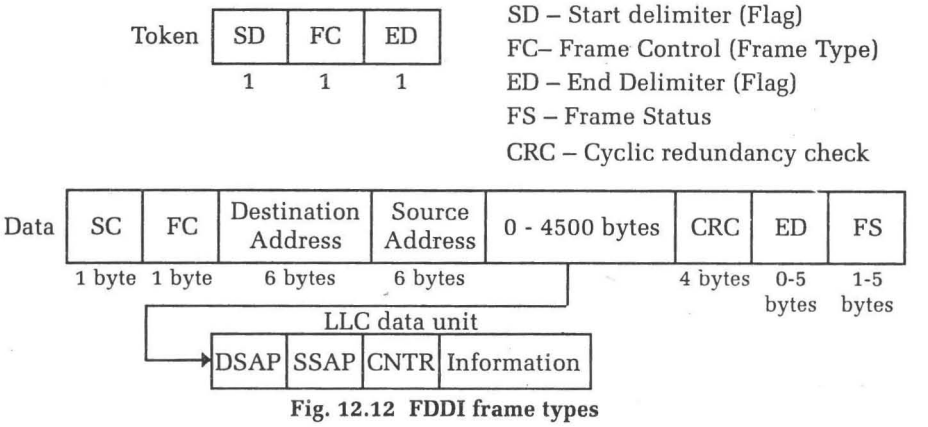


Fig. 12.12 FDDI frame types

Start delimiter (SD)

- First byte of the field is the frames starting flag.
- As in token ring, these bits are replaced in the physical layer by the control codes (violations) J and K (the five bit sequences used to represent J and K).

End delimiter (ED)

- The field consist of a 0.5 byte in the data frame or a full byte in the token frame.
- It is changed in the physical layer with one T violation symbol in the data frame or two symbols in the token frame.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Frame Status (FS)

Similar to the token ring. It is included only in the data frame and consists of 1.5 bytes.

PMD – Physical medium dependent layer

This layer defines the required connections as well as electronic components. The vital specifications for this layer largely depend on the transmission medium used (fiber–optic or copper cable).

FDDI is implemented as a dual ring which are two counter rotating rings. In most cases, data transmission is confined to the primary ring. Secondary ring is provided as an emergency if the primary fails. Data traffic usually will be on the primary ring, though can travel on both. Secondary ring serves a backup transmission circuit. Two types of FDDI computers are dual attachment station (DAS) on both rings an single attachment station (SAS) on only the primary ring.

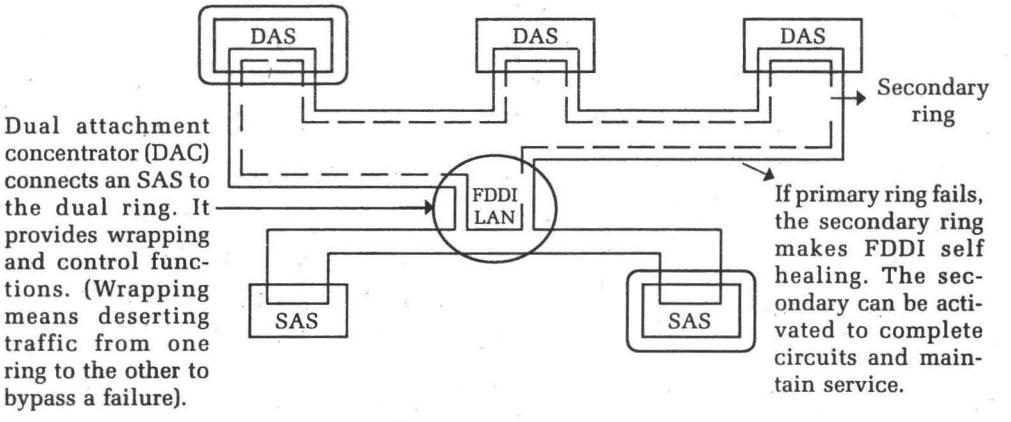


Fig. 12.13 Optical cable topology for an FDDI LAN.

Nodes

These connect to one or both rings using a MIC (either male or female depending on the requirements of the station). Each MIC has two fiber ports that allow to connect both ring cables.

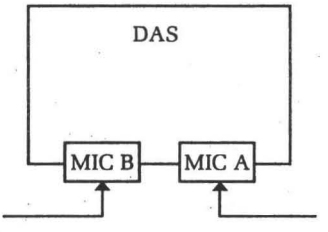


Fig. 12.14 Dual attachment station (DAS)

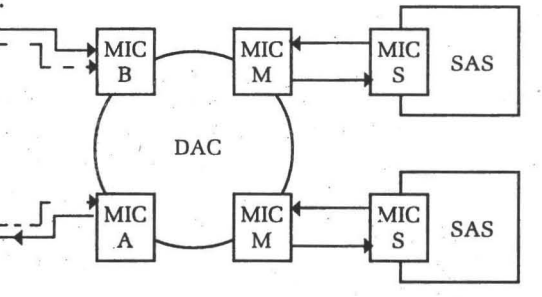


Fig. 12.15 Dual attachment concentrator and single attachment station (SAS)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

DAS (Dual attachment station)

- Two MICS (MIC A and MIC B)
- Connects to both rings to give improved reliability and through put.
- To do so, an expensive NIC with two inputs and two outputs required.
- Faults are by passed by a station's making a wrap connection from primary ring to secondary ring to switch signals.
- DAS stations must be active (switches turned on)

SAS (Single attachment station)

- Most workstations, servers and minicomputers attach to the ring in SAS mode.
- An SAS has one MIC (MICS)
- Connects only to one ring.
- Robustness is achieved if SASs are connected to intermediate nodes DACs rather than FDDI ring directly.
- Each workstation operates through a single NIC (only one input and one output)
- Concentrator (DAC) provides the connection to the dual ring.
- Faulty stations can be turned off and bypassed to keep the ring alive.

Wireless LANs

It is an alternate method of cabling; using the same protocols (Ethernet) but transmit data through the air rather than through physical media like coaxial cable, twisted pair or fiber optic cable. Most of these LANs have a NIC that is installed in the computer and connected to an external infrared or radio transmitter. Some wireless LANs are wireless only between the hubs. NICs are connected via traditional cabling to a network hub which contains the transmitter.

The advantages are :

- Wireless (specially suited for old buildings where wiring is difficult and expensive).
- Low cost
- Suitable for Lap top Computers (Permitting new capabilities of mobile computing)

The disadvantages are :

- Increased opportunity for noise to disrupt transmission.
- Slower data transmission rate than wired network (only 1 to 3 Mbps)
  - can go upto 100 Mbps with microwave based wireless networks under development.
- Lack of security.

POINTS TO REMEMBER

- The purpose of developing a LAN are (i) information sharing and (ii) Resource sharing. Information sharing refers to business needs that require users to access the same data file exchange information via e–mail or search the internet for information etc., Resource sharing refers to the same computer

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

sharing a hardware device (eg. printer) or a software package with other computers on the network, for the benefit of cost savings and improved decision making.

- A dedicated server LAN can connect any other network and handle large databases. It has a dedicated network server and use sophisticated LAN software. High end dedicated server LANs can be interconnected to form enterprise – wide network, this replacing the host mainframe central computer in some cases.
- Four common types of dedicated server LANs are file servers, database servers, print servers, communication servers. Zero slot LANs operate like peer to peer network. In general LANs run special network software to function both as a client and as a server.
- LANs are having four architectures ; (i) Ethernet, (ii) Token bus, (iii) Token ring, (iv) Fiber distributed data interface (FDDI).
- One classification of LAN is (i) Dedicated server LANs (ii) Peer to peer LANs (iii) Zero slot LANs.
- IEEE's project 802 is to set up standards so that LAN equipment manufactured by different companies is compatible. It divides the data link layer into two sublayers (i) Logical control layer (LLC) 802.2 and Media access control (MAC) 802.3. In the physical layer, FDDI uses 4B/5B encoding that converts 4 bits to 5 bits.
- Three LANs coming under project 802 are (i) Ethernet 802.3 (ii) Token bus 802.4 and (iii) Token ring (802.5).
- LLC is the upper sublayer considered same for all LANs and functions included are (i) flow control and (ii) Error detection. Here logical addresses, control information and data from the upper layers are packaged into a packet (Protocol Data Unit). MAC sublayer coordinates the data link tasks within a particular LAN.
- In addition to two sublayers LLC and MAC, Project 802 contains a section governing Internet working 802.1 in the network layer.
- CSMA/CD access method operates as under. It is an access method wherein stations transmit whenever the transmission medium is available. It retransmits when collision occurs. Collision is an event that occurs when two transmitters transmit at the same time on a channel which has been designed for one transmission at a time only. Data gets destroyed by collision.
- Token bus (IEEE 802.4) is used in factory automation, process control and combines features of token ring and Ethernet. Token ring (IEEE 802.5) uses token passing as a method of transmission initiation.
- Ethernet (IEEE 802.3) is the most commonly used LAN throughout the work for nearly 50 percent of all LANs using a bus topology and a connection based technique media access called carrier sense multiple access with collision detection (CSMA/SD). Many different types of ethernet are (i) 10 BASE 5 (thick Ethernet (ii) 10 BASE 2 (Thin Ethernet) (iii) 10 BASE – T (Twisted pair type Ethernet (iv) 1 BASE 5 (Star LAN) (v) 100 BASE T (Fast Ethernet) (vi) 10 BROAD 36 (Broad band Ethernet).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

- The network interface card (NIC) enables the computer to be physically connected to the network cable. This provides the physical layer connection among the computers in the network. Most LANs use a combination of UTP (unshielded twisted pair wires); STP (Shielded twisted pair), coaxial cables and fiber optic cable.
- Token ring switches can be encased in a MAU Multistation access unit. The frame is captured through the token in token ring which entitles a station to send one frame of data. The frame travels from node to node. (regenerated node) until the destination is reached.
- FDDI (Fiber distributed data interface) is a set of standards originally designed for use in MANs but has made its way into backbone networks. It is a token passing ring network operating at 100 Mbps over a fiber optic cable.
- FDDI have two rings : one primary ring for data transmission and a secondary ring assisting at the time of primary's failure.
- MIC is called as Media interface connector connects the dual FDDI ring to a node. DAS, a dual attachment station is a node with 2 MICs whereas SAS a single attachment station is a node with one MIC. SAS is attached to the FDDI rings through a dual attachment concentrator (DAC)
- FDDI has three time registers to control circulation of the token and distribute link access opportunities among the nodes (i) synchronous allocation (SA) (ii) Target token rotation time (TTRT) (iii) Absolute maximum time (AMT). The timers used are two types (i) Token rotation timer (TRT) and (ii) Token holding timer (THT). FDDI specifies protocols for the physical and data link layers.
- FDDI's signalling 4B/5B ensures that there cannot be a data sequence of more than three 0s transmitted across media in FDDI protocol and takes care of the bit synchronisation problems arising from long strings of 0s in NRZ–1 encoding.

QUESTIONS

1. Define local area network (LAN)
2. For what purposes LANs are developed?
3. Explain the distinguishing features of LAN.
4. What are the different architectures of LAN ?
5. What are the different classifications of LAN? Explain one atleast.
6. Compare and contrast, a word processing used on a LAN with a word processor used on a single computer.
7. What is the difference between base band and broad band?
8. Define and explain the data link layer in IEEE project 802. What is the reason behind dividing this layer into sub-layers?
9. Describe CSMA/CD and CA. What part of the 802 project uses CSMA/CD?

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

10. What is a collision? When does collision takes place?
11. Define the terms 10 BASE 5, 10 BASE 2, 10 BASE T, 1 BASE 5 , 100 BASE T, 10 BROAD 36.
12. What are the advantages of FDDI over a basic token ring?
13. What is FDDI and what are its features?
14. Compare and contrast Ethernet, Token bus, token ring and FDDI.
15. Why there is no field in the 802.3 frame?
16. What are the two methods of LAN access supported by the IEEE 802 committee?
17. How does a token passing network mechanism operates?
18. What is the mechanism involved to enable an SAS to access both the primary and secondary rings?
19. Compare SAS, DAS and DAC with special reference to their functions.
20. Explain how 4B/5B encoding under FDDI guarantee that there will be no sequence of four or more 0s in the data field?
21. Explain MAU.
22. Compare and contrast TRT with THT. What are timers?
23. Explain wireless LANs.
24. What is PMD? Explain.
25. It is said that looking some computers together with a cable does not make a network. Why?
26. Should you select a network because of its protocol or its performance characteristics? Give your views supported with reasons.

FILL IN THE BLANKS

1. LANs are developed for purposes of _____ and _____ sharing.
2. Four architectures of LAN are Ethernet, Token bus, Token ring and _____.
3. IEEE project 802 covers the first two layers of the _____ model.
4. In CSMA/CD, the number of collisions as compared to MA, it is _____.
5. Star topology used in 10 BASE – ____.
6. 10 Base 5 and 10 Base 2 uses _____ and _____ coaxial cables respectively.
7. 1 Base 5 is not used much because of _____ _____.
8. Fast ethernet have two categories 100 BASE ____ and ____.
9. The counter part of 802.3 frames preamble field is the _____ field on the 802.5 frame.
10. The source address field used in the MAC frame in Ethernet is the previous station's _____ address.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

11. Project _____ standards provides a collision free protocol.
12. The IEEE project has two sub layers in the data link layer upper _____ sublayer, lower _____ sublayer.
13. Star topology featuring a central hub and daisy chaining are found in _____
14. In token ring _____ houses the switches.
15. _____ is another name for CSMA/CD and as well as IEEE 802.3.
16. When the frame reaches its destination in a token ring message is copied and _____ __ ___ ____ __ ___ _____ happens.
17. FDDI means _____ _____ _____ _____.
18. Example of 4B/5B sequence is 1 1 1 0 0 0 __ 1 1.
19. FDDI uses encoding NRZ–1 and _____.
20. Three registers of FDII are SA, _____ and AMT.
21. SA register holds the amount of time a station has to send _____ data.
22. _____ _____ _____ type of node has two MICs and connected to both the primary and secondary rings.
23. _____ type of node has one MIC, only one ring is used.
24. Two timers used by FDDI are _____ and _____.
25. Timer used by TRT is _____ _____ and by THT is _____ _____.

Answers

1. information ; resource
2. FDDI
3. OSI
4. less
5. T
6. thick ; thin
7. low speed
8. TX ; FX
9. SD
10. physical
11. 802.5
12. LLC ; MAC
13. 1 BASE 5
14. MAU
15. Ethernet
16. interchange of two bits in the packet
17. Fiber distributed data interface
18. 1
19. 4B/5B
20. TTRT
21. synchronous
22. DAS and DAC
23. SAS
24. TRT ; THT
25. Token rotation ; Token holding

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

13

METROPOLITAN AREA NETWORKS (MAN)

MAN is a network that spans a geographical area of the size of a city. These typically span from 3 to 30 miles and connect back bone networks. When LANs are in close proximity need to exchange data, they are connected privately using cables, routers or gateways. When LANs of a single enterprise are distributed over a larger area (city or campus) privately owned connecting infrastructure is impractical. Organisations prefer to use the services of existing utilities like telephone company rather than having their own cables (even there is no problem in laying cable on public land). The services include :

- Distributed queue dual bus (DQDB) IEEE 802.6 (DQDB resembles LAN standard)
- Switched multi megabit data services (SMDS)

MAN provides dial-in and dial out capability to LANs, backbone networks (BNS) and mainframes.

Most organisations cannot afford to have long stretches of cable, build microwave towers or lease satellites. Alternatively, they go for rent or lease circuits from common carriers like AT&T, MCI, Bellsouth, PACTEL or NYNEX.

13.1 IEEE 802.6 DISTRIBUTED QUEUE DUAL BUS (DQDB)

It is a protocol used by IEEE to be used as a LAN or MAN. It is a standard developed for local and Metropolitan area networks and cover the MAC sublayer for networks using the DQDB access method.

DQDB uses a dual bus configuration. Each device in the system is connected to two backbone links and access to the links are granted not by contention or by

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

token passing (like 802.4 and 802.5). It is granted by a mechanism known as distributed queues.

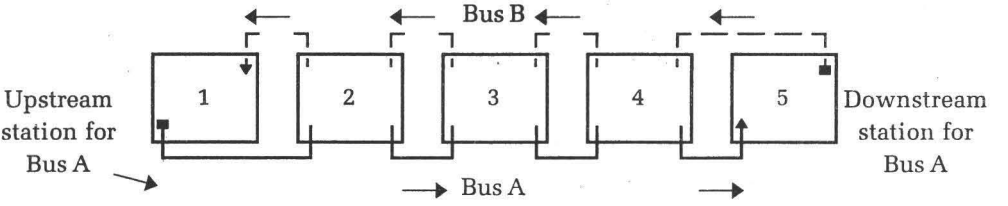


Fig. 13.1 DQDB topology

Two unidirectional buses are shown in figure 13.1 (Bus A and BUS B). Five stations are connected to the two buses. Buses are connected to stations through input and output ports (without any drop lines). Each bus supports traffic in one direction. The direction in each of the two buses are opposite to one another. Each bus starts by a square and the end by a triangle. Bus A moves from left to right; Bus B moves from right to left. Bus B moves from station 5 to station 1. Opposite route is that of Bus A.

For Bus A, station 1 has no upstream stations; station 2 has station 1 as an upstream. Station 3 has 2 upstream stations 1 and 2. Station 5 has four upstream stations, but no down stream station; it is the end of Bus A.

For Bus B, it is the reverse of Bus A.

Data travel on each bus as continuous steady stream of 53 byte slots. These slots are not packets. Head of Bus A and head of bus B in stations 1 and 5 generates empty slots for use on bytes A and B respectively. The data rate depends on the number of slots generated per second. Today number of different data rates are used.

The empty slot will be travelling down the bus expecting a transmitting station to drop data into it and the intended data reads the same.

Question is which bus will be the source station?
which bus carries the data to a given destination station?

The source station should choose the bus for the intended destination station and it should be in the down stream.

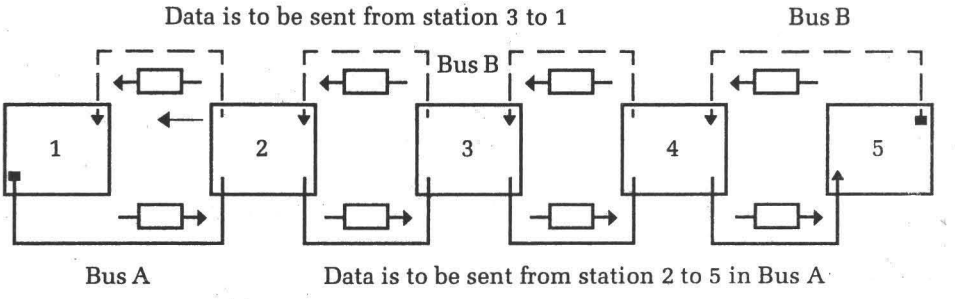


Fig. 13.2 Data transmission in DQDB

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Data from station 2 to 5

- Increasing number in the station is observed
- Station 2 is in upstream station 5 is in downstream
- Flow is from station 2 to station 5
- Hence Bus A could be selected. It creates an empty slot in station 1.
- Station 2 drops its data into the passing slot and addresses it to station 5.
- Station 3 and 4 reads the address and passes the slot to station 5
- Station 5 reads the data and changes the status of the slot

Data from station 3 to 1

Bus B is selected. Procedure is similar as above.

The direction of traffic in each bus is the opposite of the other. Each bus supports traffic in one direction. A station should wait for the arrival of an unoccupied slot to transmit data.

Question is what is to stop an upstream station monopolising the bus and occupying all the slots. The stations near the end of the bus suffer since the stations at the start have access to empty slots. This unbalance is an injustice, by degrading quality of service, specially for time sensitive information (voice or video).

The solution for data being sent from station 2 to 5 on Bus A. Here station 2 can set reservation bit in a slot on Bus B to tell each station it passes that station is reserving a slot on Bus A. The slot passes every station down stream from station 2 on Bus B – the same stations that are upstream from it on Bus A. The stations must respect the reservation of a downstream station and leave slots free for the down stream station's use. No station must send data without first making a reservation, even if the slot passes empty. A station which has made reservation should occupy the particular slot reserved.

This shows that to send data on one bus, a station must use the other bus for reservation.

Distributed Queues

Queues are adopted here. Each station has one queue A for Bus A and another queue B for Bus B (to make reservations and tracking the reservations of other stations). A queue works on first in, first-out principle for storage mechanism. DQDB queue is something like a waiting list of stations.

Let us study the first figure 13.3 with respect to Bus A

- Station 1 creates slots continuously and releases to Bus A.
- In order to send its own data and to use one of the slots created, it must place itself in queue A like other stations.
- If tokens in front of its own are there, station 1 releases empty slots for the down stream stations 2, 3, 4, 5.
- Waits until its own token comes up. Then it inserts its data into a slot and sets the slots busy bit before releasing the slot to the bus.
- Station 5 cannot send data by Bus A (No down stream). It does not even need a queue.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

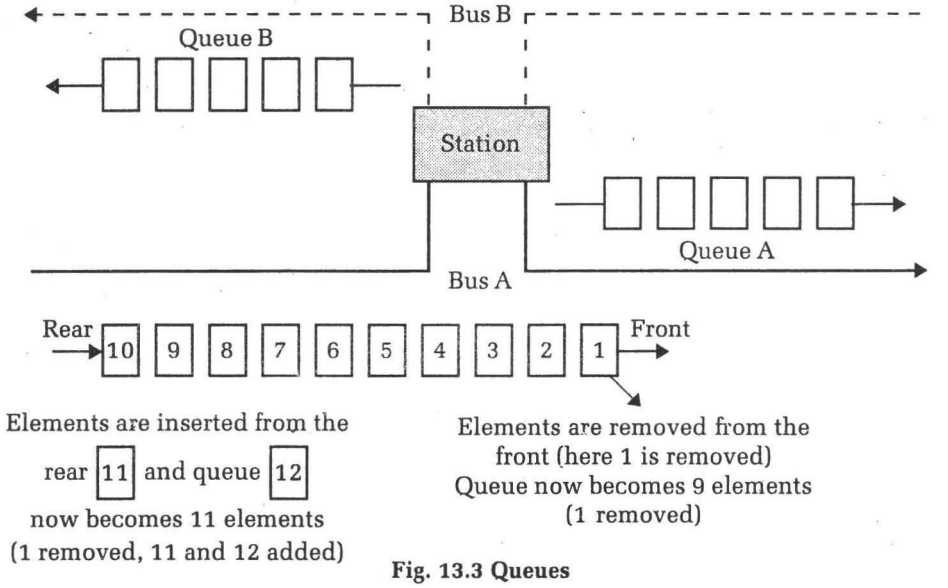


Fig. 13.3 Queues

The preceding description also applies to Bus B. In Bus B station 5 creates and releases the slots and station 1 does not need a queue B.

DQDB standard states how logical queues A and B are to be used. Networks and stations can be made to stimulate the operations of the queues as long as those simulations follow the stated rules. It is also implemented as a ring.

In this case one station plays the role of both header and end. This is reconfigurable whenever a link or station fails.

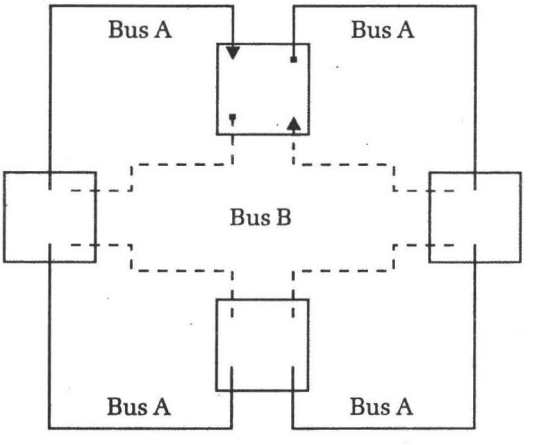


Fig. 13.4 Ring without failure

Operation DQDB Layers

IEEE defines both

- Media access control (MAC) sub layer
- Physical layer of DQDB

Copyright © 2009. Global Media. All rights reserved.

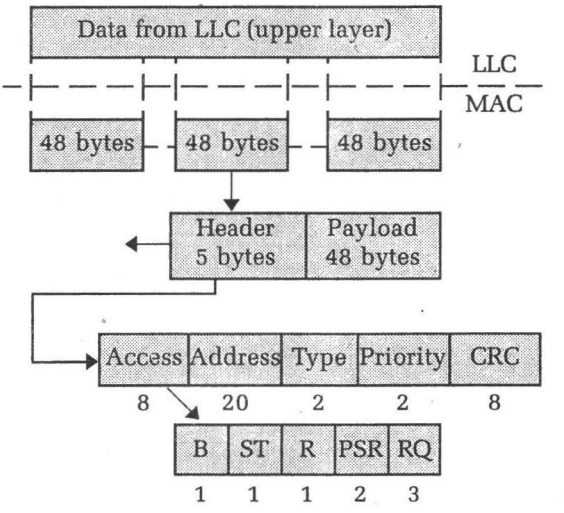
Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

MAC layer splits the data stream coming from LLC layer (upper layer) into 48 byte segments and adds a 5 byte header to each segment. It creates slots of 53 bytes. Thus making a DQDB slot compatible with the size of a cell in ATM.

Five bytes of header are distributed among five major fields :

(i) Access field :

- Fields – an eight bit field that control access to the bus.
  - Busy (B) – indicates whether or not the slot is occupied.
  - Slot type (ST) – defines two types of slots, one for packet and other for isochronous transmission.
  - R bit is reserved
  - Previous slot read (PSR). Two bit field is set to 0 by the addressed station once it has read the contents of the slot.
  - Request (RQ) – 3 bits set by stations to make reservations for slots. Represent eight levels of priority in network with different station levels. In networks with no priorities, the first bit is used.



B – Busy, ST – Slot type, R – Reserved, PSR – Previous slot read; RQ – Request.

Fig. 13.5 DQDB layers

(ii) Address field – holds a 20 bit VCI (Virtual Channel Identifier) to be used for MAN and WAN transmission. When used in a LAN, field contains all 1s and an additional header is added to carry the MAC Physical address.

(iii) Type field – 2 bits; identifies the type of the payload as user data, management data and so on.

(iv) Priority field – identifies the priority of the slot in a network that uses priorities.

(v) CRC – 8 bit cyclic redundancy check ($x^8 + x^2 + x + 1$) ; used to detect single or multiple bit errors and to correct single bit errors in the header.

13.2 SMDS (SWITCHED MULTIMEGABIT DATA SERVICES)

It is an alternative to private network data transmission within the LATA areas in which they operate. It is a service for handling high speed communications for Metropolitan area networks. This was developed to support organisations that need to exchange data between a number of LANs located in different parts of a city/campus. First, it was aimed at MAN market, particularly the interconnection of LANs, then the WAN environment.

SMDS is a switched version of the T–carrier and SONET services. The Regional Bell operating companies (RBOCs) offer SMDS at two transmission rates:

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

DS–1 at 1.544 Mbps

DS–3 at 44.736 Mbps

SMDS is a precursor to the full broad band ISDN transmission and the full implementation of SONET at OC–3 rates (155.52 Mbps). Before the introduction of SMDS, making these exchanges was often difficult, the options are :

(i) To subscribe to an existing telephone company service such as switched / 56 or DDS. Most LANs create and consume data at 10 to 16 Mbps, where as the data rates of the switched/56 and DDS services (56 Kbps and 64 Kbps) create unsupportable delays and a degradation of service.

(ii) To subscribe to a DS–1 service with a leased T–1 line and data rate of 1.544 Mbps or to a DS–3 service with a leased T–3 line and data rate of 44.736 Mbps.

Though data rate problems are solved from the above options, these are expensive.

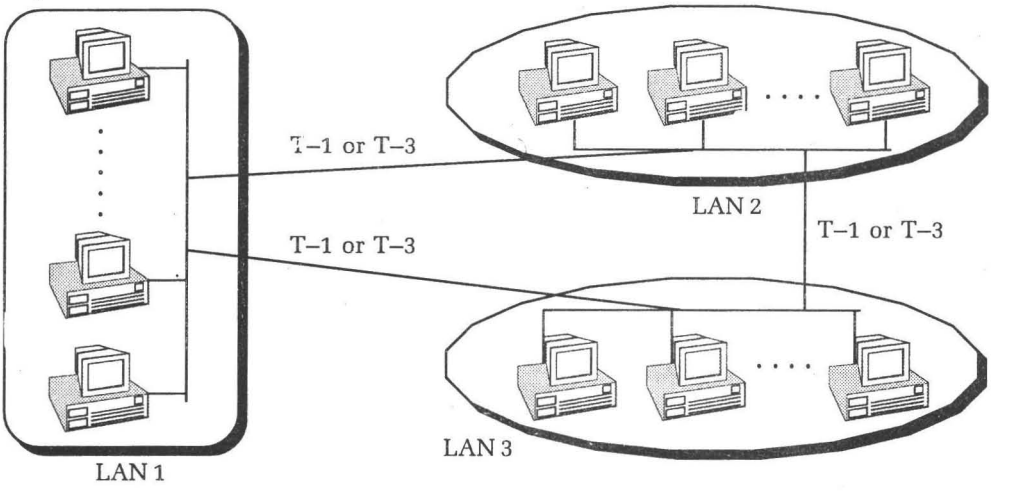


Fig. 13.6 Connecting LANs with T–1/T–3 lines

3 T_1 lines means more than US $ 50,000 per year for a data rate of 1.544 Mbps.

T_3 lines cost are still higher (10 times to T–1 lines) – more than 500,000 US $ for a data rate of 44.736 Mbps

Not all companies can afford this and companies do not use data traffic 100 percent of the time. Lines are affordable, if they could be shared. Telephone companies do not offer switched based leases for T–lines. SMDS is a packet switched diagram service for high speed MAN traffic. It is provided by common carriers and is intended to replace switched services such as switched/56. It is a switched network, subscribers pay only for the time they use.

Subscribers LAN Link to an SDMS network through routers.

In figure 13.7, a customer LAN is connected by its router and a dual bus to the SMDS network. If only one LAN is there to connect to the network the DQDB mechanism is simple. No queues are required.

In figure 13.8, a customer site can connect multiple LANs to the SMDS network through a single DQDB. Full capability of the DQDB is required. Access to SMDS is coordinated using the SMDS interface protocol (SIP) which is based on

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

DQDB. SMDS networks offer rates that differ from those provided by the services (DS–1 to DS–4) and cannot be used for WAN traffic.

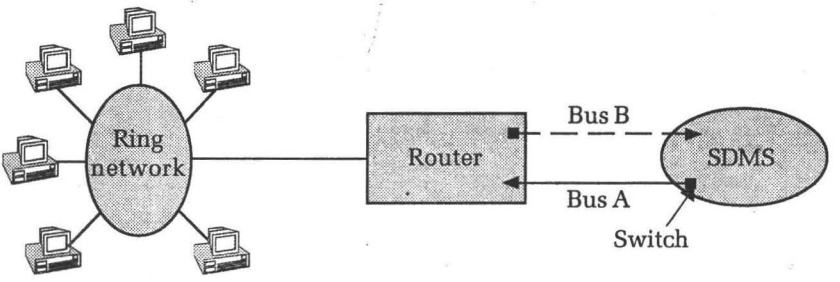


Fig. 13.7 DQDB in a MAN (Single LAN connection to SMDS)

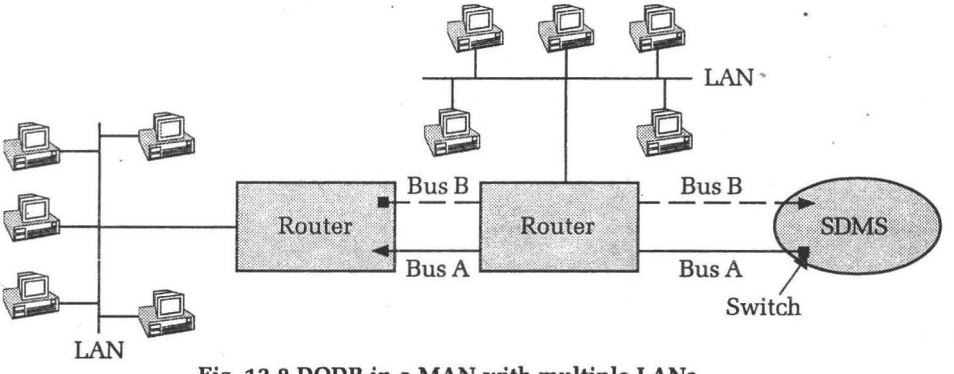


Fig. 13.8 DQDB in a MAN with multiple LANs

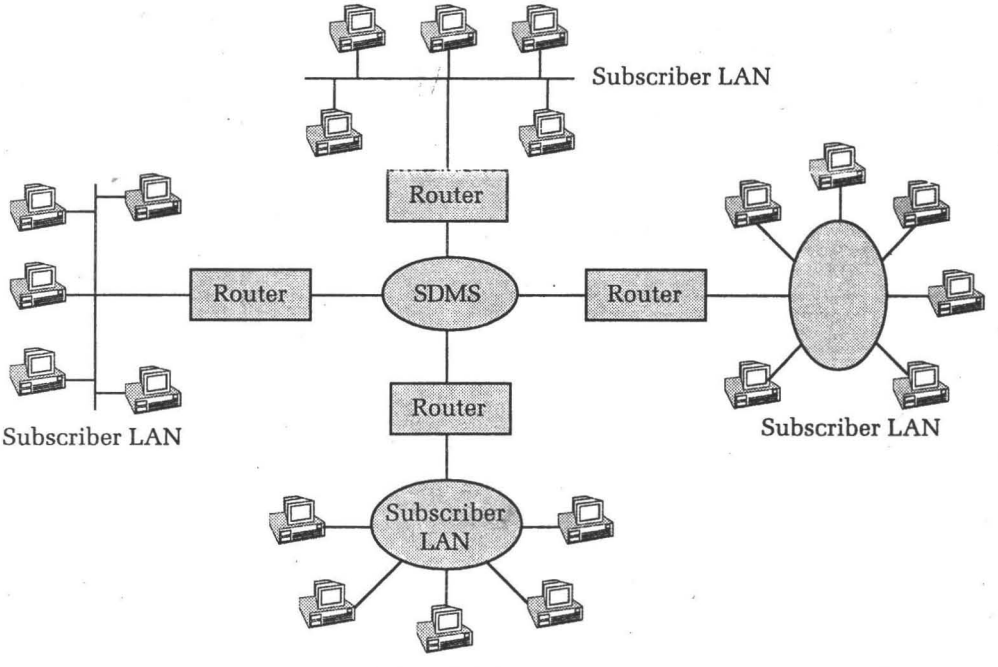


Fig. 13.9 SMDS as a MAN

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

POINTS TO REMEMBER

- MAN is a network that spans a geographical area of the size of a city (spans from 3 to 30 miles) and connect bone networks.

  The services of MAN include
  - Distributed queue dual bus (DQDB) IEEE 802.6
  - Switched Multimegabit data services (SMDS)
- IEEE 802.6 DQDB is a protocol used by IEEE to be used as a LAN or MAN, a standard developed for local and metropolitan area networks. DQDB operates in the physical layer and the MAC sublayer. It uses two unidirectional buses which travel in opposition directions.
- Data transmission in DQDB occurs through capture of an empty slot and insertion of data into the slot.
- A data is transmitted from a station only in the downstream direction. The reservation is made for a slot on the other upstream bus.
- Through the use of FIFO queues, each station has an equal opportunity to send its data.
- In a MAC sublayer, there are 48 byte payload added to a 5 byte header.
- In the physical layer, the protocol define the electrical devices, media and data rates.
- SMDS is a packet switched datagram service for handling high speed communications for MAN. It is a switched version of the T–carrier and SONET services.
- SMDS is a good choice for users who require a data rate greater than that of switched /56 or DDS. It does not need full time use of a link. SMDS uses DQDB for media access.
- IEEE defines both Media access control (MAC) sublayer and Physical layer of DQDB.

QUESTIONS

1. Draw four token ring LANs connected to SMDS through a DQDB.
2. What is MAN? Explain.
3. What is IEEE 802.6? Explain DQDB topology.
4. Explain upstream and down stream stations. How the data transmission takes place in DQDB?
5. What are distributed queues?
6. Show how DQDB can be implemented as a ring?
7. Explain SMDS network through routers with a sketch.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

FILL IN THE BLANKS

1. DQDB is distributed _____ _____ _____.
2. SMDS is switched _____ _____ _____.
3. SMDS is a service handles high speed communications in a _____.
4. DQDB operates in the physical and _____ ____ layer.
5. DQDB access field byte is set too after the slot contents are read in _____ bit field.
6. A DQDB is made up of _____ one directional buses travelling in opposite directions.
7. SMDS interface protocol (SIP) specifies the use of _____ as a media access method.
8. DQDB header identifies the type of payload in _____ bit field.
9. DQDB access field byte is used for station reservations in _____ bit field.
10. _____ uses a dual bus configuration.
11. _____ is a switched version of the T-carrier and SONET services.
13. RBOCs offer SMDS at two transmission rates :

    DS–1 at _____ Mbps

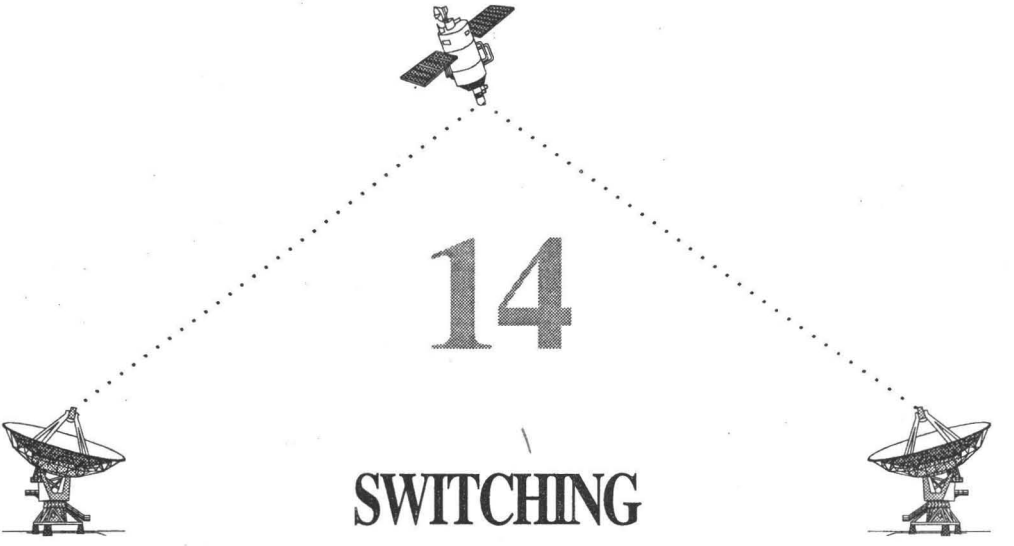
    DS–3 at _____ Mbps

Answers

1. queue dual bus
2. multimegabit data services
3. MAN
4. data link
5. PSR
6. two
7. DQDB
8. type
9. RQ
10. DQDB
11. SMDS
12. 1.544 ; 44.736

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

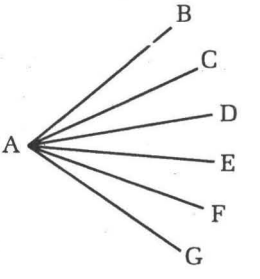


14

SWITCHING

Always in a multiple devices, one should know how to connect each of the devices to make communication possible. The simplest is to instal a point-to-point link wherein a link is established between each pair of devices called as a mesh topology or a link between central devices with other devices called as a start topology. These are cumbersome and impractical and at the same time wasteful if we consider large networks. The number and length of the links needed are very high and hence such infrastructure is not cost efficient. Further, the utilisation of these links are also not up to the expectations.

If A is connected to all points B, C, D, E, F and G only if A and B are used frequently, the other devices are idle and not used.



Even in the case of multipoint connections through a bus the distances between devices and the number of devices makes them unsuitable if a particular limit is exceeded (beyond the capacities of the media and equipment.

In such cases, the ideal solution would be to join for *switching. Switching* includes identifying and connecting independent transmission circuits to form a continuous path from your telephone to the telephone you are calling. A switched network consists of a series of interlinked nodes called switches which are hardware and/or software devices which have the capability of creating temporary connections between two or more devices linked to the switch but not to each other. Here in this network, some of these nodes are connected to the communicating devices, but the rest are used for routing only.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

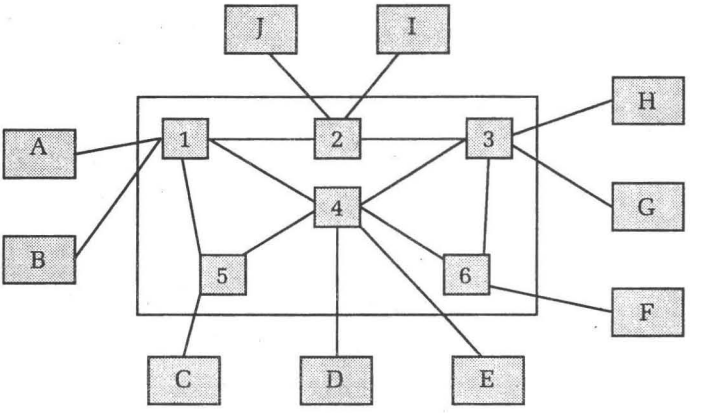


Fig. 14.1 Devices connected to switches

A, B, C, D, E, F, G, H, I, J are the communicating devices connected to switches 1, 2, 3, 4, 5, 6. Each device is connected to one switch atleast and each switch is connected to number of devices to have multiple links and complete the connections between them, two at a time.

A more flexible and economical interconnection arrangement to allow for temporary connections between any two telephones that wish to communicate with each other. Such a process is called *switching,* a methodology that eliminates the need for direct wire connection between all station parts in a network.

COMMUNICATION PATH

Computers connected to transmission lines may communicate with one another in any one of the three ways :

- Circuit switching (to interconnect telephones in a network)
- Packet switching (a block of information known as 'packet' communication from computer to computer in a formatted way)
- Message switching (all message packets are received and stored by a central node connecting to all the terminals)

Circuit or line switching

It is a switching technology that establishes an electrical connection between stations using a dedicated path.

It is the most common type of switched network e.g. Home telephones uses circuit switched connections. It creates a direct physical connection between two devices such as phones or computers and messages go directly from one to the other. E.g. a voice message going from one telephone to another telephone after the two communication circuits are switched together at the telephone company central office.

Communication costs are high in the total cost of using a wide-area computer network. Various techniques are available for reducing these costs through sharing mechanism. The establishment of a dedicated data-transmission path from source to destination for each information exchange is called *'circuit or line switching',* which is the usual mode of communication used in the public telephone network. *Circuit switching* is initiated by dialing and implemented by telephone exchanges.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

It has the disadvantage that once a path is established between two locations, it cannot be used by other potential users along the path, even if the utilisation of that path is very low. This problem can be overcome by another technique called *'Message Switching'*.

The example for this is a phone network which is a circuit switched network. The phone connection between Bangalore and Hyderabad (if dialled from Bangalore to Hyderabad) switches along the line route the call and reserve a circuit straight up to the destination. The circuit is dedicated to your call and only your call. It is something as though a single wire strung between you and the person you are talking to. Circuit switching is the simplest of the three types and is exclusively used by the two parties till the caller hangs up the phone. Computers and terminals connected to a telephone network may also use this method of establishing communication paths among them, but are inefficient as bursts occur during communication among computers for short period and some long silent periods wherein the communication line not used. However it is ideal for low speed communication.

If A, B, C, D computers are to connected to E, F, G, H computers. This would have needed long links and 4 x 4 = 16 numbers of links.

This could be connected in a simple way by having switches and suitable servers. Now any computer in the left hand side can be connected to any computer in the right hand side through switches and severs.

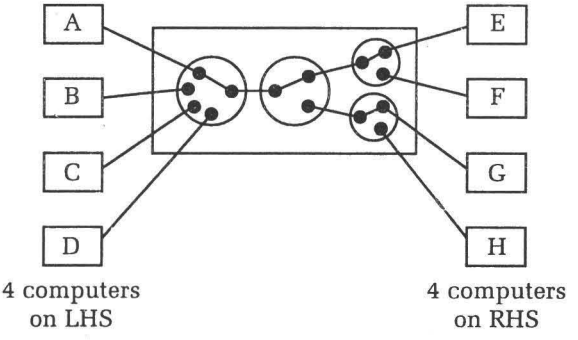


Fig. 14.2 Circuit-switched network

Circuit switches

A circuit device is a device having a number of inputs and a number of outputs that creates a temporary connection between the two input and output links. The number of inputs could vary from the number of outputs. Circuit switching today have two technologies.

- Space – division switches
- Time – division switches

A combination of the above also can be adopted, known as space and time division switching combination.

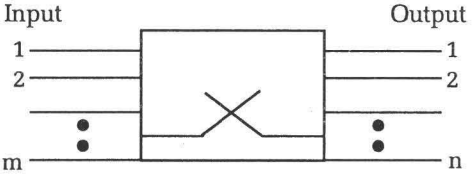


Fig. 14.3 A circuit switch

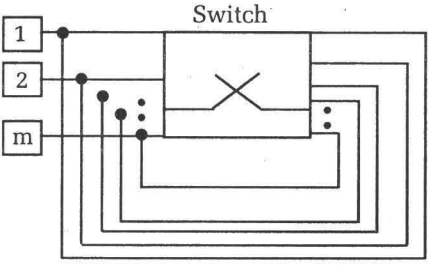


Fig. 14.4 A folded switch

Copyright © 2009. Global Media. All rights reserved.

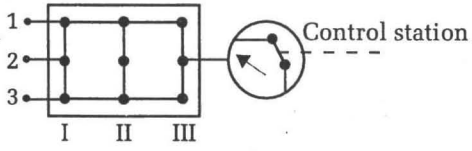
Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Space division switches

- The paths in the circuit are separated from each other spatially.
- Used for both analog/digital networks (originally designed only for analog)

(i) Cross bar switch

- Connects m inputs to n outputs in a grid, using electronic microswitches (transistors at each cross point) – Limitation is number of switches.
- Makes the cross bar huge size (to cover more cross points). This is impractical as well as inefficient since only 25% of the cross points are used at a given time – 75% of the cross points idle.



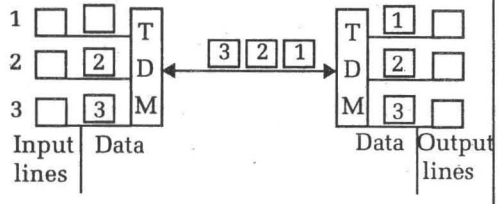
E.g. : If inputs are 1000 and outputs are 800, cross bar required is 800,000

(ii) Multistage switches

- Solution to the above problems are by using multistage switching, where cross bar switches are combined at different stages.

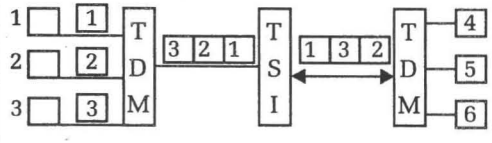
Time division switches

- Slots are divided by time rather than space
- Switching is accomplished using time division multiplexing (TDM)
- TDM is not sufficient. A device known as a Time Slot Interchange (TSI) is required.



Example : No switching without TSI.

If we use TDM only, Data as input will go from input lines 1,2, 3 to the output lines 4, 5, 6 in the same order. eg. Data 1 will reach from 1 to 4; Data 2 will reach from 2 to 5 etc.



Example : No switching without TSI.

In this case if we use TSI, and data is to be transmitted from 1 to 6 and 2 to 4 and 3 to be 5, TSI changes the ordering of the slots based on the desired connections.

Space and time division switching combination

- Space division switching is instantaneous
- Time division switching needs no cross point.

These are the advantages :

- Space division has number of cross points required to make the switching acceptable in terms of blocking.
- Time division creates delays in processing each connection. Each time slot must be stored by the RAM and then retrieved and passed on

These are the disadvantages :

- To take advantages of both type, a third option which is the combination is used.
- Multistage of the sort can be designed as Time-Space-Time (TST), Time-Space-Space-Time (TSST), Space-Time-Time-Space (STTS) or other combinations.

These would optimise :

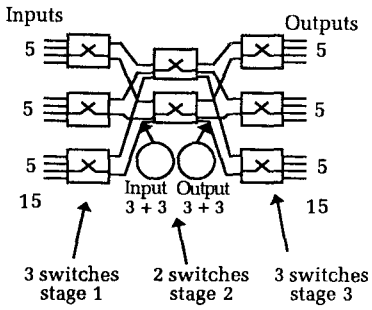
Physically (on the number of cross points)
Temporarily (the amount of delay)

A simple TST is as shown below :

Copyright © 2009. Global Media. All rights reserved.

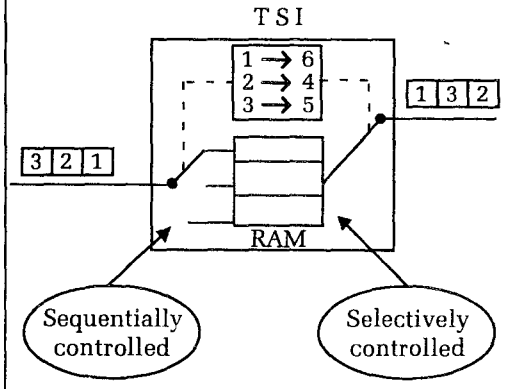
Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

- Devices are linked to switches which are in turn linked to a hierarchy of other switches.
- Designs is based on number of stages and number of switches required in each stage.
- Assumption is middle stages have fewer switches than the 1st and last stages.



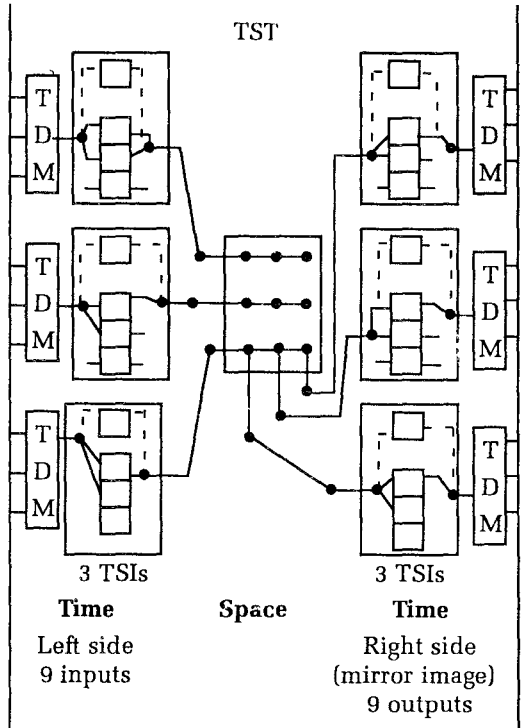
When the demultiplexer separates the slots, it passes then to the proper outputs.

How TSI works?



Time slot interchange

TSI contains a random access memory (RAM) with a number of memory locations. Size of each location is same as the size of a single time slot. Number of locations is the same as the number of inputs. RAM fills up with incoming data from the time slots in the order received. Control will decide the slots order to be sent.



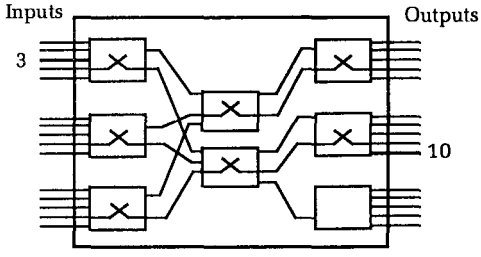
- The result in this case is that the average delays 1/3 of that would result from using one time slot interchange to handle all the 9 inputs.
- The middle stage is a space division switch (cross bars); connects TSI groups together to allow connectivity between all possible input/output pairs.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Multiple paths

A multistage switch can be used for connecting each pair of linked devices providing several options as shown below in the figure 14.5.



(3 connected to 10 similarly 8 can be connected to 11 and so on)

Fig. 14.5 Switching path

A pathway is shown from 3 to 10 in the above figure 14.5. The path uses the lower intermediate switch and that switches centre output live to each the last stage switch connected to line 10.

(i) Number of cross points in a 15 × 15 single stage cross bar switch with 15 × 15 multistage switch if compared.

Single stage switch needs 225 cross points.

Multistage needs :

- Three first stage switches each with 10 cross points (5 × 2) and a total of 30 (5 × 2 × 3) cross points at the 1st Stage.
- Two second stage switches each with 9 cross points (3 × 3) and a total of 18 (3 × 3 × 2) cross points at the 2nd stage.
- Three third stage switches each with 10 cross points (5 × 2) and a total of 30 (5 × 2 × 3) cross points at the 3rd stage.

Total number of cross points 30 + 18 + 30 = 78 one multistage switch at against 225 cross points with a single stage cross bar. (35%).

This savings comes with a cost in the reduction in the number of cross bar. The reduction in the number of cross points results in a phenomenon called blocking during periods of heavy traffic. Blocking refers to time when one input cannot be connected to an output because there is not path available between the two all of the possible intermediate switches are occupied. In a single-stage switch blocking does not occur. There would be always a path because every combination of inputs and outputs has its own switch. Under normal circumstance, blocking is not usually a problem. In countries that can afford it, the number of switches between lines is calculated to make blocking unlikely. The formula for finding the number of switches is based on statistical analysis.

Disadvantages of circuit switching

- Circuit Switching is meant for voice communication. It creates temporary dedicated lines suitable for telephone communication, where once a circuit is established, it remains connected for the duration of the session.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

- It is less well suited to data and other nonconversational transmissions. Non voice transmissions are bursty (data come in spurts with idle gaps between them). Therefore the line is often idle and its facilities unused. Though multiplexing improves line utilisation here it is only effective on the minimum side, unless transmission is predictable and the transmission by each user is at essentially the same rate.
- Another weakness for data transmission is in its data rate. It creates the equivalent of a single cable between two devices and there by assumes a single data rate for both devices, limiting the flexibility and usefulness of a circuit-switched connection for networks interconnecting a variety of digital devices.
- It is inflexible. If a circuit is established, it is the path taken by all parts of the transmission (whether or not it remains the most efficient or available).
- Lastly, it sees all the transmissions as equal. Any request is granted to whatever link is available. With data network transmission, prioritising using is required (e.g. transmission *x* can go any time, but *y* should go immediately – time dependent)

Packet switching

Packet switching overcomes the problems of circuit switching. It is a better solution for data transmission. *Packet switching* is a store and forward data transmission technique where in message are split into small segments called packets (usually 128 bytes). Data are transmitted in discrete units of potentially variable length blocks called packets. The maximum length of the packet is decided by the network. The packets are sent over the network node to node. At each node, the packet is stored briefly and routed afterwards as per the information available in its header. Each packet contains data and also a header with control information. Layer transmissions are broken into multiple packets.

Short messages can be delayed while longer messages are being transmitted. This problem can be minimised in a message switching system by dividing all messages into short packets of fixed length and format and transmitting packets from long messages interspersed with packets from short messages. The store and forward switching centers are responsible for storing the packets from the various messages and transmitting them to their proper next destinations. At the final destination of a message, it must be reassembled from its individual packets. This form of communication known as *'packet switching'* used when very fast communication is required with small computers acting as the *store-and-forward* switching centers.

It is ideal for extensive high speed transmission lines. It breaks up a length block of text into small, fixed bundles of data (generally 128 bytes each) called *packets*. Packet switching are used when lots of data are sent between two points. It is something like sending ten post cards instead of sending one big letter, to accommodate all the matter of ten post cards. Let us take a case where the long letter is not available in the post office and you write only post cards numbering them 1, 2, 3, ... up to 10. So that your friend on receipt of these post cards would join them in the order to get the full matter. This is how the internet works and it is called *packet switched network*.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

Imagine phone calls are not efficient when lots of data are to be sent, and you have to resort to sending by post using the postal service you write the message & put it in an envelope in the post box, giving correct address. The post office takes care of every thing and what you need to do is putting the correct address, so that the envelope reaches the destination. You are not bothered how it goes. In the case of internet also, put the right address to make it to do the rest. It doesn't send directly data from one point to another. It sends it to another computer called *'Router'*. Router sends it to another router closer to the destination. Finally, the data reaches the destination.

Each packet travels independently through the network. Packet of data originating at one source can be routed through different paths in the network, and then may be reassembled into the original message when they reach their destination. Hence this can be resorted to be utilised more fully by more users.

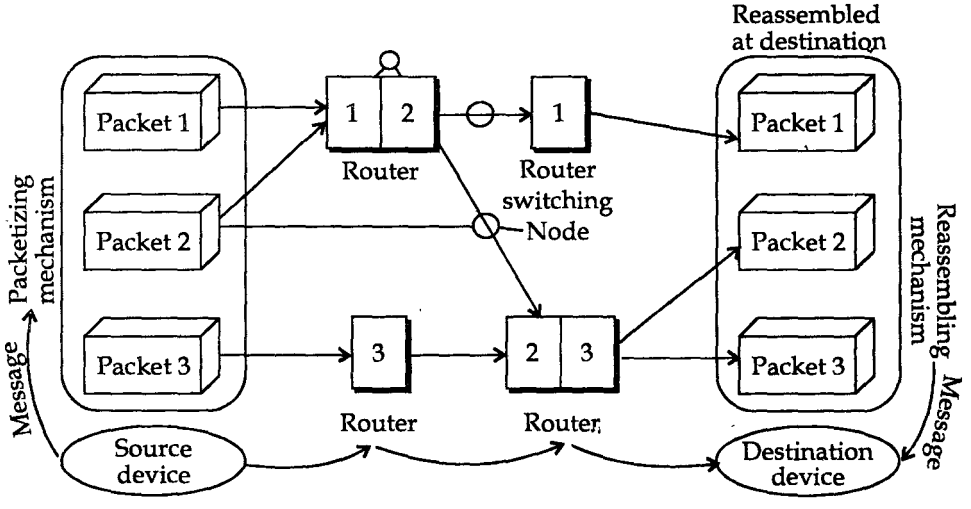


Fig. 14.6 Packet switching (using store and forward method)

Just like post office working, the packets move from router to router and finally reaches the destination.

A packet contains besides the block of data to be sent, the following:

- bits for synchronisation
- link number
- control information
- acknowledgement
- message number
- error checking bytes.
- number of the current packet
- number of the last packet
- destination
- source address

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

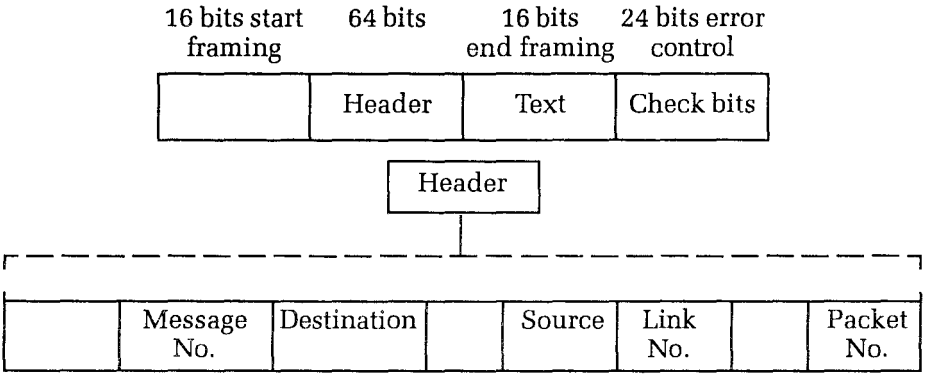


Fig. 14.7 Packet contents

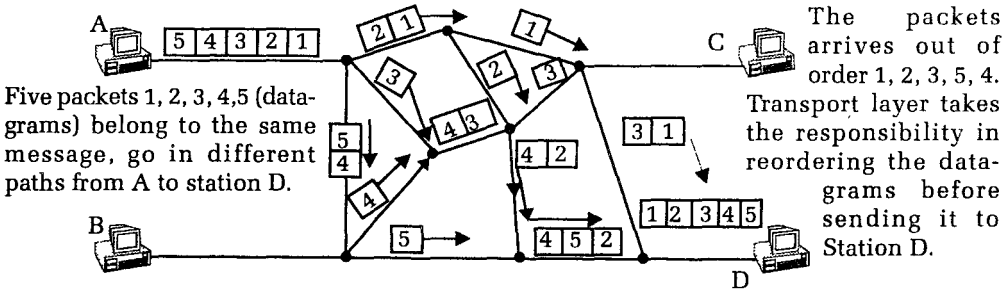
Approaches to packet switching

Two popular approaches are :

- Datagram approach
- Virtual Circuit approach

Datagram approach

- Each packet is treated independently from others.
- Even one packet is just a piece of a multipacket transmission, the network and (network layer functions) treats its as though it existed alone. Packets in this technology are datagrams.



Example of delivering of 5 packets from A to D (Stations)

Fig. 14.8 Data gram approach

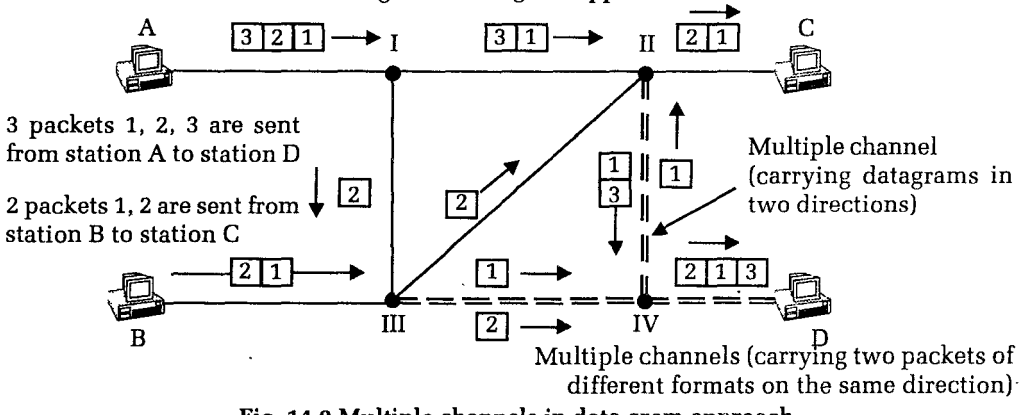


Fig. 14.9 Multiple channels in data gram approach

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

- Multiple channels is capable of carrying datagrams either from several different sources or from one single source simultaneously.
- Packets can be carried simultaneously by either TDM or FDM multiplexing.

Virtual circuit approach

- The relationship between all packets belonging to a message or session is preserved.
- A single route is selected between sender and receiver at the beginning of the session.
- If data are sent, all packets of the transmission travel one after another along that route.

Difference between circuit switching and virtual circuits

- Circuit switching can use multiplexing at the end-user level
- No multiplexing is done at the switches
- Multiplexing at the switches (in the case of virtual circuits)

} circuit switching

Two formats of virtual circuit transmission

SVC (Switched virtual circuit)

- Comparable conceptually to dialup circuit switching.
- Here is a virtual circuit is created whenever it is required and exists only for the duration of the specific exchange.

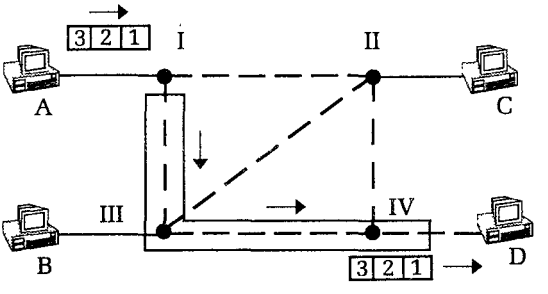


Fig. 14.10 Switched virtual circuit

- Station A to send 3 packets to station D
- Connection is established I to III to IV (Based on A's request)
- Packets are thereafter sent in the same way.
- After the receipt of last packet, if necessary acknowledge, connection is released, virtual circuit ceases to exist .
- Only one single route exists for the duration of transmission though the network could take an alternate route in response to failure or congestion.
- The routes can differ in response to varying network conditions. This is the main difference between SVC and PVC
- SVC allows a Virtual Circuit reliability with a degree of datagram flexibility.

PVC (Permanent virtual circuit)

- These are similar to the leased lines.
- The same virtual circuit is always provided to the same users on a continuous basis.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

- No one else can use it, is always in place.
- Can be used without establishment of the connection and connection termination.

14.3 MESSAGE SWITCHING

Message switching is also known as *store and forward switching*. If one of the devices is engaged, the central switching site stores the incoming message from the sending device (by opening it to disk) and retransmits the message to the destination when the device become free. With modem high speed computers, many data communication networks are able to combine store and forward switching with circuit switching. But circuit switching is attempted first and if the destination is busy, sorting and forwarding is used. This combination offers data communication network users.

- The highest level of throughput
- Used for data communications and has recently available even for voice communications.

AT&T, MCI and several other leading companies now provide a calling service that enables you to leave a message if the phone you are calling is busy. The service continuously tests the destination telephone whenever it becomes free, the service rings the telephone and delivers the stored message.

It is different from packet switching. Here all message packets are received and stored by a central router, which is connected to all the terminals. This central node then routes messages to their addresses. But this method is used where message delays do not matter.

Here, intermediate switching centers on a long communication path are used to store data items in a message format as under :

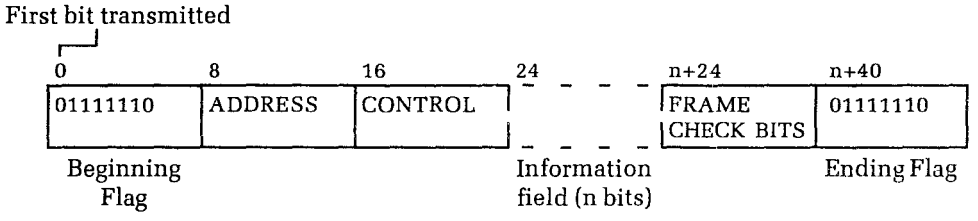


Fig. 14.11 High level data link control format

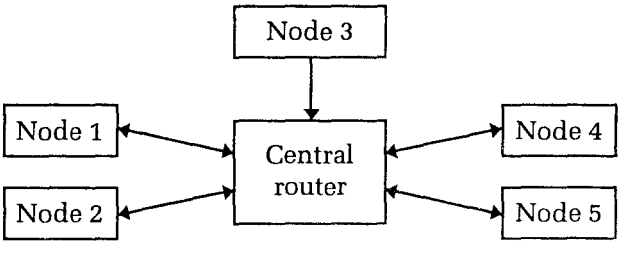


Fig. 14.12 Message switching with central router

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

A node (a special computer with number of disks) receives a message and stores it until the appropriate route is free, then sends it along. In this case, there is no direct link between the sender and the receiver of a transmission. A message is delivered to the node along one path, then routed along another to its destination.

In message switching, the messages are stored and relayed from the secondary stage (disk), whereas in packet switching the packets are stored and forwarded from primary storage (RAM) This was common in 1960s and 1970s. The main we have been to provide high level network services (e.g. Delayed delivery, broadcast) for unintelligent devices, which have been replaced now and hence the type of switch has become uncommon. Further, the delays inherent in the process, as well as the requirements for large capacity storage media at each node, makes it unpopular for direct communication.

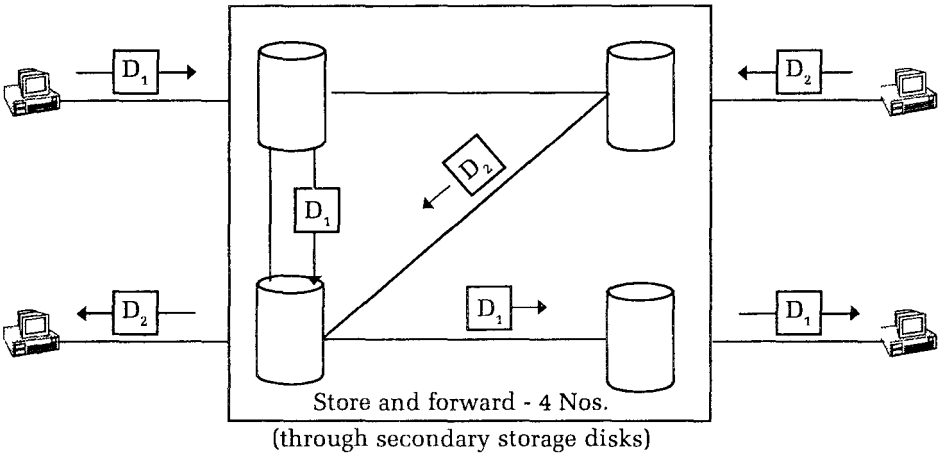


Fig. 14.13 Message switching

14.4 NETWORK LAYER

From the network layer, we achieve connections between physical networks for:

- Establishing
- Managing and
- Terminating

Protocols at the layer provide i) transport routing ii) relaying services between networks, and these are used by protocols of the upper layer of the OSI model.

Two types of protocols supported at the network layer of the OSI model are:

- Connection oriented network services (CONS)
- Connectionless network services (CLNS)

Transmissions can be connectionless or connection oriented at three layers (data link, network and transport) and can still switch between the two states depending on the protocol.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

CONS

- It establishes a virtual circuit for the transmission of data that is active for the entire transmission. All packets belonging to a single transmission are sent, in order, over the same route. It allows a degree of control over the quality of service, otherwise not possible.
- A connection is established between both ends of a transmission – sending and receiving, before data is sent. The sending device transmits a request-to-send packet before transmission commences.

  If the receiver is available, it returns a ready-to- receive packet. This exchange alerts the receiver to expect an entire transmission rather than a single packet. Readiness should be indicated at both ends for data transmission.
- Connection is made; A single path is chosen and maintained for the entire transmission (relevant to connection – oriented services at the transport layer). A transmission is a series of related data units travelling in one direction; handled by both network and transport layers connections for the duration of an entire exchange handled by the session layer (Packet switching allows transmissions to be split into a number of small segments and sent by various routes) If a connection is established the segments are numbered and sent in sequence by a single route one after the other.
- Five general steps followed are :
  (i) sender transmits a connection request packet
  (ii) receiver acknowledges with a connection – confirm packet
  (iii) sender transmits data
  (iv) repeat steps of (iii) ; sender transmits a disconnect – request packet
  (v) receiver acknowledges with a disconnect – confirm packet.

Advantages

- It allows a protocol to include comprehensive sequence, error and flow control.
- Sequential numbering allows the protocol to ensure that all packets make it to the receiver and received in order.
- Packets are identifiable, acknowledged, retransmitted, if required.
- Numbering also allows the use of sliding window for flow control.
- All segments of a transmission must be received and acknowledged before a transmission is considered complete; the virtual circuit can be discarded.
- Packet size – packets follow the same path less protocol control information (PCI) need on subsequent packets.

  E.g. First packet contain explicit addressing information subsequent could be abbreviated to save overhead.

Disadvantages

- Once a connection is established routing flexibility is lost.
- If a link becomes congested or problematic in otherways, subsequent packets do not free themselves to take alternative routes.
- Speed (packets must be checked, acknowledged or retransmitted)
- If complete reliability is unimportant to a particular exchange the extra time required can be wasted.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

CNLS

- Each packet of multipacket transmission is treated as an independent unit.
- Connectionless protocols provide no logical connection (no virtual circuit)
- Sender does not alert the receiver to the coming transmission, it just sends the data.
- The arrival of each datagram at the destination is a separate event, unexpected by the receiver (who may or may not accept it)

  The CNLS process is simpler
- Sender transmits data (can be repeated)

Advantages

- If accountability and reordering can be handled by upper layer protocols (e.g. checksum at the transport layer) a CNLS provides advantages of speed and cost.
- If a particular route becomes congested or breaks down, packets can take alternate routes.
- The various segments of a single transmission can travel by different paths to maximise efficiency.

Disadvantages

- If reliability is essential or if packets must arrive in a specific order, connectionless routing is inadequate.
- Overhead required by each packet, since packets are not transmitted as a stream, each must carry complete PCI making transmission unwieldy.

POINTS TO REMEMBER

- *Switching* is connecting multiple communicate devices to one another in an efficient way. A *switch* is a device connecting multiple communication links together. It is an intermediary hardware/software that links devices together temporarily.
- Three fundamental switching methods are (i) circuit switching (ii) packet switching and (iii) message switching/store and forward switching.
- A *switched network* consists of a series of interlinked nodes called switched. In circuit switching, packets travel from a single device on dedicated links to the destination. Space-division, time-division switches are used.
- In *space division switch*, the paths in the circuit are separated from each other spatially. It is used for both analog and digital networks. Cross bar switch connects m inputs to n outputs in a grid using electronic micro switches. Multistage switches reduce the number of crosspoints needed. Blocking would result. Blocking occurs, if each of the inputs has its own unique path to each of the outputs.
- In *time division switch*, slots are divided by time rather than space. Switching is accomplished using time division - multiplexing (TDM). TDM is not enough. A time slot interchange (TSI) device is needed in addition to TDM. A control

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

unit sends the input to the correct output device. Space–and–time division switches may be combined.

- *Packet switching* overcomes many of the problems found in circuit switching. *Packet switching* is a technique where in messages are split into small segments called packets. (usually 128 bytes). The packets are sent over the network node to node. This is more suited to nonconversational transmission.
- Two popular approaches to packet switching are : Datagram approach and virtual circuit approach. In the *datagram approach*, each packet (datagram) is treated independently from other packets. In the *virtual circuit approach*, all packets of a message or session follow the exact and same route. The two formats implemented by virtual circuit transmission are (i) switched virtual circuit (SVC) and (ii) permanent virtual circuit (PVC)
- Dedicated path is followed by different segments of a message under circuit switching whereas a virtual circuit packet switching the segments follow dedicated channels.
- *Message switching* also known as store and forward switching. Here a node receives a message and stores it until the appropriate route is free, then sends it along. Here there is no direct link between the sender and the receiver of the transmission.

QUESTIONS

1. What do you mean by switching? Explain.
2. What are the three possible switching methods?
3. Explain circuit switching and a circuit switched network.
4. What are circuit switches? Explain.
5. What are folded switches? Explain.
6. What are the two categories of circuit switching?
7. Compare and contrast space division switching and Time division switching.
8. Explain a cross bar switch.
9. Explain space and time division switching combination.
10. What is packet switching? Explain the two popular approaches to packet switching.
11. Compare and contrast datagram approach and virtual circuit approach.
12. Which are the two formats of virtual circuit transmission?
13. Compare and contrast SVC and PVC.
14. What is message switching? Why is it called as store and forward switching?
15. Which are the two types of protocols support at the network layer?
16. Explain CONS.
17. Explain CNLS.
18. Compare and contrast CONS and CNLS.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

19. What are the advantages and disadvantages of CONS and CNLS?
20. In your opinion, Is circuit switching or virtual circuit switching efficient? What are the reasons?

FILL IN THE BLANKS

1. _____ ____ switch connects m inputs to n outputs.
2. _____ network consists of a series of interlinked nodes called switches.
3. In _____ switching, packets from a single device travel on dedicated links to the destination.
4. _____ _____ _____ switching makes all the datagrams of a message follow the same channels.
5. _____ switching is less well suited to data and other non conversational transmission.
6. _____ controls the order of delivery of slot values that are stored in RAM.
7. _____ contains a random access memory with a number of memory locations.
8. _____ _____ Circuit switching, delivery of data is delayed.
9. In _____, each packet of message follows the same path from sender to receiver.
10. In _____ approach, each packet is treated independently from others.
11. In _____ _____ approach, the relationship between all packets belonging to a message or session is preserved.
12. In _____ _____ approach the same virtual circuit is always provided to the same users on a continuous basis.
13. A permanent virtual circuit is similar to the _____ lines.
14. A permanent virtual circuit involves _____ _____.

Answers

1. cross bar
2. Switched
3. circuit
4. Virtual circuit packet
5. packet
6. TSI
7. TSI
8. Time division
9. Virtual approach to packet switching
10. datagram
11. virtual circuit
12. permanent vertical
13. leased
14. data transfer

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-12 19:01:57.

UNIT 4

CHAPTER 15

INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

CHAPTER 16

X.25

CHAPTER 17

FRAME RELAY

CHAPTER 18

ASYNCHRONOUS TRANSFER MODE (ATM)

CHAPTER 19

SYNCHRONOUS OPTICAL NETWORK SONET/SDH

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

15

INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

A communication facility is the medium which carries voice, data or image transmissions from one point to another. Though we find separate communication facilities for the above, technology is evolving toward a single facility that can handle voice, data and image communications. One such is Integrated Services Digital Network (ISDN) and T-carriers is another one; which are the prominent ones. ISDN is an example of circuit switched network, an evolving communications network standard that provides universal end-to-end connectivity over digital lines. ISDN is not available everywhere but it is fast emerging. If ISDN is fully implemented, today's disparate transmission and switching services will be available everywhere internationally via a single set of interface standards. ISDN has been more of a concept than a reliable service in the USA. It is highly popular in California because PACETEL has developed and marketed it well. It is far less popular in New York because NYNEX has shown little interest in it.

ISDN's acceptance has slowed because vendors, common carriers and RBOCs have conflicting interpretations of the ISDN standards. As a worldwide telecommunications network standard, ISDN will draw a wide variety of consumer services into a single access package. An ISDN combines voice, video and data over the same digital circuit. It allows users to send the above including fascimile etc. and so on over the same wires and to have ready access to digital services. Equipment from different vendors which conforms to the ISDN standard won't necessarily work together or with a specific RBOC ISDN line. Skeptics say that ISDN actually stands for 'I Still don't know' or "It still does nothing". In 1992, RBOCs and other interexchange carriers in the USA developed National ISDN –

Copyright © 2009. Global Media. All rights reserved.

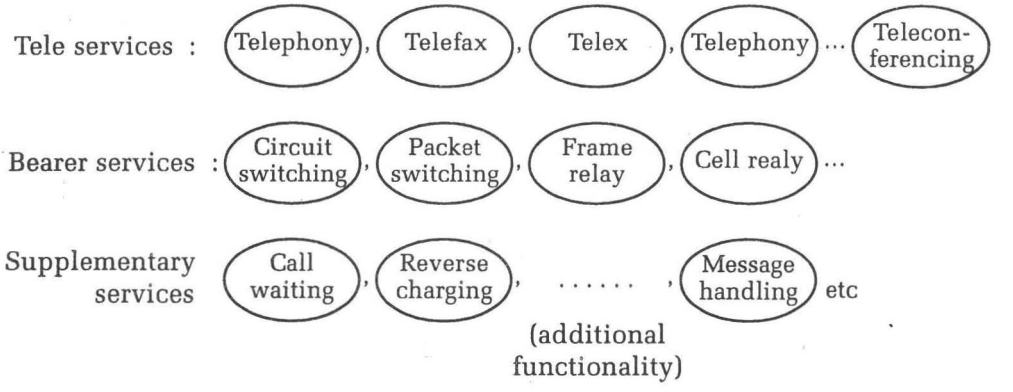
Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

1 (N–1) and ISDN–2 (N–2) to specify exactly how ISDN services will be provided in the USA and Canada. As N_1 and N_2 have come up, it is hoped that many of the current standardisation problems will disappear.

15.1 SERVICES

ISDN is to provide fully integrated digital services to users, which falls into three categories :

- Bearer services – Provide the means to transfer voice, data and video information between users without the network manipulating the content of that information.
- Tele services – In teleservicing, the network may change or process the contents of the data. These services correspond to 4–7 layers of the OSI model.
- Supplementary services – These are those services that provide additional functionality to the above two types of services e.g. reverse charging, call waiting, message handling, etc.



Bearer services belong to the first three layers of the OSI model and are well defined in the ISDN standard.

Tele services relay on the facilities of the bearer services and are designed to accommodate complex user needs without the user having to be aware of the details of the processes.

As we are all aware, telecommunication networks were fully analog in the earlier days and were reserved for the transmission of analog information in the form of voice. Even the telephone company's central office which were connected to the subscriber's handset from the local loop were analog.

Voice and data communication over an Analog network

After the digital processing was introduced, subscribers started exchanging data as well as voice and hence modems were developed to allow digital exchanges over existing analog lines.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

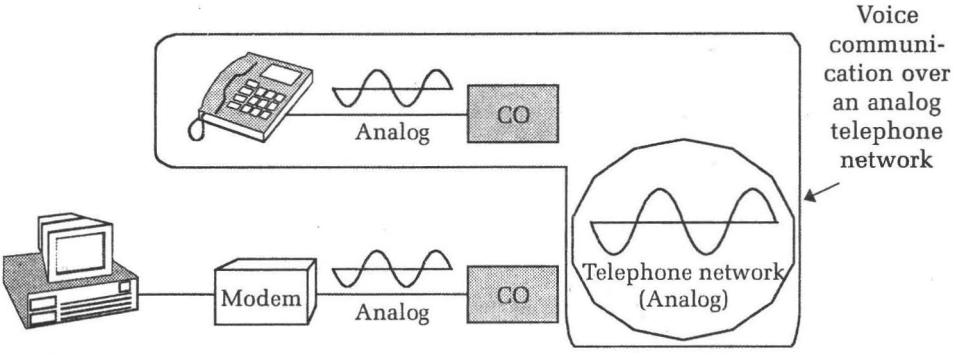


Fig. 15.1 Voice and data communication over an analog telephone network

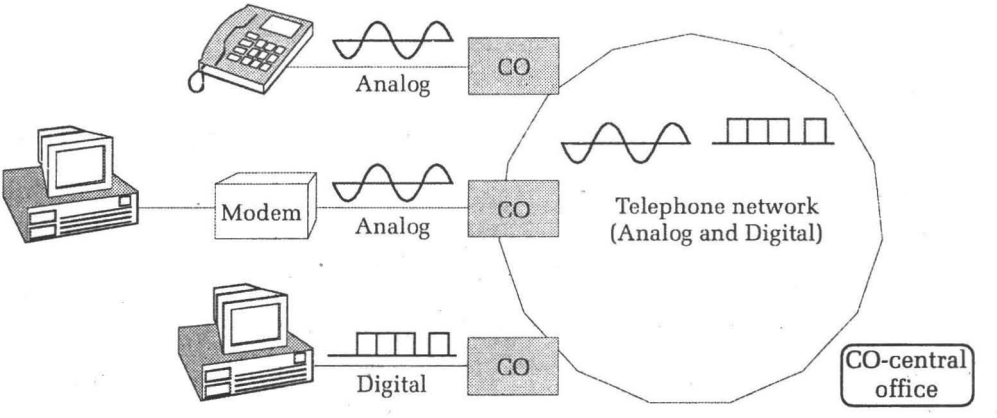


Fig. 15.2 Analog and Digital services over the telephone network.

Telephone companies started adding digital technologies, while continuing their analog services to their customers. The types of customers identified are :

(i) Traditional customers (using analog loops)

(ii) Customers using analog facilities to transmit digital information (via modem)

(iii) Customers using digital services to transmit digital information.

Group (i) is still prominent even today and hence most of the services rendered are analog.

Integrated digital network (IDN)

Next stage came when customers needed access to a variety of net works, specially for packet and circuit switched networks. This made the telephone companies to create IDNs to meet the customers needs. An *IDN* is a combination of networks available for different purposes. Digital pipes usage was the means to access these networks, which are time multiplexed channels sharing very high speed path. Customers can use their local loops to transmit both voice and data to their telephone company's central office (Telco). This office then diverts these calls to the appropriate network through the digital pipes. Digital local loop services covering switched/56, DDS and DSS are presently available. However, many subscribers even today continue to use analog loops.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

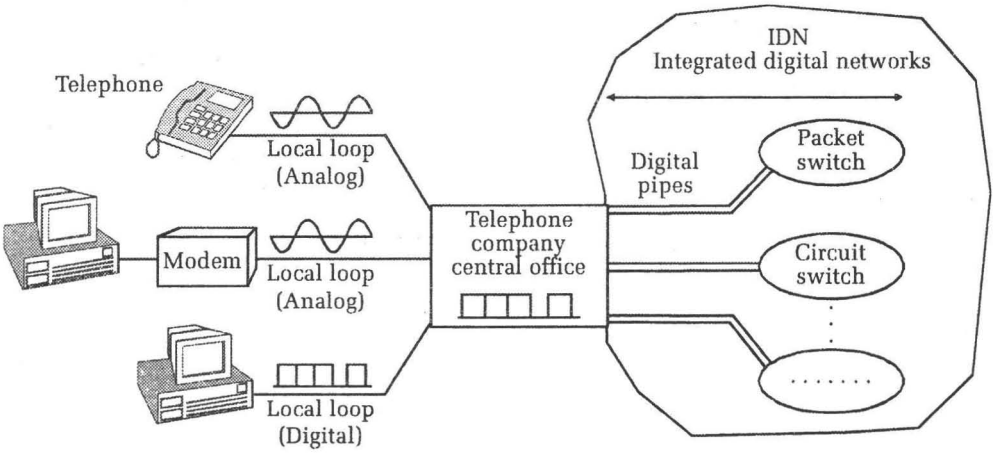


Fig. 15.3 IDN

Integrated services digital network (ISDN)

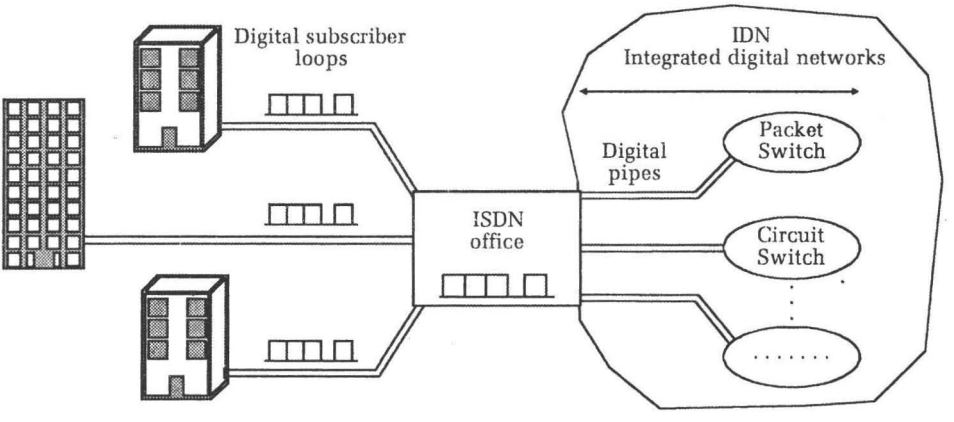


Fig. 15.4 ISDN

15.2 ISDN

- Integrates customer services with the IDN.
- Fully digital services are more efficient and flexible than analog services.
- Replace the analog local loops with digital subscriber loops to gain maximum from IDN.
- Voice transmissions can be digitised at the source to remove the final need for analog carriers. With this, data, voice, image, fascimile etc can be sent on any digital network.
- With ISDN, all customer services will become digital (no analog). Flexibility offered with this new technology will ensure customer services on demand.
- ISDN allows all communication connections in a home/building via a single interface.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

- Digital pipes are used to each of the users to link to the central office. Pipes are of different capacities, allows different rates of transmission, supports different subscriber needs.

15.3 ACCESS TO THE ISDN

As said already digital pipes are used between subscribers and the ISDN office (subscriber loops). These are organised into multiple channels of different sizes. The three channel types under ISDN standards (each with a different transmission rate) are : (1) Bearer channels (B) 64Kbps (ii) Data (D) 16,64 Kbps (iii) Hybrid (H) 384, 1536, 1920 Kbps.

CHANNELS	
B Channel (Bearer Channel) • 64 Kbps rate • Basic user channel • Carry any type of digital information in full duplex mode upto 64 Kbps (carries digital data, digitised voice, other low data information). • Several transmissions can be accomodated immediately if the signals are multiplexed first. • Multiplexed transmissions must be destined for a single recipient. • B channel carries transmissions end to end. • Not designed to demultiplex a stream midway in order to separate and divert transmissions to more than one user. • Also called as digital transmission channels • Handles digitised voice, data and image transmissions. • Code must be installed between the telephone and ISDN connection. **H–Channels (Hybrid Channels)** • Data rates of 384 Kbps (H0) • 1536 Kbps (H11) • 1920 Kbps (H12) • Rates suit H Channels for high data rate applications such as video tele-conferencing etc.	**D Channels (Data Channels)** • 16 or 64 Kbps rate (on the needs of the user) • It is to carry control signalling for the B channels (though Data is named as the function) • All transmission protocols hither to discussed use in-channel signalling. Control information is carried by the same channel that carries the message data (like call establishment, ringing, call interrupt, synchronisation). ISDN separates control signals on to the D channel. A D channel carries the control signalling for all of the channels in a given path (Method is common channel signalling). • Subscriber uses the D channel to connect the network and to secure a B channel connection. • Further uses the B channel to send actual data to another user. • A given subscriber loop use the same D channel for signalling, but each sends data over a B channel dedicated to a single exchange for that duration. • D channel acts, like a telephone operator between the user and network in the network layer. • D channel less common uses include : – Low data transfer – Applications in telemetry and alarm transmission. • Used for control messages acknowledgments, call setup, termination and other functions such as automatic number identification.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Two types of ISDN services are :

(i) Basic rate interface (BRI) or Basic Access Service or 2B + D

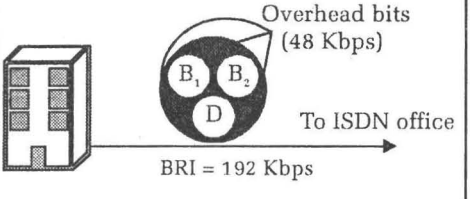
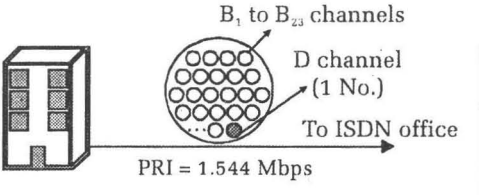
(Two B channels+ 1D channel)

The advantage of BRI is that it can be installed in almost any existing telephone location without adding new cables. It uses the existing two pairs or twisted pair wires. The only changes are the end connections at the customer's location and at the telephone companies switching office.

(ii) Primary Rate Interface or Primary Access Service or 23B + ID

(Twenty three B channels +1D channel)

- Offered to commercial customers who want to hook upto their PBXs or LANs.
- Consists of 23 nos of 64 Kbps B channels + one 64 Kbps D channel, that is same capacity as T–1 circuit (1.544 Mbps). In Europe, PRI is defined as 30 B channels plus one D–channel (Interconnection between USA and Europe is difficult) with a capacity of 2.048 Mbps – The capacity of an E–1 line.
- Interconnection for BRI service to an organisation involves a network termination box at the customer's site.
- Users get a single local loop that carry 144 Kbps between their premises and local telephone company end office. Signals are then combined for transmission over the IXC to the telephone company end office at the transmissions destination.
- Information is next sent over another single access line to the receiving site, where it enters a network termination box and it is distributed to the appropriate computer, terminal or telephone.

BRI (Basic rate interface)	PRI (Primary rate interface)
• Digital pipe of 192 Kbps consisting of two B channels and on 16 Kbps D channel (2B+D)	• Digital pipe of 1.544 Mbps with 23 channels and one 64 Kbps D channel.
	
$(B_1 + B_2 + D = 64 + 64 + 16 + 48 = 0192)$ [48 is the overhead]	$[23 \times 64 + 1 \times 64 = (B_1 + B_2 + \ldots B_{23} + D)$ $+ 8$ over head $= 1544]$
• BRI service is like a large pipe containing three smaller pipes (2B+1D). The remainder space inside the large pipe carries the overhead bits. • BRI could support only a maximum of 2B+1D • 192 Kbps used to carry a single signal (using in channel signalling)	• PRI service is like a large pipe containing 24 smaller pipes (23 for B and 1 for D channels) remainder space is for the overhead bits required for the operation (D channel is shown in shaded) • PRI could support a maximum of 23 B channels and 1 D channel (23 B + 1D)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

• Designed to meet the needs of residential and small office customers. • No need to replace the existing local – loop cable. • Same twisted pair local loop which delivers analog transmission can be used for digital. • Occasionally, some conditioning of the line is needed.	• One PRI can provide full duplex transmission between as many as 23 source and receiving nodes. • Individual transmissions are collected from their sources and multiplexed onto a single path (digital subscriber line) for sending to the ISDN office. • 1.544 Mbps of a PRI can be divided in many ways to meet the requirements of a number of users. • Capacity of the PRI digital pipe is exactly the same as the capacity of the T–1 line used to support the North American DS–1 telephone service. • The other channel combinations for specialised transmission needs supported by the PRI standard are :3H0 + D, 4H0 + D, H12 + D.

Functional grouping

In ISDN standard, the user access the services of the BRI or PRI based on the functional duties and collected in functional groupings, which are best suited to their needs. ISDN does'nt speed out implementation but only tells the functional behaviour of each group.

Each functional grouping is a model that can be implemented using devices, or equipment chosen by the user/subscriber. Groupings used at the subscriber's premises include :

(i) Network terminations (NT1) and (NT2) – Types 1 and 2
(ii) Terminal equipment (TE1) and (TE2) – Types 1 and 2
(iii) Terminal adapters.

(ii) Terminal equipment 1 (TE1)

- Terminal equipment used by ISDN standard mean the same as DTE in other protocols.
- Refers to digital subscriber equipment.
- TE1 is any device that supports the ISDN standards e.g. Digital telephones, Integrated voice/data terminals and digital fascimiles.

Terminal equipment 2 TE2

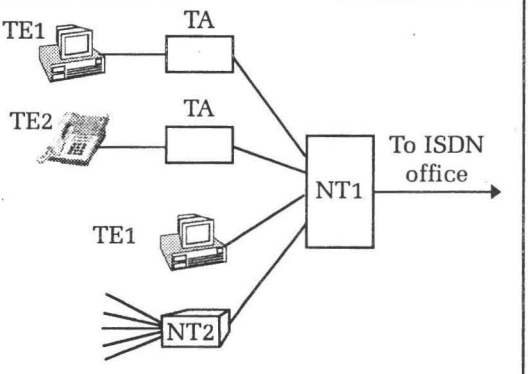
- ISDN standard defines a second level of terminal equipment (TE2) to provide backward compatibility with a customer's existing equipment.
- This is any Non-ISDN device, eg. terminal, work station, host computer, regular telephone.
- TE2 devices are not immediately compatible with an ISDN network; can be used with another device called a terminal adapter.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Terminal adapter (TA)

- Converts information received in Non–ISDN format from a TE2 into a format capable of being carried by the ISDN.

NT1 (Network termination 1)	NT2 (Network termination 2)
• NT1 device controls the physical and electrical termination of the ISDN at the users premises; connects the user's internal system to the digital subscriber loop. • Comparable to those defined for the OSI physical larger. • Ref. functional grouping figure 15.5 An NT1 organises the data streams from a connected subscriber into frames which can be sent over the digital pipe; It translates the frames received from the network into a format usable by the subscribers devices. • It performs the basic multiplexing functions of byte interleaving (It is not a multiplexer) • It synchronises the data stream with the frame building process; multiplexing occurs automatically (this mechanism is implicit multiplexing or multiplexing that occurs as part of another process in this case, frame building) • NT1 can result in an interleaved signal is by analog (similar to two belts used in a manufacturing plant, one for the product, other for the empty crate on which the product falls; packaging is done after this). Timings should match properly (timing of the two belts, must be controlled to keep the synchronizations accurate). Still discrepancies can result in product sending in the wrong box or missing the boxes etc. In the same way, NT1 synchronises the timing of the contributing data streams to the building of the outgoing frames so that bytes are interleaved without the need for multiplexing devices.	 **Fig. 15.5 Functional Grouping** • NT 2 device performs functions of the physical, data link and network layers of the OSI model (layers 1, 2, 3) • Provide multiplexing (layer1), flow control (layer 2), packetising (layer 3) • Provides intermediate signal processing between data generating devices and NT1. NT1 is still requires to provide a physical interface to the network. • Point to point connection is needed between a NT1 & NT2. • Used primarily to interface between a multiuser system and an NT1 in a PRI. • Can be implemented by a variety of equipment bytes eg. digital PBX can be on NT2. • Coordinates transmissions from a number of incoming links (user phone lines) multiplexes them to make them transmittable by an NT1. A LAN can also function as NT2. • If PRI carries signals from multiple devices, those signals are to be multiplexed in a separate process provided by the NT2 before the composite signal passes to the NT 1 for transmission to the network– known as *explicit multiplexing*. E.g. Digital PBX – is NT2 with explicit multiplexing.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Reference point

This refers to the interface between a TE_2 and TA in ISDN, represented by R. It refers to the lable used to identify individual interfaces between two elements of an ISDN installation. It defines the connections between the equipments. How two network elements must be connected? What is the format of the traffic between them? is defined. Reference points are R, S, T and U (other reference points define functions within the ISDN)

R – connection between a TE_2 and TA; S–Connection between a TE_1 or TA and an NT1 or NT2 (if present); T– Interface between NT2 and NT1, U defines the interface between NT1 and ISDN office.

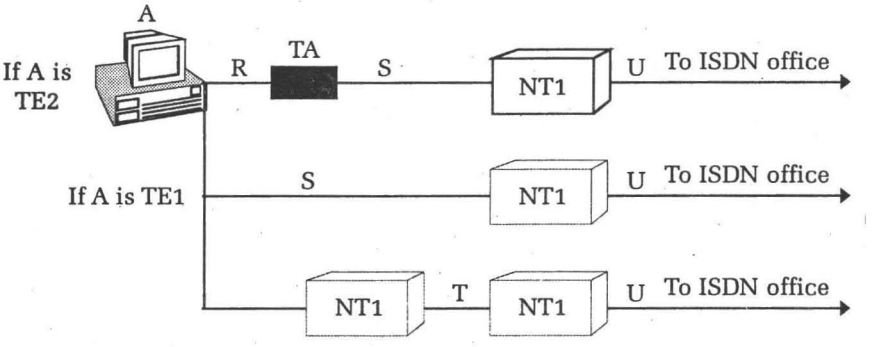


Fig. 15.6 Reference points

15.4 ISDN LAYERS

The question is to how to integrate the simple seven layer architecture specified by the OSI to the ISDN. Further, ISDN includes two different channels (B and D) with different functionalities. The two channels B and D are for different purposes (i) User to user communication (Information exchange) (ii) D channels are predominantly for user to network signalling.

Subscriber uses → D channel for connecting to the network
Subscriber uses → B channel to send information to another user.

The above functions need different protocols from each other at many of the OSI layers. ISDN also differs from the OSI standards in its management needs. ISDN's primary consideration is global integration. It is also to be noted that a great deal of management is required in order to maintain the flexibility required to keep the network truly integrated using public services.

Considering all the above points ITU–T has come out with an expanded model of the ISDN layers.

Instead of the single seven–layer architecture like the OSI, ISI is defined in three separate plans :

- The user plane – defines the functionality of the B and H channels (user to user connection)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

- The control plane – defines the functionality of the D channel (used for signalling) (when used for subscriber data, D channel is defined on the user plane)
- The management plane – It encompasses both the above planes (used for managing the whole network).

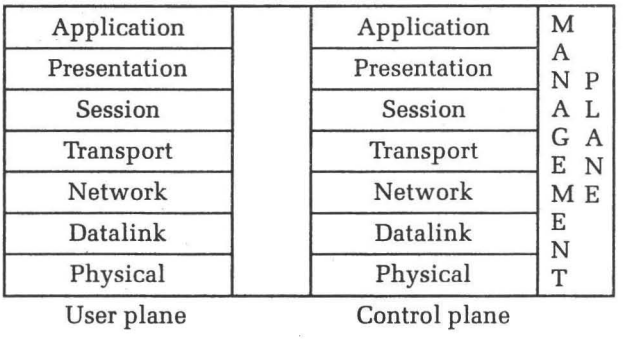


Fig. 15.7 ISDN Layers

All the three planes are further divided into seven layers, which corresponds to the OSI model.

A simplified version of the ISDN architecture for the user and control planes is shown in figure 15.7. We can make a number of assumptions for simplifying the model for the purposes of discussion.

- Subscriber uses the D channel only for signaling (when D channel is used for data, it behaves like a B channel). Eventually D channels will be used for services like telemetry (the protocols that makes these services possible are still under study).
- D channel is used primarily for user to network signalling (Functions are therefore confined to first 3 layers. Layers 4 to 7 are concerned with end to end user signalling, use other ISDN protocols like SS7).

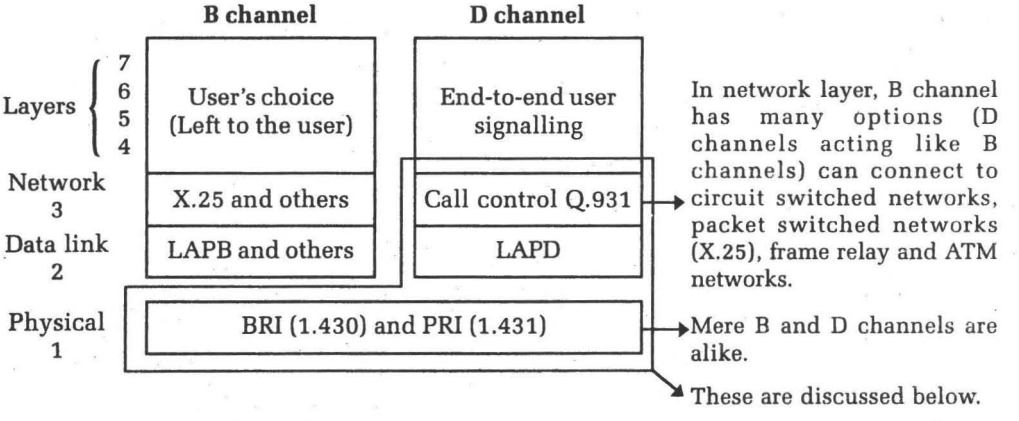


Fig. 15.8 Simplified version of the ISDN structure

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Physical layer

ISDN physical layer specifications are defined by ITU–T standards

- 1.430 for BRI access.
- 1.431 for PRI access.

All aspects of BRI and PRI are defined. The important ones are :

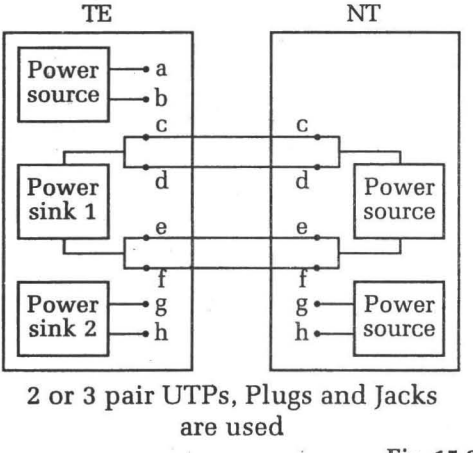
- Mechanical and electrical specifications of interfaces R, S, T and U
- Encoding
- Multiplexing channels (to make them carriable by BRI and PRI digital pipes)
- Power supply.

Specifications for BRI

BRI consists of 2B + 1D channels A subscriber connects to the BRI using R, S and U interfaces. Refer figure 15.9 Reference points.

(i) R interface is not defined by the ISDN. Instead, EIA standards are used eg. EIA–232, EIA–449 or EIA–530 or any of the V or X series standards (X.21)

(ii) S interface – Here, ITU–T specifies the ISO standard, ISO 8887. The standard calls for four, six or eight wire connections (minimum 4 wires are necessary to support full duplex communication for every B or D channel.



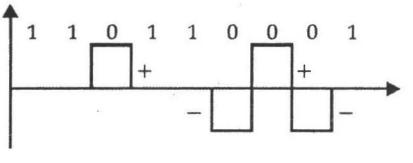
	TE	NT
a	Power source 3	Power sink 3
b	Power source 3	Power sink 3
c	Transmit	Receive
d	Receive	Transmit
e	Receive	Transmit
f	Transmit	Receive
g	Power link 2	Power source 2
h	Power sink 1	Power source 2

Fig. 15.9 Reference points

The individual wires in the S interface connection are organised according to the table shown above.

Encoding : U Interface

ISDN signal encoding is pseudo-ternary. A version of Bipolar AMI with the 0 and 1 levels are reversed.



1 is NO voltage. 0s are alternatively positive and negative voltages.

The 0s are alternatively positive and negative.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

For U interface digital subscriber of local loop, the ITU–T specifies a single pair twisted cable in each direction. Encoding for this interface uses a mechanism known as 2BIQ (2 Binary, 1 Quaternary). 2BIQ uses four voltage levels instead of two. Two bits are represented at each level rather than one thus lowering the baud rate and to use more efficiently the available bandwidth. The voltage levels representing the dibits are 00, 01, 10 and 11 volts.

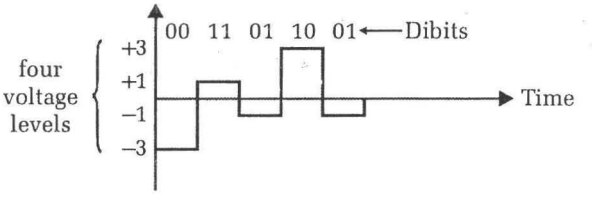


Fig. 15.10 2BIQ encoding

BRI Frame

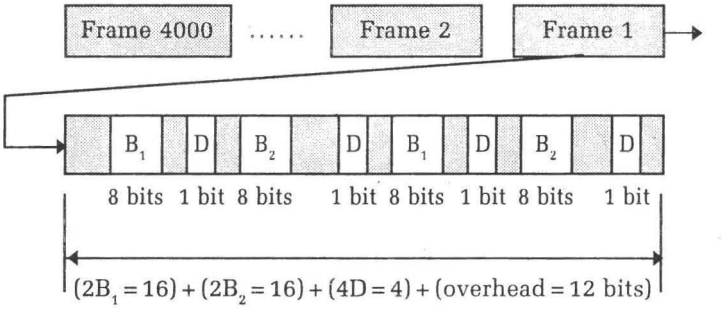


Fig. 15.11 BRI Frame

BRI = 4000 frames/s = 4000 ×48 bits per frame = 192 Kbps.

Note:Each B is sampled twice during each frame (8 bits/sample) = 16 ×2

Each D channel is sampled four times during each frame (1 bit/sample) = 4

The hatched portion is the balance of the frame reserved for overhead = 12

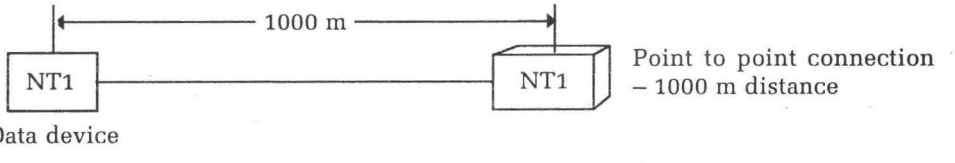
48 bits

- To create a longer frame, B and D channels are sampled number of times and to make it a precise match for ATM cell.

Connection and Topology

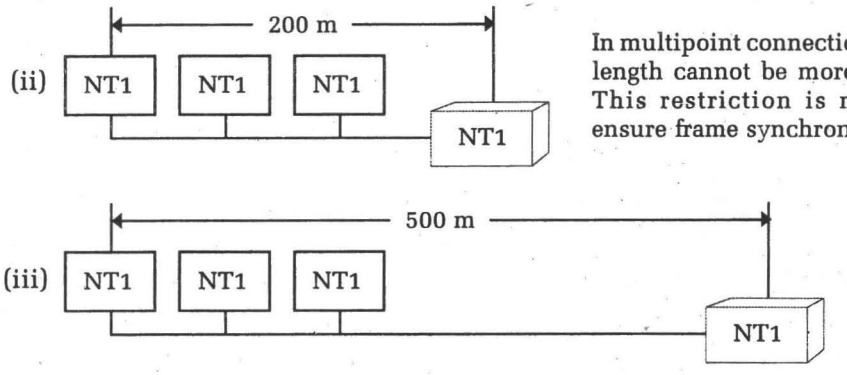
- BRI services is supported by either a bus or start topology.
- The choice of topology for a BRI is the distance of data devices from NT1.

(i)



Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.



In multipoint connection, maximum length cannot be more than 200m. This restriction is necessary to ensure frame synchronisation.

Fig. 15.12 Connection & Topology

NTI is to interleave the outputs of connected devices as part of the process of frame building. The results of this implicit multiplexing are evident in the structure of the frame. To make this possible, the frame building functions of the NT, must be timed to coordinate precisely with the data dumps of the connected devices. If the synchronisation between the frame and devices is off, data dumped by one device can end up in a part of the frame devoted to data from another device, or to another kind of information altogether. Unavoidable propagation delays over distance can result in a shifted frame. Further if the distance between the first and last device on a link is great, data collection timing can deteriorate to the point where much of the frame becomes unusable.

The link distance between the devices is made limited to ensure frame accuracy for multiple link and limit the impact of timing shifts between the data units dumped by each device. The total length of the link is restricted to 200m. If the devices are clustered at the end of the link at the other end of the NT1, the length of the link could be extended to 500 m. (Fig. 15.12 (iii))

Clustering the devices would mean that propagation delays would impact the data from all devices almost equally, allowing the relationships between the data units to remain predictable for 500m.

If only one device is attached to a link, NT1 does not need to distinguish between the data of different devices. Greater timing distortions can be tolerated. Star topology links can be as long as 1000 m. Nearly an eight devices can be connected to an NT1. Only two can access the B channels at one time, one exchange per channel. Every device can contend for access to the D channel. D channels use a mechanism like CSMA to control access. After the device accesses to the D channel, it can request a B channel; if available the connection i made by the D channel and the user may then send data.

PRI Physical layer specifications

- PRI consists of 23 B and 1 D channels
- Interfaces with PRI are R, S , T, and U (Refer figure 15.6, Reference points)
- R and S standards are the same as those of BRI
- T standard is same to the S standard but with the substitution of B8ZS encoding.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

- U interface is the same for both standards (PRI rate is 1.544 Mbps instead of 192 Kbps).
- 1.544 Mbps allows the PRI to be implemented using T–1 specifications (Already discussed in chapter 8)

PRI frame

- B and D channels are time multiplexed using synchronous TM for creating a PRI frame .
- Frame format is identical to T–1 lines

  PRI = 64 × (B1 to B23) + 64D +8 overhead

  = 8000 frames/s = 8000 × 193 bits/frame = 1.544 Mbps

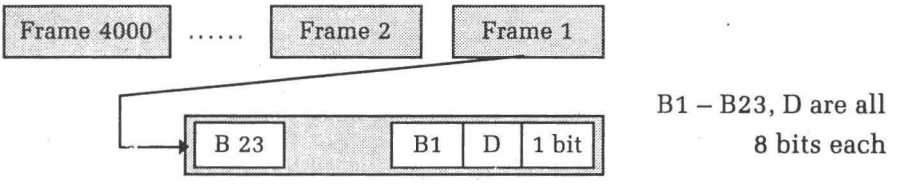


Fig. 15.13 PRI Frame

- PRI frame samples each channel including the D channel, only once per frame.

Connection and Topology

- Linking data generating devices to an NT2 can be the same similar to device-to - NT1 links in the BRI or they can differ.
- Specific implementation depends on the application
- If NT2 is a LAN, its topology depends on the LAN being used.
- If NT 2 is PBX, its topology depends on the PBX being used etc.

  The link from NT2 to NT1 is always point to point.

Data link layer

As shown in figure ISDN layers for B and D channels, these channels use different data link protocols.

- B channels use LAPB protocol
- D channel uses link access procedure for D channel (LAPD)

LAPD is HDLC with few modifications.

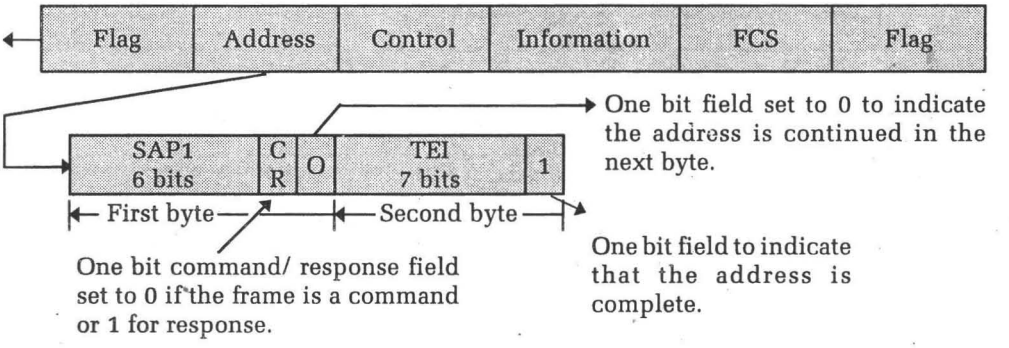
- LAPD can be used in either unacknowledged, without sequence numbering or acknowledged with sequence numbering. The unacknowledged format is used rare. In general LAPD and HDLC are similar.
- Addressing (LAPD addressing is explained below)

LAPD addressing

The LAPD address is given below :

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.



SAPI – Service Access Point Identifier (6 bits)

TEI – Terminal Equipment identifier (7 bits)

Fig. 15.14 LAPD Address field

SAPI Field (6 bits)

- Identifies the type of upper layer service (network layer) using the frame.
- Indicates the intended use of the D channel.
- Defined upto 64 different service access points (As on date, four of the possible bit combinations assigned).
  - 000000 call control for network layer (signalling use of D channel)
  - 000001 call control for upper layer (end-to-end signalling); not yet in use
  - 010000 Packet communication (Data use of D channel)
  - 111111 Management

TEI field (7 bits)

- Can identify up to 128 different TEs
- Unique address of TE

Network layer

- Soon after the connection is established by the D channel, the B channel sends data uing circuit switching X.25 or other similar protocols.
- The network layer functions of the D channel are defined by ITU–TQ .931 standard
- The network layer packet is called a message.

Message Type (1 byte field)

- Identifies the purpose of the message.
- Message Types — Call establishment messages
  — Call information messages
  — Call clearing messages
  — Miscellaneous messages

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

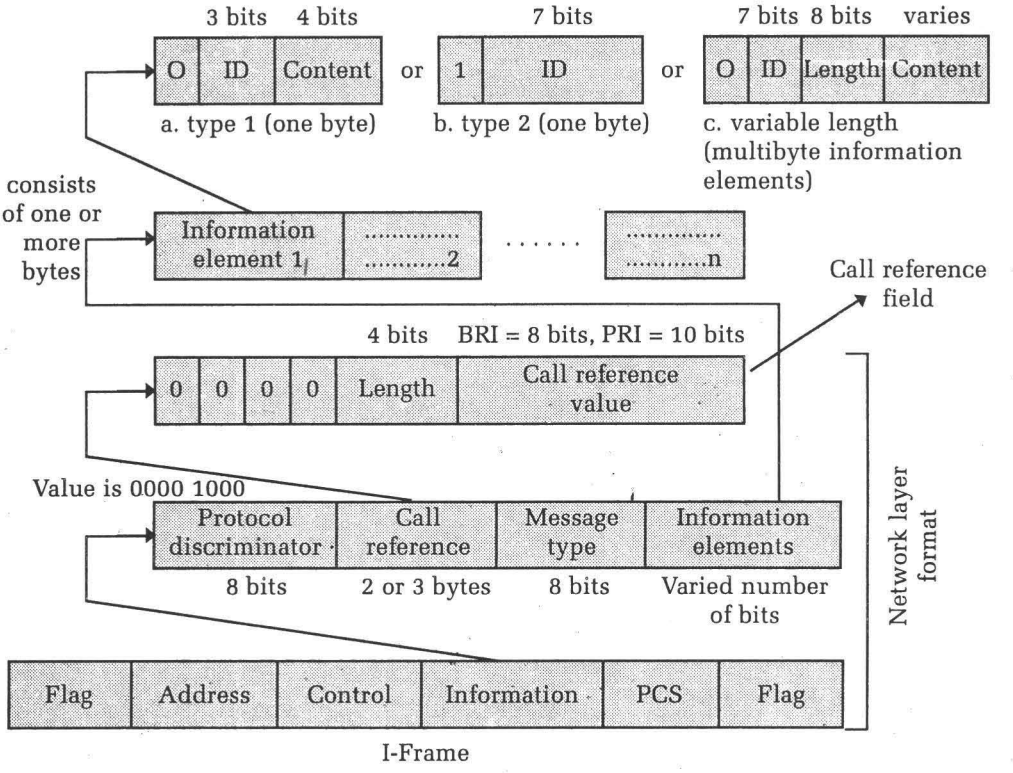


Fig. 15.15 Network layer format

(i) Call establishment messages

- Setup : Calling user sends to the network or network to the called user to initiate a call.
- Setup : Acknowledgment - called user sends this to the network or network to the calling user to indicate that the setup has been received. Message does not mean that a connection is in place merely that the desired process has begun.
- Connect : sent by called user to the network or by the network to the calling user to indicate acceptance of the call.
- Connect acknowledgment : Sent by network to the called user to say that the desired connection has been awarded.
- Progress : Network sends to the called user to indicate that the call establishment in progress. Works as a 'Please stand by' request in case the call establishment process wants more time.
- Alerting : Called user sends to the network or by the network to the calling user to indicate that the call user alert – ringing has been initiated.
- Call processing : Sent by the called user to the network or by the network to the calling user; indicates that the request call establishment has been initiated; no more information needed.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

(ii) Call clearing messages

- Resume : Sent by a user to the network, requests that a suspended call be resumed.
- Resume acknowledgment : Sent by the networks to the user; To acknowledge a request to resume the call.
- Suspend : Sent by a user; to request that the network suspend a call.
- Suspend acknowledgment : Sent by the network to the user; to acknowledge the requested suspension of the call.
- Suspend reject : Sent by the network to the user to reject the requested suspension.
- User information : Sent by a user to the network; to be delivered to the remote user, Message allows the user to send information using out-of-channel signalling.

(iii) Call clearing charges

- Disconnect; Sent by the calling user to the network or by the network to the called user; to clear the end-to-end connection (termination)
- Release : sent by a user or network; to indicate the intention to disconnect and release the channel.
- Release complete : Sent by a user or network; to indicate the intention to disconnect and release the channel.
- Release complete : Sent by a user or network; to show that the channel has been released.

(iv) Miscellaneous

- Other messages carry information defined in the protocols of specific services.
- Not used in routine communication

An information elements field carries specific details about the connection required for call establishment eg. Address of the sender/receiver, routing information types of network that is desired for the B channel exchange (circuit switched, X. 25 ATM or frame relay)

Addressing in ISDN

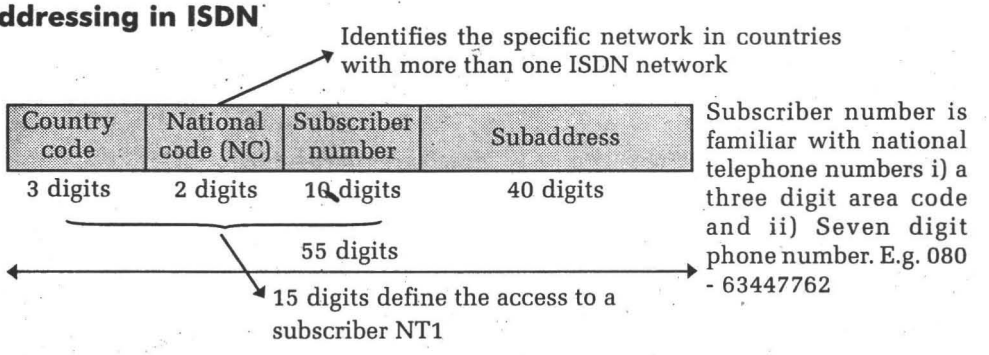


Fig. 15.16 Addressing in ISDN

Note : NT_1 may have multiple devices connected to it.

- Either directly or
- Indirectly through an NT2

} Each device is identified by a subscriber (up to 40 digits)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Broad band ISDN (B–ISDN)

- It is a switched version of SONET
- Not widely available
- Has potential to change the future of high speed networking.
- ISDN was designed in the initial stages for data rates of 64 Kbps to 1.544 Mbps sufficient to handle all existing transmission needs at that time. The telecommunications networks advanced and its applications increased. The rates provided were found inadequate to support recent / new applications. The original bandwidths were also narrow to carry the large numbers of concurrent signals produced by the developing industry of digital service providers.

Applications	Bit rates
Telex – Text	100 bps to 1 Mbps
Voice – Hifi	5 Kbps – 4 Mbps
Videophone – Video conference –TV–HDTV	50Kbps – 10 Gbps
File transfer	1 Kbps–100 Mbps
Fax – CAD/CAM	10 Kbps – 5 Mbps
Transaction	1 Kbps – 50 Kbps

BRI capacity is 192 Kbps

PRI capacity is 1.544 Mbps

Figures shown in rectangles are beyond the capacities of BRI and PRI

To meet the next generation of technology an extension of ISDN called B – ISDN is introduced. The original ISDN is known as Narrow band ISDN (N–ISDN)

- B–ISDN provides subscribers to the network with data rates in the range of 600 Mbps (400 times faster than the PSI rate). Technology is found to support higher rates but is not yet implemented or standardised.

Telephone system $\xrightarrow{\text{evolution}}$ Narrow band ISDN $\xrightarrow{\text{evolution}}$ Broad band ISDN (alters entire aspects of communication)

- B–ISDN is based on a change from metal cable to fiber optic cable at all levels of telecommunications.

- B–ISDN services are
  - Interactive services
    - Conversational
    - Messaging
    - Retrieval
    - Require two way exchanges between two subscribers or between a subscriber and a service provider.
  - Distributive Services
    - without user control
    - with user control
    - Uni-directional services from a provider to subscribers without the subscriber having to transmit a request each time a service is desired.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Interactive	Distributive
(i) *Conversational services :* Telephone calls that support real time exchanges (as supposed to store and forward) – used in telephony, video telephony, video conferencing, data transfer etc.) (ii) *Messaging services :* Are store and forward exchanges. These are bidirectional (can use them at the same time by all parties in an exchange. Actual exchange do not occur in real time subscriber requesting for information from another may have to wait for answer, though both parties are available at the same time. Eg. Voice mail, data mail, videomail. (iii) *Retrieval services :* To retrieve information from a central source (Information centre). Services are like libraries – allow public access; allow users to retrieve information on demand. Information is not distributed unless asked eg. Videotex allows subscribers to select video data from an on-line library. Service is bidirectional since it requires action by both (requester and the provider).	Without user control: Broadcast to the user without the user's having requested them; do not have control over either broadcast times or content. User choice is nil or limited to whether or not to receive the service at all eg. commercial TV programming content and times are decided by the provider alone. The user turns on the TV and change the channel but cannot ask a specific program or a specific broadcast time. *With user control :* Broadcast to the user in a round robin fashion. Services are repeated periodically to allow the user a choice of times to receive them. Broadcasting number of times, and at which time is left to the provider alone. E.g. Educational broadcasting, tele-advertising pay TV (a program is made available in a limited number of time slots). A user wishing to view the program must activate his television to receive it but no other control is possible for him.

Physical specifications of B–ISDN

Three levels of user needs (access methods designed) are there :

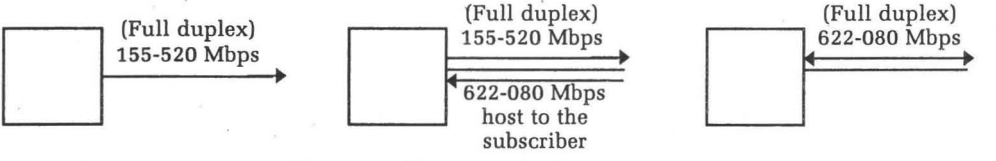


Fig. 15.17 Three levels of user needs

(i) Symmetrical

- For bidirectional information exchange.
- The rate matches to OC-3 SONET link.
- Suits well to support customers who needs access to all narrow band ISDN services, plus one or more regular video transmission services.
- Geared to fulfil the needs of most residential and many business subscribers.

(ii) Asymmetrical

- Outgoing rate is 155.520Mbps (same as an OC–3SONET link)
- Incoming rate is 622.080 Mbps (same as an OC–120 SONET link)
- Designed to fill the needs of businesses that require the simultaneous receipt of multiple services and video conferencing but that are not service providers; do not broadcast distributive services.
- Input needs of these subscribers are far grater than their output needs.
- If only one rate provided, it would either limit their receipt of services or result in wasted link capacity.
- Provides for a balanced use of resources.

(iii)

- For bidirectional information exchange
- Designed for businesses that provide and receive distributive services.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

The functional groupings of equipment in the B-ISDN model are same as ISDN and called B-NT1, BNT2, B-TE_1, BTE_2 and B-TA. B-ISDN also uses same reference points such as R, S, T and U. These are being currently scrutinised and may be redefined in due course.

POINTS TO REMEMBER

- ISDN combines voice, video and data over the same digital circuit. A communication facility is the medium which carries voice, data or image transmissions from one point to another. Technology is evolving towards a single facility that can handle the above one such is ISDN and T-carriers is another one, which are the prominent ones. ISDN has been more of a concept than a reliable service in the USA. It provides fully integrated digital services to users which falls into three categories (i) Bearer services (ii) Tele services (iii) supplementary services. The differences between them are i) no network manipulation of the information contents in the first one (ii) In tele services, network may change or process information contents (iii) In the third one, it cannot stand alone and must be used with bearer or teleservices.
- An IDN is a combination of networks (specially packet and circuit switched networks) available for different purposes. Digital pipes usage was the means to access these networks, which are time mulitplexed channels sharing very high speed paths. There are three types of channels (i) Bearer –B which is a basic user channel (ii) Data (D) for control of B channels, low rate data transfer and other applications. (iii) Hybrid (H) – High data rate applications.
- A BRI is a digital pipe composed of 2B channels and one D channel (2B+D).
- A PRI is a digital pipe composed of 23 B channels and one D channel (23B+D).
- Three functional groupings of equipment (network terminations, terminal equipment and terminal adapters) enable users to access an ISDN. Two types of network terminations are NT1 and NT2. These are the equipment that i) controls the physical and electrical termination of the ISDN at the user's premises and ii) performs functions related to layers one through three of the OSI model, respectively.
- Terminal equipment 1 is used by ISDN standard. It means the same as DTE in other protocols. It refers to digital subscriber equipment. TE2 is a subscriber equipment which does not conform to ISDN standards.
- A reference point defines ISDN interfaces. These points are R, S, T and U . R is between a TE2 and TA; S is between a TE or TA and an NT; T is between an NT1 and NT2; U is between an NT1 and ISDN office.
- The three planes found in ISDI architecture are :
  - User plane (to define the functionality of the B and H channels)
  - Control plane (to define the functionality of the D channel when used for signalling purposes)
  - Management plane (it encompasses the other two planes and used for network management)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Each plane is made up of the seven layers of the OSI model. The physical layer of the user and control planes are the same.

- BRI and PRI have data rates of 192 Kbps (4000 frames/sec, 48 bits/frame) and 1.544 Mbps (8000 frames/sec, 193 bits/frame) respectively. The distance from a TE to an NT depends on the connection, topology and placement of multiple TEs.
- In the data link layer, B channel uses LAPB and others. The D channel (control) uses LAP D control, which is also similar to HDLC. Similarly in the network layer, B channel has many options. D channels acting like B channels can connect to circuit switched networks, packet switched networks (X.25) , frame relay and ATM networks. The D channel data packet is called a message. The four fields are (i) Protocol discriminator (ii) Call reference (iii) Message type (iv) Information elements (multifield).
- Broad band ISDN provides subscribers to the network with data rate in the range of 600 Mbps (400 times faster than the PSI rate). The two services offered are (i) Interactive services (two way exchanges between two subscribers or between a subscriber and a service provider). (ii) Distributive services - one way service from service provider to subscriber three access methods are : 155.520 Mbps full duplex; 155.520 Mbps outgoing and 622.080 Mbps incoming, assymetric full duplex; 622. 080 Mbps full duplex.
- The functional groupings of N-ISDN and B-ISDN are same. (N-ISDN is known as narrow band ISDN). Both have the reference points R, S, T and U.

QUESTIONS

1. Explain ISDN. Why ISDN's acceptance has slowed?
2. What are national ISDN? Explain N1 and N2.
3. Mention the three categories of services provided by ISDN and its applications.
4. What is an IDN? Explain. Mention the differences between ISDN and IDN.
5. How ISDN is accessed? What are the three channel types of ISDN standards? Explain the channels.
6. Compare and contrast B channels with D channels.
7. Explain BRI. Explain PRI.
8. Compare and contrast BRI and PRI.
9. Compare and contrast S interface with U interface for BRI.
10. Why is the T interface not needed for BRI ?
11. Why is the R interface not defined by ISDN?
12. Explain the functional grouping of ISDN standard.
13. Compare and contrast NT1 and NT2.
14. What do you mean by reference point? Explain the various reference points.
15. What are the two different channels used in ISDN layers? Explain them.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

16. Explain LAPB and LAPD Protocols? In which layers they are used?
17. What is broad based ISDN? What is the need for it?
18. What are the two services used in B-ISDN ? Compare and contrast the two services.

FILL IN THE BLANKS

1. _____ combines voice, video and data over the same digital circuit.
2. _____ provides fully integrated digital services to users.
3. For the control of B channel _____ channel can be used.
4. ____ channel can be used for telemetry.
5. _____ services belong to the first three layers of the OSI.
6. ____ channel has 64 Kbps rate; _____ channel has 16 or 64 Kbps rate.
7. ____ channel has the lowest data rate.
8. ____ channel is used for greater than 64 Kbps transmission rates.
9. BRI has ____ B channels, and ____ D channel.
10. PRI has ____ B channels, and ____ D channel.
11. The normal user interface to an ISDN is PRI or _____.
12. PRI frame lasts put a _____ microsecond.
13. Connecting the ISDN office with NT1 is reference point ____.
14. Connecting TE_2 and TA is Reference point ____.
15. Connecting NT_1, and NT_2, is reference point _____.
16. Connecting NT_1 and TA is reference point ____.
17. Example of non ISDN terminal equipment is _____.
18. Signalling and D channel are coming under ISDN's _____ plane.
19. B channel and transmission of user information are coming under ISDN's _____ plane.
20. The network can change or process the content of data in ISDN's _____ services.
21. WIth _____ full duplex, B –ISDN access method is designed for customers who need to receive distribute services but not providing the same to others.
22. IN B-ISDN, the general class of service between subscriber and service provider or between two subscribers is _____ services.
23. Commercial TV is an example of _____ services without user control whereas _____ is an example of distribute services with control.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

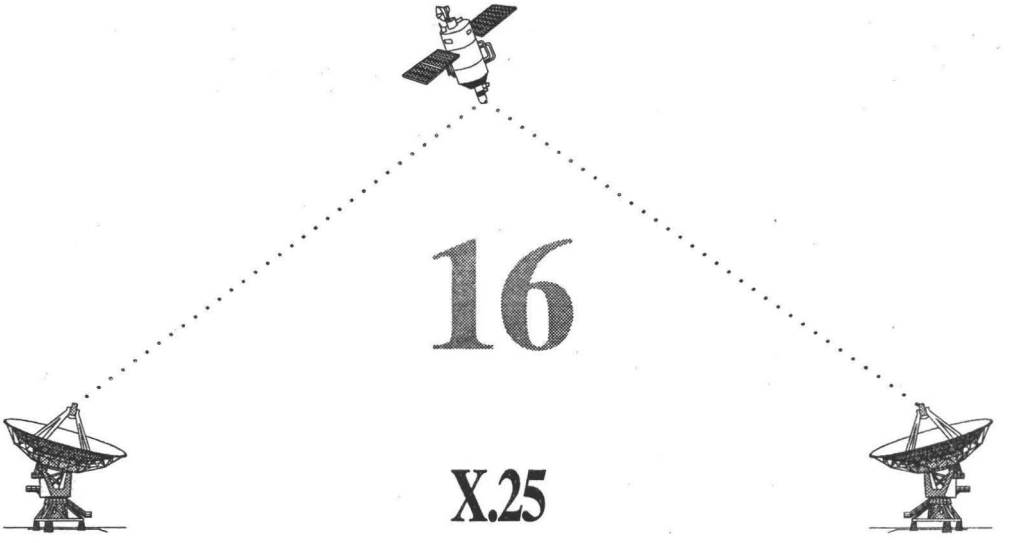
24. Store and forward messages in B-ISDN, is an example of _____ services.
25. Information from a public center in B-ISDN can be got using _____ services.
26. ISDN's equivalent of DTE is _____.
27. The data rate of symmetrical _____ Mbps full duplex outgoing rate matches with an OC–3 SONET line and _____ Mbps incoming rate matches with OC–120 SONET link.

Answers

1. ISDN
2. ISDN
3. D
4. B
5. Bearer
6. B, D
7. D
8. H
9. 2 ; 1
10. 23 ; 1
11. BRI
12. One
13. U
14. R
15. T
16. S
17. TE2
18. control
19. user
20. supplementary
21. asymmetrical
22. interactive
23. distribute ; pay TV
24. messaging
25. retrieval
26. TE_1
27. 155.520 ; 622.080

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.



16

X.25

X.25 defines how terminals and packet switching nodes exchange packets. The consultative committee of International telegraph and telephone (CCITT) has defined a number of international standards that apply to packet switching networks. X.25 is the most important ones. It is subscriber network interface (SNI) protocol.

X.25 is a standard developed by ITU–T's in 1976 for wide area networks. It is a mature, global standard used by many international organisations and today it is most widely used. This has been revised several times. X.25 is an interface between data terminal equipment and data circuit terminating equipment for terminal operation at the packet mode on public data networks. It defines how a packet-mode terminal can be connected to a packet network for exchange of data. It describes.

- The procedures necessary for establishing, maintaining and terminating connections (connection establishment, data exchange, acknowledgement, flow control and data control).
- Describes a set of services called facilities to provide functions in the areas of reverse charge, call direct and delay control.
- How the user's DTE communicates with the network.
- How packets are sent over that network using DCEs.
- A virtual circuit approach to packet switching (SVC and PVC) rather than a datagram approach.
- How asynchronous (statistical) TDM is used to multiplex packets.

X.25 is an end-to-end protocol. The actual movement of packets, through the network is not seen by it. It is something like a cloud wherein the each packet passes on its way to the receiving DCE in the network.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

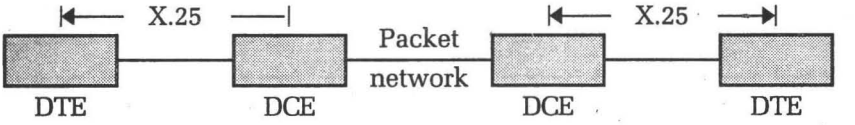


Fig. 16.1 X.25

16.1 X.25 LAYERS

The three layers under X.25 protocol are :

- The physical layer – Specifies a protocol X.21 (or X.21bis) specially defined for X.25 by the ITU–T. X.21 which is close to other physical layer protocols such as EIA-232 that X.25 is able to support them as well.
- The link access procedure, balanced layer – X.25 provides data link controls. It uses a bit oriented protocol called link access procedure balanced (LAPB) which is a sublet of HDLC.
- The packet layer protocol layer (PLP) – Comes under the network layer in X.25. This is responsible for (i) establishing the connection (ii) transferring the data (iii) terminating the connection. Users and system data comes from the top layers. At the PLP, a header containing control information is added to transform the data into PLP packet.

The ISDN layer B channel, X.25 layers in relation to the OSI layers are as shown below :

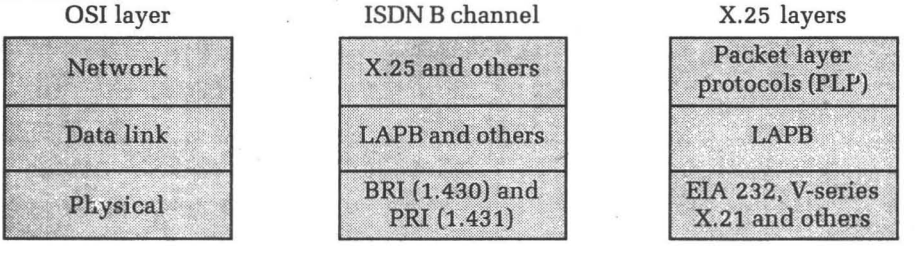


Fig. 16.2 Comparison of X.25 layers with others

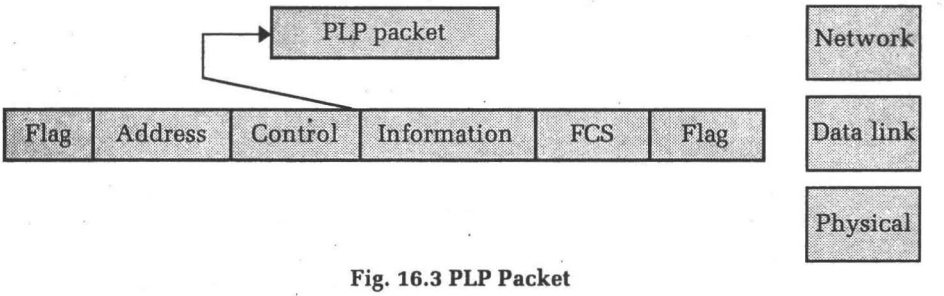


Fig. 16.3 PLP Packet

- PLP Packets from network layer are passed on to the LAPB layer for encapsulation into LAPB information frames.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

- These are next passed on to the physical layer for sending it through the network.
- X25 needs error detection and correction in network and datalink layers.

16.2 PACKET LAYER PROTOCOL (PLP)

It is the routing protocol that performs the network layer functions for routing and addressing.

Two types of PLP packets are :

- Information packets (I–packets) – contains user data coming from the upper layers.
- Control packets (C–packets)– contain an information necessary for the operation of the work but does not contain user data.

Formats are the same for both.

Information packets

- Used to transmit user data (a simple format)

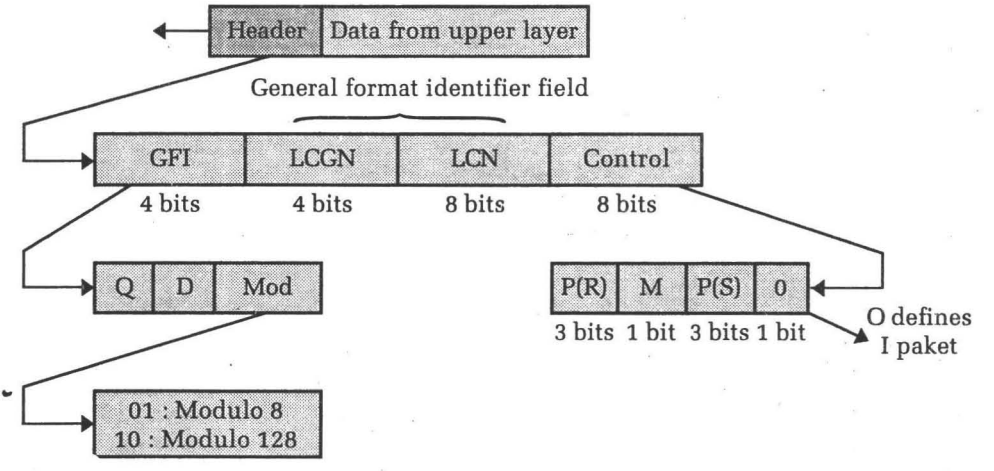


Fig. 16.4 Information packet

The fields in the header are :

(i) GFI field (ii) Virtual circuit Identification fields (iii) Control fields

(i) General format identifier field (GFI)

- 4 bit field; 1st bit – Q bit, not defined in the standard, allows the user to define two types of data e.g. if the transport layer uses two different protocols, the Q bit can be set to show the protocols from where the data is coming; D-bit is the 2nd bit used in packet sequencing ; 3rd and 4th bits are modulo bits indicating the length of the header; if the bits are 01, header is short, if bits are 10, header is long.

(ii) Virtual circuit identification fields (LCGN / LCN)

- The logical channel group number (LCGN) and Logical channel number (LCN) are 4 bits and 8 bits respectively make up together a 12 bit number; It identifies the virtual circuit chosen for a given transmission.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

(iii) Control field

- Consists of four sections :
  - P(S) and P(R) carry the packet sequence numbers for flow and error control
  - P(S) is packet send - number of packets being sent; the number is assigned by the sending DTE to outgoing packets to be used for sliding window ARQ.
  - P(R) stands for packet receive - number of the next packet expected by the receiver; the field is used to piggy back acknowledgements to information packets when both parties have data to send.
  - In short headers, P(S) and P(R) fields are three bits long. Three bits limit the size of the window to eight packets (modulo 8). In long headers, each field contains 7 bits allowing the window size to 128 packets (modulo 128). M bit used in packet sequencing. Last bit defines the packet as an I–packet.

Control Packets

Category I

- Used for flow and error control; do not carry data, hence no P(S) fields. They contain a new field, the type field.

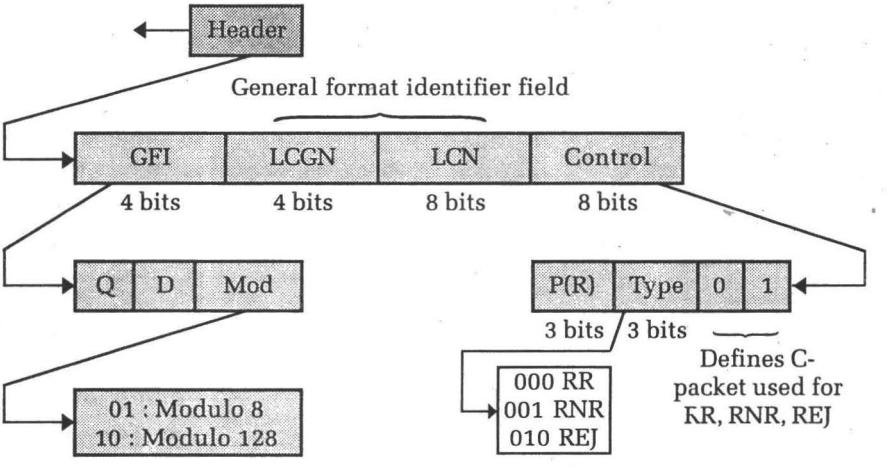


Fig. 16.5 Control packet category I

General format of the header is the same for information as well as control packets.

- Type field carries a code number which indicates the purposes of the packet; Packets can be of three types RR (Receive ready, RNR (Receive not ready) and reject (REJ)

  RR(000) : Station is ready to receive more packets. It acknowledges the receipt of a data packet by indicating the number of the next packet expected in the P(R) field.

  RNR (001) : Station not ready; cannot accept packets at this time; other party must stop sending packets as soon as the packet is received.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

REJ (010) : Reject means an error in the packet identified by the P(R) field; other party must resend all packets including and following the packet indicated (goback-n error recovery)

Category II

- Used for connection, termination and management control.

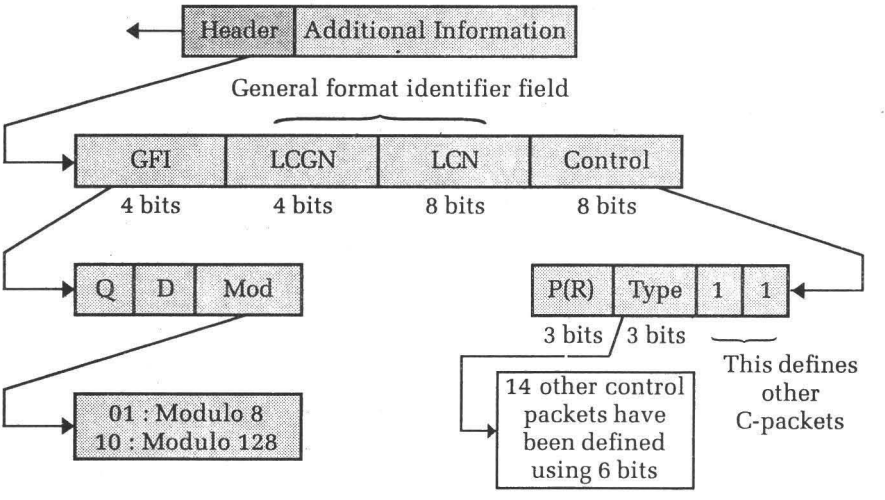


Fig. 16.6 Control packet for category II

- Information is carried in addition to header.
- Information is only for control; do not contain user data.
- General format is same as information packet (Difference is in control field and D bit significance). When set 1, it means that the sender requires confirmation from the remote DTE; When not set (0) it means that the sender needs confirmation only from the local (senders own) DCE.
- Type field – 6 bit, long; used to specify up to 64 different functions. Few of them are given below

DTE to DCE	DCE to DTE	Code
Call request	Incoming call	000010
Call accepted	call connected	000011
Clear request	Clear indication	000100
Clear confirm	Clear confirm	000101
Interrupt	Interrupt	001000
Interrupt confirm	Interrupt confirm	001001
Reset request	Rest indication	000110
Reset confirm	Reset confirm	000111
Restart request	Restart indication	111110
Restart confirmation	Restart confirmation	111111

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Category II details are explained below :

(i) *Call request/ Incoming Call :* These packets are used to request the establishment of a connection between two DTEs' call request goes from the local DTE to local DCE. Incoming call goes from the remote DCE to remote DTE.

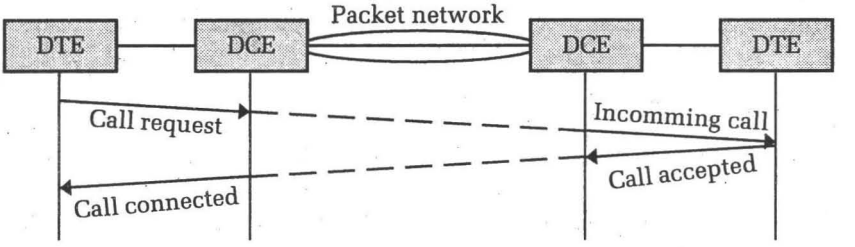


Fig. 16.7 Connection establishment

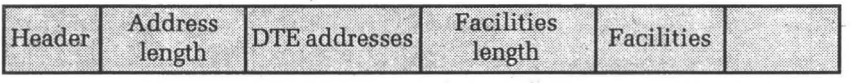


Fig. 16.8 Control packet format

In addition to the header, each of these packets include fields specifying the length of the address, DTE addresses, the length of any facilities, facilities and optimal information such as log-on-codes and database access information. Facilities are optimal services can be included on a contractual or per call basis and facilities made available by agreement between users and network providers. Contractual options include services as (i) barred incoming calls (ii) barred outgoing calls (iii) flow control parameter negotiation (iv) fast select acceptance and (v) D-bit modification. Per call options include (i) flow control negotiation (ii) fast select and (iii) reverse charging.

(ii) *Call accepted/call connected :* Same figure 16.8 applies here. These packets indicate the acceptance of the requested connection by the called system (in response to call request/incoming call packets); sent by the remote (called) DTE to DCE and local (calling) DCE to the local DTE respectively.

(iii) Clear request/ Clear indication and clear confirm

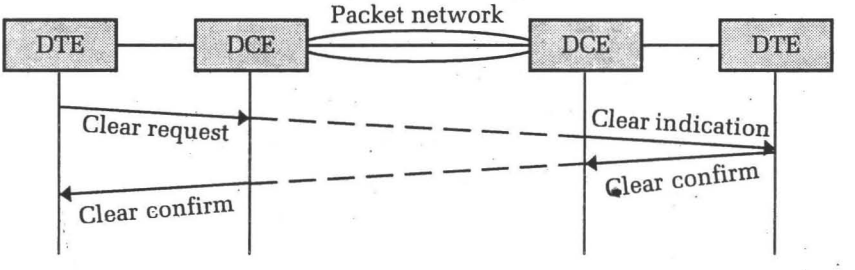


Fig. 16.9 Clearing

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

These packets are used at the end of an exchange to disconnect (clear) the connection. Either DT/DCE can imitate. Packets can also be used by a remote DTE to respond negatively to an incoming call packet when it is unable to accept the requested connection. The clear confirm packet is sent in response to the clear indication packet.

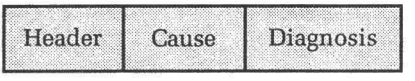


Fig. 16.10 Control packet format for
Clear request / Clear indication
Reset request / Rest indication
Restart request /Restart indication

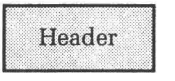


Fig. 16.11 Control packet format for
Clear confirm
Interrupt confirm
Restart confirm
Reset confirm

Interrupt

Interrupt packet is used under unusual circumstances to break into an exchange and get attention. Either DTEs or DCEs send it; involved in the exchange; acts as an alert.

E.g. An interrupt message is sent to get the attention in a situation when it cannot send more packets and cannot quit (while a DTE wait a long time without receiving either a positive or negative acknowledgement from the remote DCE and its window has reached the end).

The Interrupt confirm packet confirms the receipt of the interrupt packet.

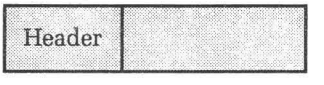


Fig. 16.12 Control packet format for interrupt

Reset request/Reset indication

These packets are used to reset the sequence numbers in an exchange over a particular virtual circuit; Reset packets are used, when a connection has been damaged to the point where the virtual circuit must be reinitialised; virtual circuit remains active, the transmission begins again from a predetermined point; all packets from that point on are renumbered starting from 0. The reset confirm packet confirms the reset process.

Restart request/Restart indication

These packets restart all virtual circuits created by a DTE; process is different from the reset process. Reset packets activate a new set of sequence numbers on an existing virtual circuit. Restart packets start up a new virtual circuit. Restart terminates and re-establishes a call by establishing a new virtual circuit for transmission. Any packets on the original pathway are lost; new packets are renumbered starting with 0. E.g. A phone call if connection not OK, hang up and dial again. The restart confirm packet confirms the restart request.

Registration request – packet allows on-line registration of new users to the network.

Registration confirm – packet confirms a registration.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Complete packet sequence

- Maximum length of data field in an information packet varies and depends on:
  (i) the network
  (ii) based on part on the limitations of the hardware
  (iii) discretion of system designers to determine.
- The above flexibility makes the information packet as too large or too small to be compatible with one or more networks. Since it has to cross several network to reach its destination; Hence resized in transit to accommodate the difference.
- Further, a given message is too long to fit within a single packet at the time of the origin.
- A long message among multiple packet are to be broken; the packet should be identifiable as a single contiguous transmission e.g. X.25 mechanism (complete packet sequence).
- A complete packet sequence use two types of packets :

A Packets

It is the one in which the data field is full; atleast one additional packet is required to carry the remainder of the message. It is identified by a 1 in the More (M) field and by a 0 in the data terminal (D) field. The 1 in the M field means that more packets are to follow in the sequence.

The D field tells the receiver about the acknowledgement required for that packet. (0 in D field – no acknowledgement is expected). 'A' packet must always be followed by atleast one other packet and do not require acknowledgement.

B Packets

These can either stand above or act as the final packet in a multipacket sequence. Datafield need not be full. It would always have 1 in the D field to indicate the requirement of an acknowledgement. A complete packet sequence = one B packet + Zero or more A packets. If all of a message's data fits into the data field of a single information packet, complete packet sequence = one B packet. If it takes two packets to carry data, complete packet sequence = one A + one B packets. For three packets to carry data, complete packet sequence = one B packet + two A packets.

- If the network requires smaller packets during transmission, the data carried by each packet can be distributed among additional A packets without losing the integrity of the message. Similarly longer packets, the data fields of the A and B packets can be combined into fewer A packets or even into a single B packet. E.g. A transmission can begin as one long B packet; In the next network, it can be subdivided into three shorter packets (2As + 1B); In the next; it can be recombined (1A packet + 1B packet) etc. Such transformations occur without affecting the integrity of the message.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

- If D bit is set to 0 → No acknowledgement needed
  If D bit is set to 1 → Packet needs an acknowledgment from the last destination.
  If M bit is set to 1 → No more packets to follow
  If M bit is set to 0 → The packet is the last packet of the message.
  Complete packet sequence → One B packet following 0 to n A packets
  Long transmission → Number of complete packet sequences.

Eg.

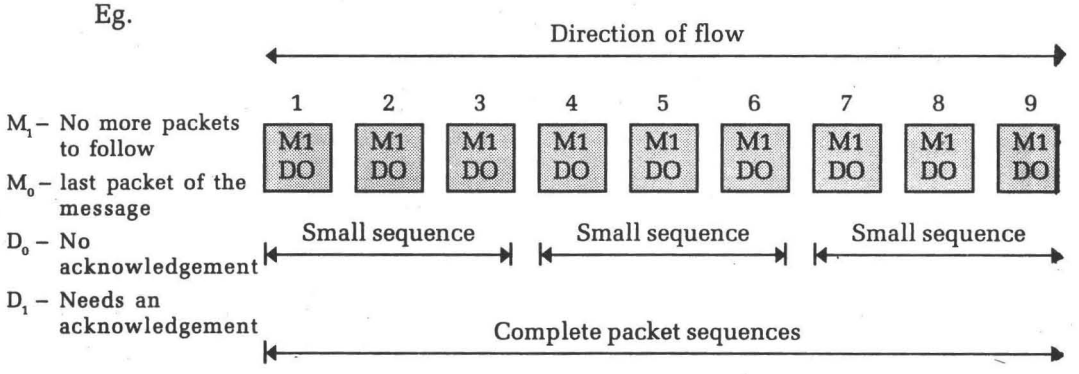


Fig. 16.13 Sequence and small sequence.

Virtual Channel ID numbers

- X.25 allows upto 4096 (2^{12}) multiplexed channels (Between each DTE and DCE)
- ID numbers are assigned to each channel to identify packets belonging to the channel.
- ID numbers are temporary, allocated dynamically as the channels are assigned; used only for the duration of the specific exchange.
- Calling and called hosts use different numbers to identify a virtual circuit.

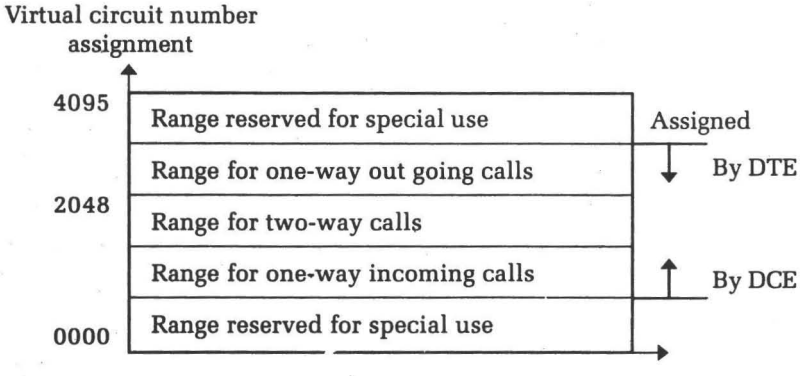


Fig. 16.14 Virtual channel ID numbers

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

POINTS TO REMEMBER

- X.25 defines how terminals and packet switching nodes exchange packets. It si a standard developed by ITU–TSS in 1976 for wide area networks. It is an end-to-end protocol. It is the procedure for data transmission between a DTE and DCE.
- X.25 protocol specifies three layers corresponding to the OSI model. (i) the physical layer (ii) the link access procedure, balanced (LAPB) layer and the (iii) packet layer protocol (PLP); (ii) and (iii) layers perform flow and error control.
- Packet layer protocol (PLP) is the routing protocol that performs the network layer functions for routing and addressing. This layer handles connection establishment and termination; data transfer and packet creation protocols.
- Two types of PLP packets are : Information packets (I–packets), control packets (C-packets). Formats are the same for both. Control packets have two categories.
- X.25 specifies protocols to handle resizing of messages. A complete packet sequence use two types of packets; Packet A and Packet B.
- Upto 4096 channels may be multiplexed at the PLP level by X.25 between DTE and DCE.

QUESTIONS

1. Define X.25. Explain.
2. Which are the three layers under X.25 protocol in relation to the OSI layer?
3. Give the reasons for the two types of headers for the I–packet in the X.25 standard.
4. Which are the two types of PLP packets?
5. Compare and contrast I – packet and C–packet.
6. Explain categories of control packets.
7. What distinguishes the PLP packet types of the X.25 standard from each other?
8. What types of packets are found in complete packet sequence. Explain the functions of these packets?
9. What are virtual channel ID number & why X.25 allows upto 4096 multiplexed channels between a DTE and DCE. What does the figure 4096 represent?

FILL IN THE BLANKS

1. X.25 protocol uses _____ _____ approach for an end-to-end transmission.
2. The ____ bit in the X.25 standard makes the user to distinguish between the two types of protocol data which follows.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

3. The PLP product is coming under _____ layer in the X.25 standard.
4. _____ is an end-to-end protocol.
5. If the _____ bit in X.25 is set to 1, indicates not more than one packet.
6. If M bit is set to ____ it is the last packet.
7. If _____ bit in X.25 is set to 1, packet needs an acknowledgement.
8. Complete packet sequence is one _____ packet following 0 to n A packets.
9. Long transmission is number of _____ _____ sequences.
10. X.25 protocol requires error checking at the _____ layer.
11. X.25 operates in the _____ _____ _____ _____ layers of the model.
12. The physical layer protocol directly specified for the X.25 protocol is ____.
13. When no data is need to be sent and an acknowledgement is required, then the PLP ____ packet is needed.

Answers

1. virtual circuit
2. Q
3. network
4. X.25
5. M
6. 0
7. D
8. B
9. complete packet
10. physical
11. Network, data link and physical
12. X.21
13. C

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

17

FRAME RELAY

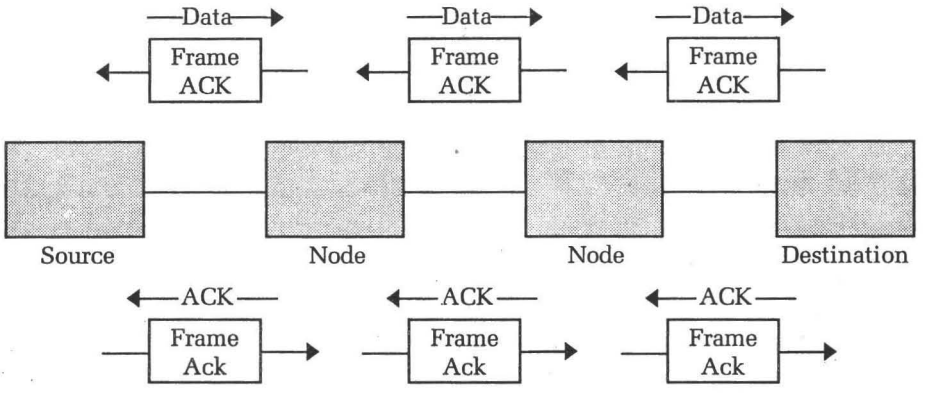
Frame relay, a newer packet switching technology transmits data much faster than the currently popular X.25 standard. A data link layer protocol that defines how frames of data are assembled and routed through a data network, frame relay provides higher performance than other wide area network packet switching technologies. Traffic in X.25 network is devoted to error checking and flow control. This is to ensure complete reliability of service. Packets are checked for accuracy at each station (node) to which they are routed. Every station retains a copy of the original frame until it gets back confirmation from the next frame where the frame would have arrived intact. This type of station to station checking is implemented at the data link layer (OSI model). X.25 has further activities. It also checks errors from source to receiver at the network layer. The source retains a copy of the original packet until it receives confirmation from the final destination. X.25 has extensive traffic because the same was required at the time of introduction since transmission media were more error prone at that time than at present. The traffic required to transmit one packet from source to destination is shown below in figure 17.1.

- All the overhead consumes bandwidth and cannot be used for message data.
- If bandwidth is limited, that data rate of the transmission which is based on the available channel width (proportionally), severely gets reduced.
- Each station has to keep a copy of the frame in its storage at the time of waiting for acknowledgement results in the bottleneck of the traffic, thereby reducing the speed.
- Improvements in traditional transmission media by using fiber optic cable rather than metallic cable (farless susceptible to noise with fiber optic) have decreased the transmission error which is unnecessary and counter productive.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Data from the network layer sent in data link layer frames



Acknowledgement from the network layer sent in data link layer frames.

Fig. 17.1 X.25 traffic (data and frame acknowledgement)

Frame relay on the other hand does not provide error checking or require acknowledgement in the data link layer. Error checking is the job of protocols at the network and transport layers which use the services of frame relay. But it operates at only the physical and data link layers. Contain data link operations get eliminated and few are combined. Hence the complex situation would emerge as the simplified transmission in the frame relay as shown in fig. 17.2.

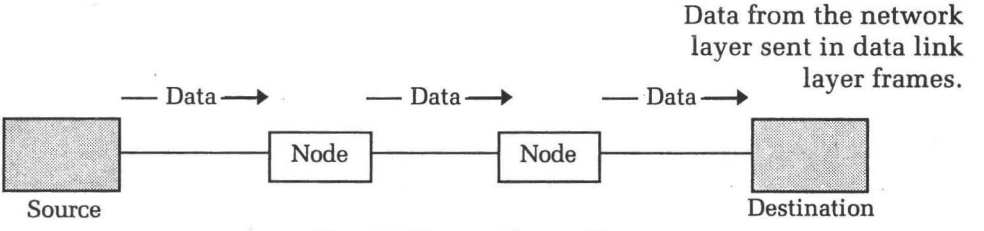


Fig. 17.2 Frame relay traffic

17.1 FRAME RELAY LAYERS

- X.25 works in 3 layers : Physical, Data link and Network function.
- Frame relay layers work in 1.5 layers – physical, portion of the data link layer functions. (eliminates all the network layer functions)
- Physical layer – No specific protocol is defined in frame relay. Frame relay support any of the protocols recognised by ANSI.

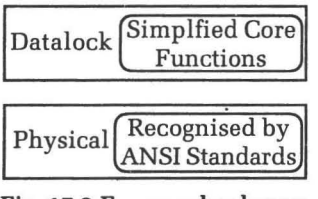


Fig. 17.3 Frame relay layers

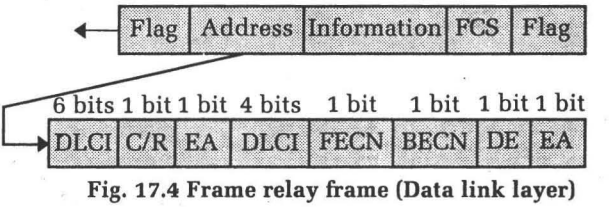


Fig. 17.4 Frame relay frame (Data link layer)

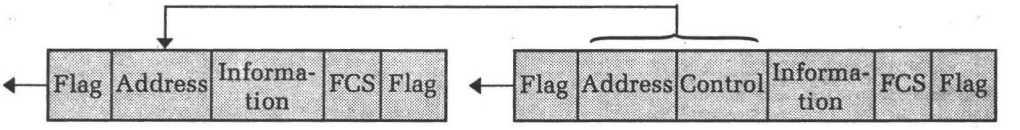
Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

C/R –	Command/response
EA –	Extended address
FECN –	Forward explicit congestion notification
BECN –	Backward explicit congestion notification
DE –	Discard eligibility
DLCI –	Data link connection identifier

Data Link Layer

Frame relay in this layer uses a simplified version of HDLC because it provides extensive error and flow control field that are needed in frame relay. See Figure 17.4. Format of frame relay is similar to HDLC.



Frame relay frame HDLC frame

Both are similar; Address & control fields have been combined in frame relay frame. (a single field of address is given).

Address field : Actually the data link connection identifier (DLCI)

DLCI (address) field consists of two or more bytes divided among a combination of address fields and control functions.

Frame relay provides more congestion control than error control (implemented in three-one-bit fields in the second byte of the address field).

DLCI fields	– First part 6 bits of the first byte and 4 bits of the second byte. Out of total 16 bit data link connection identifier defined by the standard, DLCI forms the major of 6+4 bits.
Command/Response (C/R)	– This bit is provided to allow upper layers to identify a frame as either a command or a response.
Extended address (EA)	– EA0 ⟶ Another address byte is to follow EA1 ⟶ Current byte is the final one

In a two byte address, EA is 0 in the first byte and 1 in the second byte. If an application requires additional addressing bits,

EA field in the second byte is also 0 and a third byte is added that includes a seven bit address field and an EA field of 1.

Forward Explicit congestion notification

- FECN bit is set by any routing node.
- This indicates that traffic is congested in the direction in which the frame is travelling.
- It informs the destination that congestion may cause the present or future frames to arrive late.

Backward explicit congestion notification

- BECN bit is set to indicate a congestion problem in the opposite direction to the one in which frame is travelling.
- It informs the receiver that data sent back to the sender may be delayed by congestion.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Discard eligibility (DE)

- It indicates the priority level of the frame. In urgent situations, nodes may have to discard frames to relieve bottlenecks and keep the network from collapsing due to overload. When set (DEI), this bit tells the network not to discard this frame as long as there are other frames in the streams with priorities of 0.

17.2 FRAME RELAY OPERATION

This transmission is based on permanent vertical circuit connections. These in other standards are implemented by the network layer whereas frame relay uses data link connection identifiers (DLCIs). Who identifies a permanent virtual circuit that is setup when the system is put in place. All traffics between any of the two given stations takes the same path.

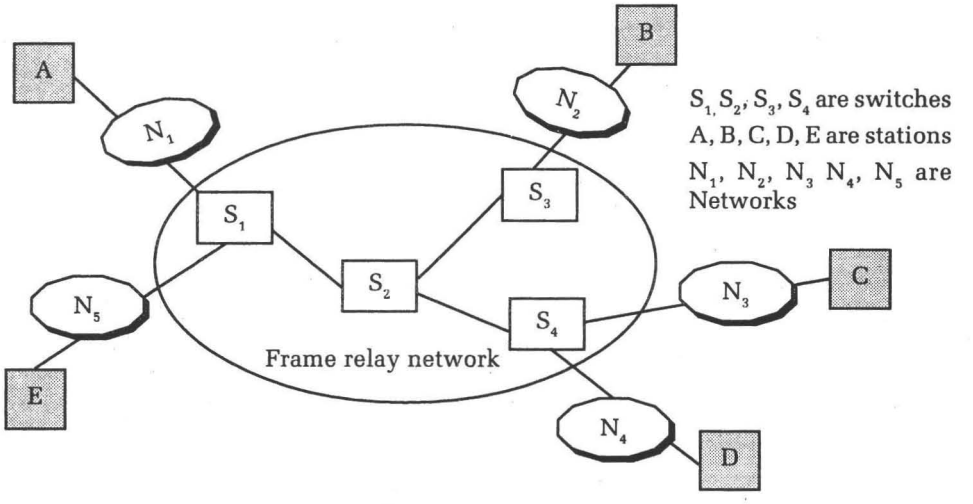
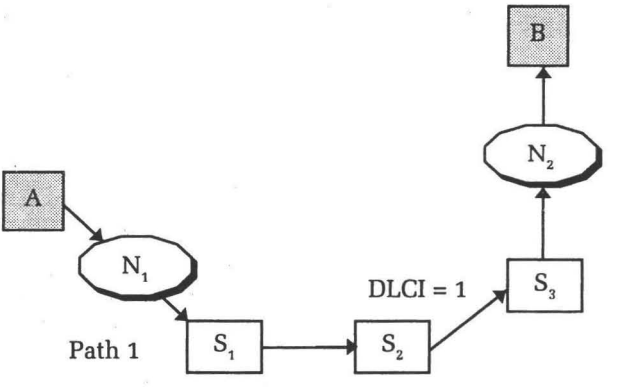


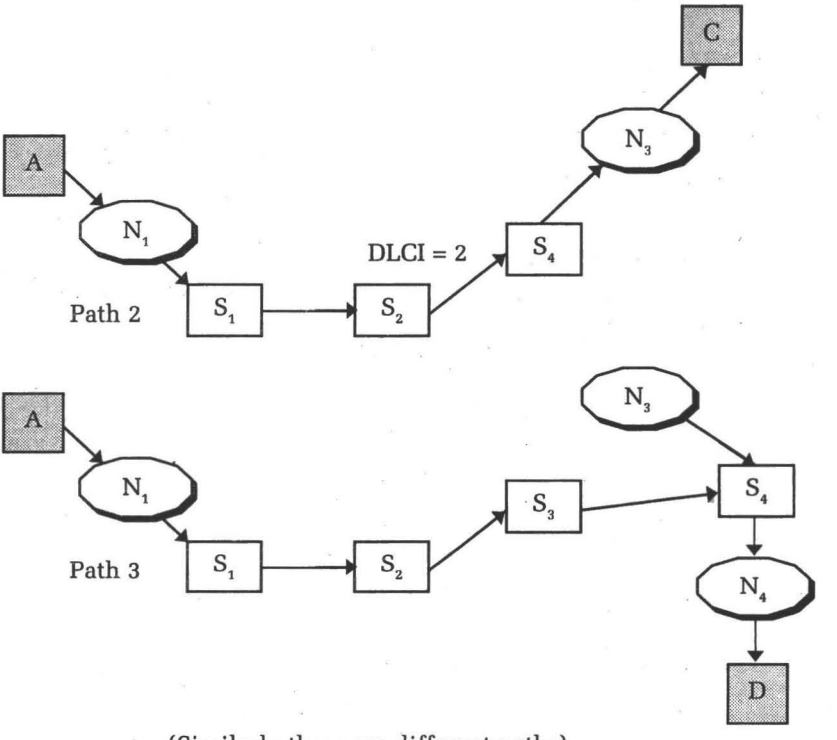
Fig. 17.5 Frame relay network

- Stations are connected to frame relay network through another type of network or services.
- A series of paths are indicated between stations.



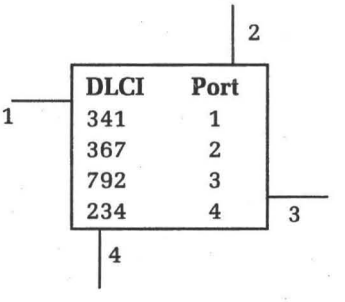
Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.



(Similarly there are different paths)

Fig. 17.6 Frame relay addresses



DLCI	Port
341	1
367	2
792	3
234	4

Fig. 17.7 Ports

Figure 17.7 shows some possible PVCs and DLCI combinations. DLCI (10 bit) can identify upto 1024 different permanent virtual circuits. A third address byte will increase this number further. The figures will indicate a significant aspect of frame relay.

The use of PVCs means that routing information is included in the destination information. If we take paths from station A to station D (path3), it always passes through the same nodes. If destination is known, the network knows the route. The functions of routing and switching handled by the network layer can be handled by the data link layer by relaying on permanent virtual circuits. Frame lay with the help of DLCI satisfies both functions of needing a network layer address and a data link layer address.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Packet switching occurs at the network layer and the transmission unit is the packet. Frame relay (Frame Switching) occurs at the data link layer where the transmission unit is the frame.

Packet switching at network layer → **Packet is** the transmission unit

Frame relay at data link layer → **Frame is** the transmission unit

Switching

Switches in the frame relay network have two functions.

(i) As soon as the frame is received, the switch checks it for errors using the FCS field, a CRC. If frame is OK, the switch compares the DLCI to an entry in a switching table.

Table tells the switch which outgoing part corresponds to that DLCI and to the correct PVC (Fig. 17.7)

Switch then sends the frame out through the port. If error is noticed in the frame, the switch discards it.

(ii) In case the frame is discarded, frame relay leaves that communication to the senders transport layer functions. The sender need not know when or where a frame is discarded/lost. He knows only that the frame has not reached its destination. The transport layer checks the integrity of the transmission at the destination. If something has happened it requests the retransmission of that portion. A switch in frame relay is to check, but not to correct errors and to route frames along predetermined paths.

Congestion Control

How to control the congestion is an issue? The switches and destination are congested with data since the standard eliminates flow control congestion delays traffic; also it causes a node to fail. Frame relay does not solve the problem but does provide ways to lessen the probability of its occurrence.

A switch in PVC encounters congestion, it warns the downstream switches and destination. This is done by turning on the FECN bit, setting it to 1. This bit indicates that congestion has started and expect some frames to be discarded.

The receiver on the other hand can set the BECN bit to warn upstream switches and the sender informing that the link is congested and to send frames slowly. Only if it is full or half duplex, this option is used and the receiver is sending its own data or acknowledgements to the sender. The sender will remain unnotified, though it is the only device in a position to take steps in avoiding congestion. It will continue to send frames unaware of the problem and the congestion becomes more and more dense.

17.3 IMPLEMENTATION OF FRAME RELAY

This is implemented in a variety of ways

- To use it as WAN backbone to connect a number of LANs (using T–1 links), an addition of interface devices such as frame relay assembler / disassemblers (FRADs) are used. This simple device assembles and disassembles packets receiving from other protocols and allows them to be carried by frame relays.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

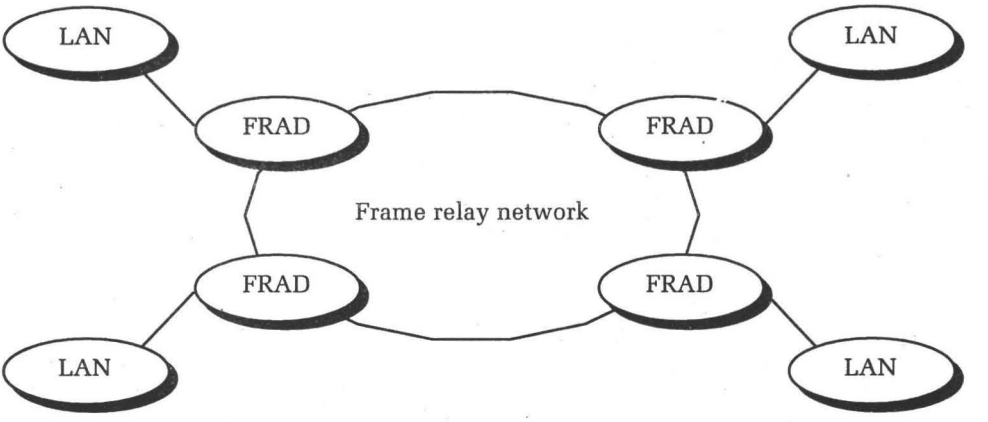


Fig. 17.8 Frame relay implementation

POINTS TO REMEMBER

- Frame relay, a newer packet switching technology transmits data much faster than the currently popular X.25 standard. It eliminates the extensive error checking necessary in X.25 protocol. It does not require acknowledgement in the data link layer.
- It operates in the physical and data link layers of the OSI model. No protocol is specified for the physical layer and the choice depends on the user.
- Frame relay works in 1.5 layers; functions in physical and a portion of the data link layer.
- It eliminates on the network layer functions.
- Frame relay in the datalink layer uses a simplified version of HDLC because it provides extensive error and flow control field that are needed in frame relay.
- Frame relay uses permanent virtual circuits (PVCs). PVC link is generally identified through the data link connection identifier (DLCI) in the address field of the data link frame.
- Packet switching at network layer uses packet as the transmission unit whereas frame relay at datalink layer uses frame as the transmission unit.
- A switch in frame relay performs error checking and routing. Error correction is left to the other protocols at the higher layers.
- Flow control is handled through setting the BECN and /or FECN bits in the address field of the frame.
- Congestion delays traffic; It causes a node to fail. Frame relay does not solve this problem but provide ways to lessen the possibility of occurrence.
- Implementation of frame relay is done in a variety of ways. A frame relay network is quite often used as the back bone of a WAN to connect a number of LANs using T-1 links.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

QUESTIONS

1. What are the functions of frame relay? Explain.
2. How is flow controlled in frame relay?
3. Compare and contrast X.25 with frame relay abut its functions.
4. What are the advantage and disadvantages of X.25 and frame relay?
5. How does a packet get retransmitted in frame relay?
6. In which layers, frame relay works?
7. How are FRADs used in a frame relay backbone?
8. Explain the frame relay operation with a sketch.
9. What are the functions of switches in a frame relay network?
10. What do you mean by congestion control? Can this problem be solved with frame relay?
11. How is frame relay implemented? Explain with a sketch.

FILL IN THE BLANKS

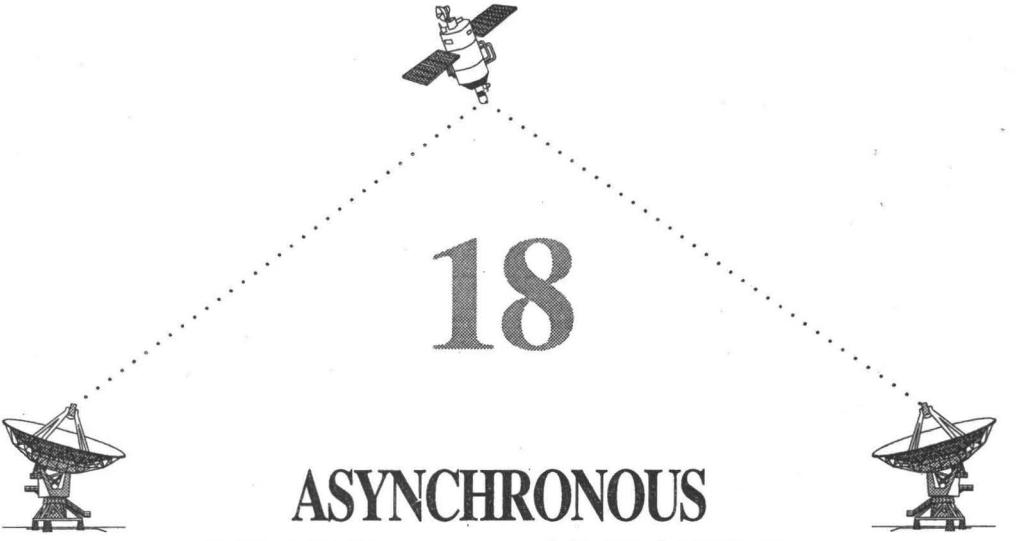
1. _____ _____ does not provide error checking or require acknowledgement in the data link layer.
2. Frame relay operates only at the _____ and _____ ____ layers.
3. _____ _____ uses the permanent virtual circuit approach.
4. A frame relay network is used often as the backbone of a _____.
5. A _____ in frame relay uses a table associating a DLCI number to a port number.
6. Routing and switching in the frame relay is performed by the ____ ___ layer.
7. Error checking in the case of frame relay needs _____ layer.
8. _____ _____ bit in the address field in frame relay determines the elimination of the frame in emergency cases.
9. Frame relay use a simplified HDLC protocol in the _____ ____ layer.
10. The last address bit is _____ bit in the address field in frame relay .
11. Switch function in the frame relay are for _____ and _____ _____.

Answers

1. Frame relay
2. physical ; data link
3. Frame relay
4. WAN
5. switch
6. datalink
7. datalink
8. Extended address
9. datalink
10. C/R
11. routing ; data regeneration

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.



18

ASYNCHRONOUS TRANSFER MODE (ATM)

It is one of the fastest growing technologies, similar to the frame relay. It is a packet switched technology originally designed for use in WAN. It is currently used in the backbone (encapsulation) and in the LAN (desk tops). It is the cell relay protocol designed by the ATM – forced and adopted by the ITU–T . Fore systems Inc. founded in 1992 by faculty from Carnegie-Mellon University was the first company to recognise the usefulness of ATM in backbone and LANs. ATM and B–ISDN together will allow high speed interconnection of the world's networks. This is considered as the highway for the information super highway.

18.1 DESIGN GOALS

ATM is an asynchronous transmission mode. Asynchronous means that each cell travels independently without being tied to others. However, transmission is connection oriented.

The following design goals stood as a challenge for the designers of ATM.

- Need for a transmission system to optimise the use of high data-rate transmission media (particularly optical fiber). Newer transmission media and equipment susceptible to noise degradation and to provide ultra wide band width for which a new technology was sought.
- Need for a system which can interface with the existing systems (various packet networks).
- To provide wide area interconnectivity between the systems without reducing the effectiveness or requiring their replacement.
- Need for a design that can be implemented with less expense; cost would not be a problem to adoption.
- System must be able to work and support the existing communications hierarchies (local loops, local providers, long distance carriers etc.)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

- System must be connection oriented to ensure accurate and predictable delivery.
- Move as many of the functions to hardware (for speed) and eliminate as many software functions as possible (for speed).

ATM is potentially as effective a LAN and short-haul mechanism as it is a WAN mechanism. Some of its followers hope that it will eventually replace the existing systems.

In ATM, all data are packet–switched, no error control at the intermediate computers within the network. Error control is the responsibility of the source and destination. Maximum data rates can be negotiated when virtual circuit are created.

Difference between ATM and frame relay

ATM realy	Frame relay
• ATM uses fixed length packet, of 53 bytes (5 bytes overhead and 48 bytes of user data) more suitable for voice transmissions. Voice transmission is not very tolerant of the receiving ends reassembly delay time that is caused by the variable length of frame relay packets. Small fixed length packets also make routing simple. It can be done in hardware and a loss of single packet of voice data has very little effect on the total message. • ATM is scalable; easy to multiplex basic ATM circuits, into much faster ATM circuits. It provides the same data transmission rates as SONET:51.84 Mbps, 622.08 Mbps. New version T–1 ATM is available. Like fractional T–1, it offers a scaled down version of the regular ATM service. (1.544 Mbps) for companies that do not immediately need such high capacity but need ATM. • ATM provides forward automatic error correction on the header (but not on the users data); Minimises the number of packets that are discarded due to errors, provided the errors are single-bit ones.	• The calls may be self contained, but all cells of a single message travel sequentially by a single path. Individual cells may be delayed in transmission, but taking the same path means that a delay affects all cells of a message equally. Small size of each cell means that such delays are likely to be short. If a cell is delayed the delay is distributed among the entire cell stream and appears to the receiver merely as if the message left the sender a little later than it did. The system can compensate for such delays either by having the sender produce the data slightly earlier than expected or by increasing the data rate so that the cells arrive faster than they can be consumed (Data rates can be controlled by adding or removing dummy bits to or from cells or by changing the bandwidth allocated for transmission). • No complex flow or congestion control mechanisms in ATM as in other WAN protocols. Smaller cells sizes offer fewer possibilities for introduction of errors. An error in ATM cell affects only a single bit. Single bit errors can be corrected easily at the receiver by the inclusion of an error code that contains sufficient redundancy to allow the original bit pattern to be reconstructed. The number of redundancy bits required for automatic correction increases with the size of the packet.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Packet networks

A packet as we have studied in the earlier chapters is a combination of data and overhead bits that can be passed through the network and treated as a self-contained unit. The overhead bits (with header and trailers) will be like envelopes that provides.

- Identification
- Addressing information
- Data required for routing, flow control, error control etc.

Data communications in the recent days are based on packet switching and packet networks. Different protocols use packets of varying size and intricacy. As networks tends to be more complex, the information that are carried on the header becomes more extensive. Since the result is larger, larger headers relative to the size of the data unit are needed. Some protocols have enlarged the size of the data unit to make use of the header in a more efficient way by sending more data with the header of the same size. Large data field creates waste. If data unit is small much of the field goes unused. Hence to improve utilisation some protocols provide variable packet sizes to users. The packets now are as long as 65,545 bytes (long-haul links) with packets of less than 200 bytes.

Mixed network traffic

The various sizes of packet makes :

- Traffic unpredictable.
- Switches, multiplexers and routers must incorporate elaborate software systems for managing.
- A great deal of header information must be read; each bit counted and evaluate to ensure the integrity of every packet.
- Internet working among the different packet networks is slow and expensive.
- Providing consistent data–rate delivery.

To get most out of broad based technology, traffic must be time–domain multiplexed onto shared paths.

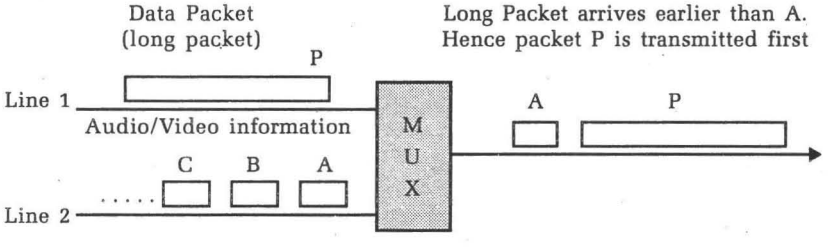


Fig. 18.1 Multiplexing different packet sizes

Packet A has to wait, since packet P arrives little earlier. It is something like a bus coming a fraction of a second later before the gate is closed near the railway crossing. The bus has to wait for a long train to cross. The size of P in the above examples makes on unfair delay for Packet A. This imbalance affects all the packets of line 2. Since audio and video packets are small, mixing them with conventional

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

data packets creates unacceptable delays of this type and makes shared packet links unusable for audio and video information. Traffic must travel over different paths (like automobile and train traffic different routes). But to fully utilise broad band width links, we send all kinds of traffic over the same links.

Cell networks

Many packet internet working problems could be solved by a concept called cell networking. A cell is a small data unit of fixed size. Cell is used in cell network as the basic unit of data exchange. All data are loaded into identical cells that can be transmitted with complete predictability and uniformity. Though tributary network feeds packets of different sizes and formats to reach cell network, they are again split into multiple small data units of equal length and loaded into cells. The cells are then multiplexed with other cells and routed through the cell network. Since the cells are of the same length and small, the problems of multiplexing different sized packets could be solved.

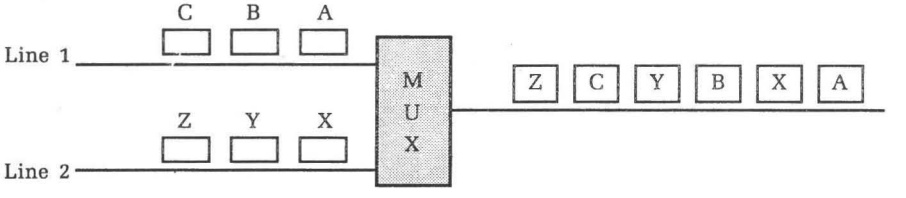


Fig. 18.2 Multiplexing from cells

Two lines 1 and 2 have cells instead of packets. Since packets are of equal sizes, the first cell from line 1(A) is sent followed by the 1st cell of line 2(X). Thus we get AXBYCZ cells interleaved so that no cell suffers a long delay. High speed of the links coupled with small size of the cells (despite interleaving), makes cells from each line arrive at their respective destination in an approximation of a continuous stream (like still photos moving continuously in a movie). The cell network can handle real time transmissions (e.g.. phone call), without the parties being aware of the segmentation or multiplexing.

Farther, the predictability conferred by fixed cell size allows switches and terminals to treat each cell as a unit rather than as a bit stream.

In a cell network, the smallest unit is a cell, not a bit.

This makes network operation more efficient and cheaper. Switching and multiplexing can be implemented in hardware instead of software, resulting in less expensive devices both to produce and to maintain.

Routing in cell networks

As we have seen earlier, cells are useful to move information point to point efficiently and with minimal delays. Cell routing strategy is therefore to be studied in more detail than cell itself.

Virtual circuits

Cell networks are based on virtual circuit routing. All cells connected with the single message follow the same path and remain in their original order until they reach their destination. If cells are routed along different paths, they will be

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

arriving out of order and with uneven and unpredictable delays. The erratic quality of a connectionless delaying of this sort makes it unsuitable for on–line video or audio transmission. Further, connectionless services need more overhead information (complete addressing, flow and error control data appended to every packet). The advantages of smaller simple uniform cells will not be found in the resulting header lengths.

Cell network is simple and the efficiency depends on simplicity. Strategy of routing these cells are simple.

Concept of cell switching could be easily examined if the sample network is limited to the following parameters.

- Assume a based band technology is used.
- Assume that the link between any two devices have only one channel.

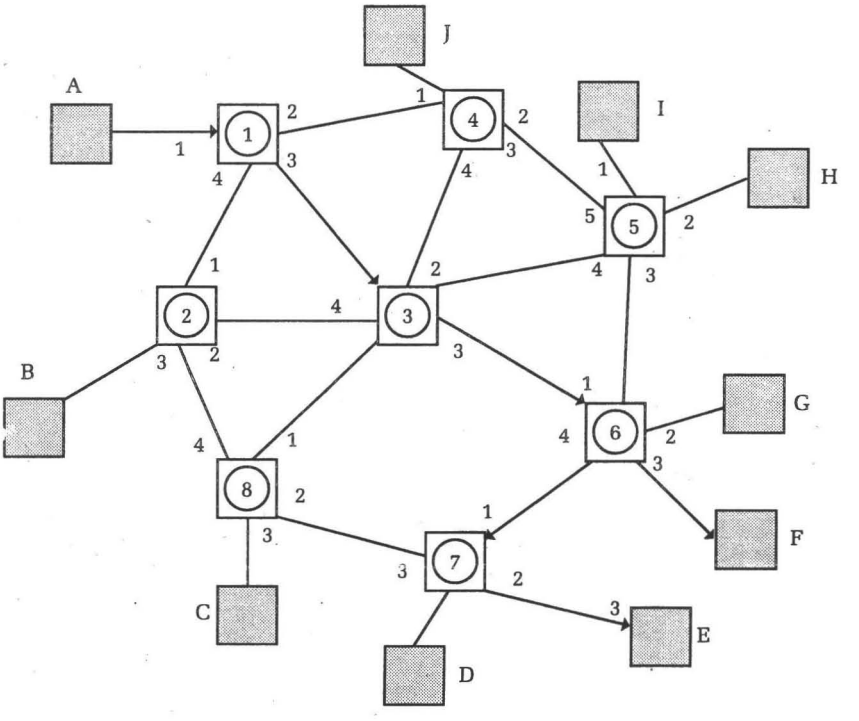


Fig. 18.3 Cell Switching

A,B,C,D, ... J are devices

(1), (2), (3), ... (8) are switches

Switches (1), (2), ...(8) have ports (Each one numbered from 1 to 5)

A sample cell network is shown in figure 18.3.

Device A sends a message to device E. Message consists off a number of cells route selected A to 1 to 3 and 6 to 7 and to E. Each cell carries identification to this route and the information in a smallest possible format. Route identification is contained in a brief header field called virtual path identifier (VPI). Every switch contains a bit of numbers which shows path to other switches in the network and

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

these numbers are pertaining to the particular switch. A single path could be identified by a different number at each switch. ID numbers for each path is chosen by each switch. This independence makes VPIs to be kept short. Each switch needs enough ID numbers to accomodate the path it serves. Independence also makes reconfiguration easier. VPI in the header is valid for only one link. Each switch replaces the arriving VPI with its outgoing VPI.

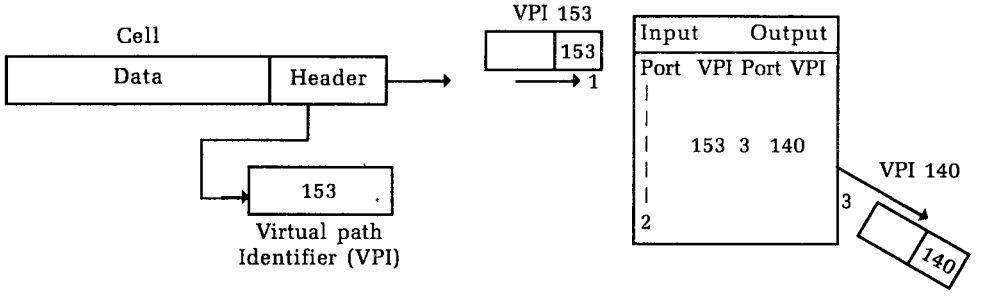


Fig. 18.4 Switching using VPI

Device A inserts into the header the VPI (in the above case it is 153) to refer to the path for the final device E.

Every note has a table to show VPI is coming from which port and how it matches each of its own outgoing VPIs. VPIs can be assigned by a network manager to create permanent identifiers.

A cell with VPI of 153 arises at the switch 1 through port 1. The switch needs to determine which of its exit ports coincides to 153 from port 1. The switch finds the port 1 entry with VPI 153 and discovers the combination corresponds to output port 3 and VPI 140. It changes the VPI in the header to 140 and sends the cell out through port 3.

Some mechanism is also applied to, switches handling traffic for multiple channels on each path. Cell header contains two identifiers VPI and VCI.

VPI is virtual path identifier. VCI is virtual channel identifier.

- Entry port number + VPI combination tells the switch through which port to route the cell.
- VPI + VCI combination tells the switch over which of the possible channels serviced by that port the cell should be directed.
- Figure 18.6 shows switch 1's table should be augmented to reflect this additional information.

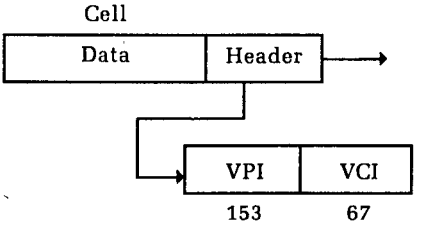


Fig. 18.5 VPI and VCI

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

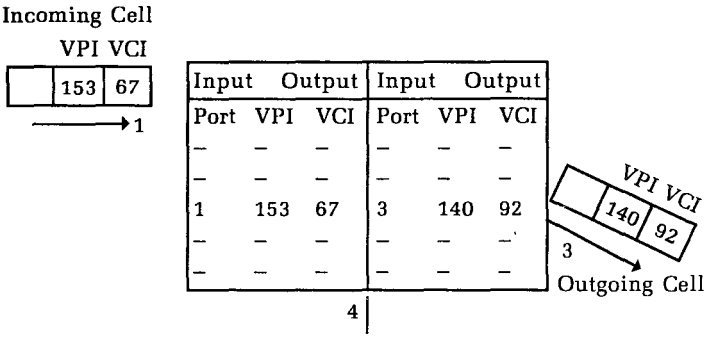


Fig. 18.6 Switching using VPI and VCI

18.2 ATM TOPOLOGY

ATM is a hierarchy of networks connected by associated interfaces. The important interfaces are :-

(i) User network interface (UNI) – Interface between a user and the wide area ATM network.

(ii) Network to network interface (NNI) – Interface between two wide area ATM networks (between two B – ISDN nodes)

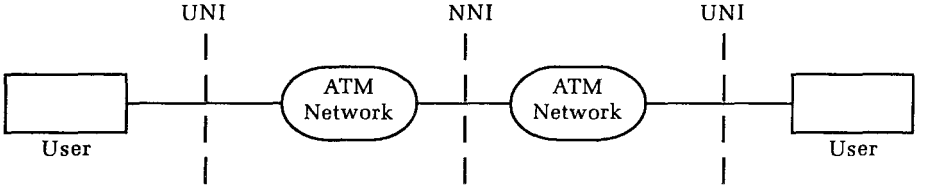
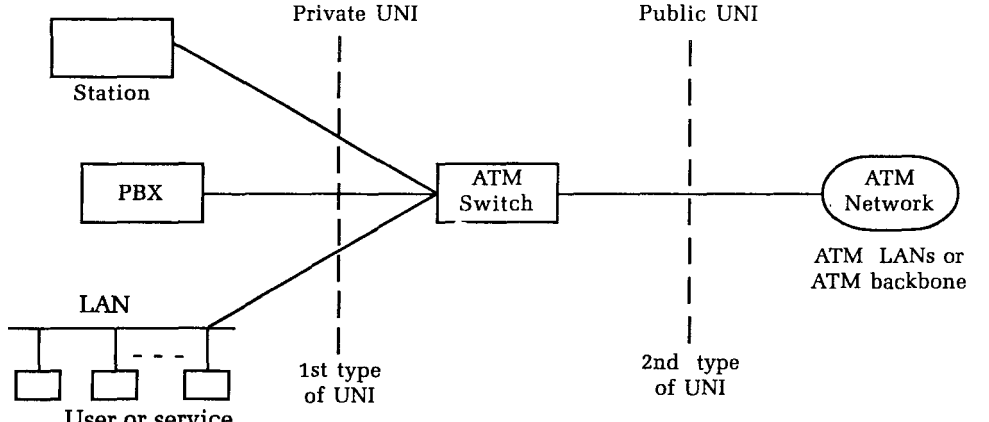


Fig. 18.7 ATM interface



A UNI that connects a user or service to an ATM switch is called a *private UNI*

Note : Private and public UNI does not indicate the ownership. They indicate whether the interface is located inside or outside the users premises.

A UNI that connects a user or service to a public ATM network is called a *public UNI*

Fig. 18.7 Private and Public UNI

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

18.3 ATM PROTOCOL ARCHITECTURE

ATM standard defines a series of layers not analogous to those of the OSI model. ATM layers are :

(i) Top layer	Application adaptation layer (AAL)
(ii) Middle layer	ATM layer
(iii) Bottom layer	Physical layer

- AAL allows existing networks (such as packet networks) to connect to ATM facilities.

Fig. 18.8 ATM layers

Application adaptation layer (AAL)

- AAL protocols accepts transmissions from upper layer services (packet data) and map them into fixed – size ATM cells. These transmissions can be of any type voice, data, audio and video and can be of variable or fixed rates.
- At the receiver end, the process is reversed – segments are reassembled into their original formats and passed to the receiving service.
- AAL layer reformat data from other protocols, acting like a gateway in internet working.

Data types

ATM standard divides the AAL layers into categories; each supports the requirements of a different type of application. ATM designers identified four types of different data streams :

- Constant bit rate data – Refers to applications that generate and consume bits at a constant rate.
- Variable bit–rate data – Refer to applications that generate and consume bits at variable rates.
- Connection oriented packet data – Refers to conventional packet applications (X.25 and TCP Protocol of TCI/IP) that use virtual circuits.
- Connectionless packet data – Refers to applications that use a datagram approach to routing (such as the IP Protocol in TCP/IP).

Constant bit rate data

Here transmission delays must be minimal transmission, must stimulate real time. E.g. constant bit-rate applications include real time voice (telephone calls) and real time video (television)

Variable bit rate data

Here the bit rate varies from section to section of the transmission (within established parameters). Eg. Compressed video, data, video.

SEAL (Simple and efficient adaptation layer)

ITU–T has introduced an additional category which is adopted for point to point instead of multipoint / internetwork transmissions. This is found superior to the above data types. The sublayer designed to meet the needs of this type of transmission is SEAL.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

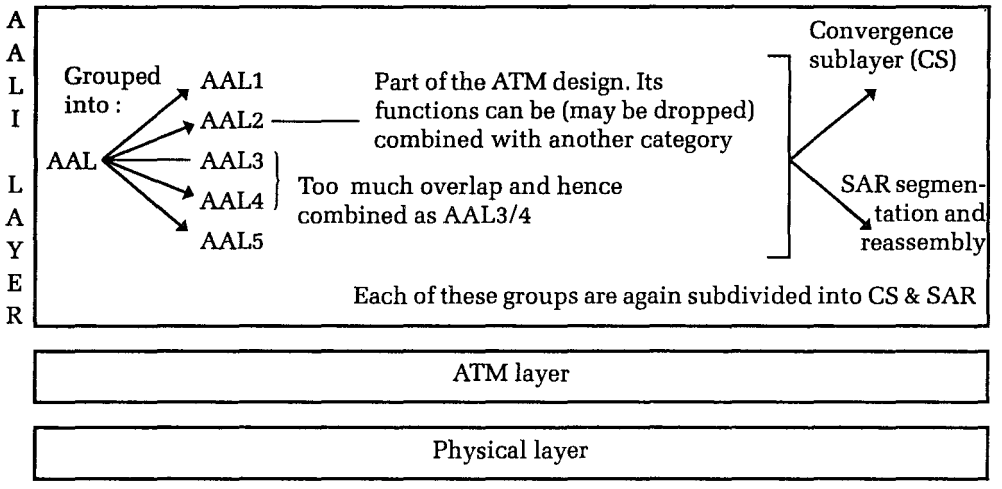


Fig. 18.9 AAL Types & other layers

AAL 1

- Supports applications that transfer information constant bit rates eg. voice, video.
- Allows ATM to connect existing digital telephone networks such as DS–3 or E–1.

Convergence sublayer (CS) :

- Divides the bit stream into 47 byte segments and passes them to the SAR sublayer (below)

Segmentation and Reassembly (SAR) See fig. 18.9

- The layer accepts a 47 byte payload from CS.
- Adds a one-byte leader → Total 48 byte data unit passed on to ATM layer; It is encapsulated in a cell.

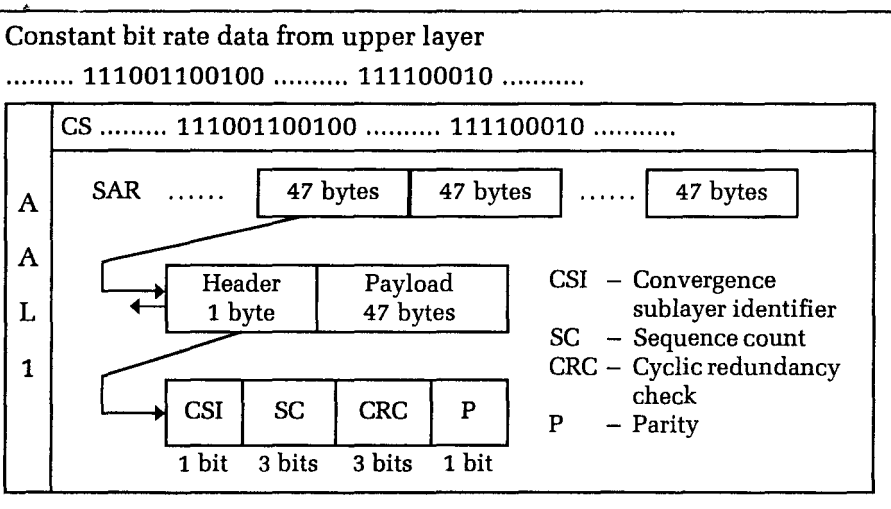


Fig. 18.10 AAL1

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

CSI (1 bit) – For signalling purposes (that are not clearly identified)

SC (3 bits) – Modalo 8 sequence number; used for ordering and identifying cells for end-to-end error and flow control.

CRC (3 bits) – Calculated over the first four bits using the four bit divisor $x^3 + x + 1$. Three bits look like too much redundancy. Intended to detect a single or multiple bit error + to correct several single bit errors. In non real time applications : (1) an error in a cell is inconsequential (cell can be retransmistted) and not an option (ii) with no retransmission the quality of the received data deteriorates; with one missing cell, a click during a telephone call/a black dot on video monitor results; large number of missing cells destroy intelligibility; Automatic correction of a single bit header errors reduces the number of cells which are missing.

Parity (P) – See the explanation in page 351

AAL2

- To support variable bit rate applications eg. News readers face on the screen; Minimum amount of change found as compared to footage in the football game. Data is sent at a lower data rate in the first case. Vice versa in the second case (at higher rate).

Convergence sublayer (CS) :

- Format for reordering the received bit stream, adding overhead is not defined. Different applications have different formats.

Segmentation and Reassembly (SAR) See fig. 18.10.

- The layer accepts a 45 byte payload from CS
- Adds one byte header and two byte trailer → Total 48 byte data unit passed on the ATM layer; encapsulated in a cell.

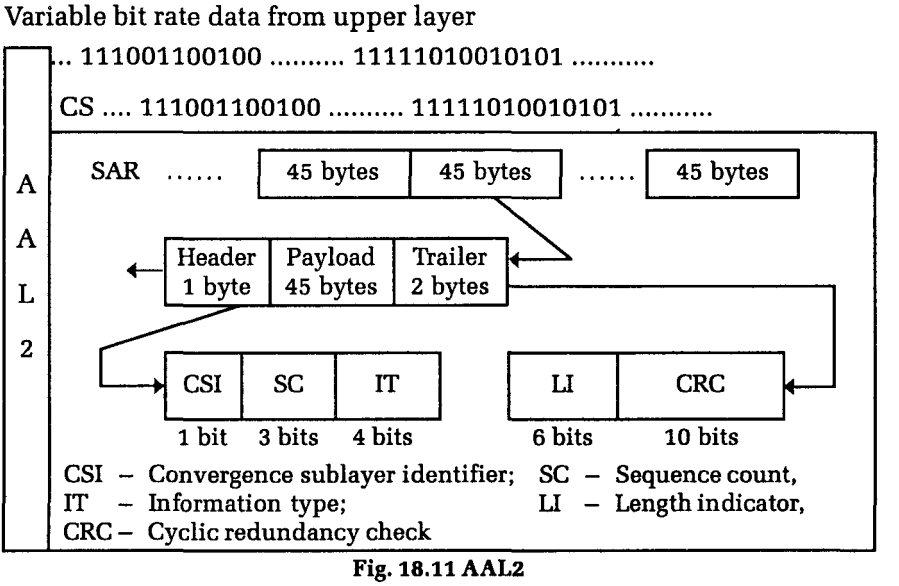


Fig. 18.11 AAL2

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

- The overhead at this layer consists of three fields in the header and 2 fields in the trailer.

CSI (1 bit)	– For signalling purposes (that are not clearly defined)
SC (3 bits)	– Modulo 8 sequence number; used for ordering and identifying cells for end to end error and flow control.
Information type	– Identify data segment at the beginning, middle or end of the message.
LI (6 bits)	– Used with the final segment of a message to indicate how much of the final cell is data and how much is padding; If the original bit stream is not divisible by 45, dummy bits added to the last segment to make up the difference. Field indicates where in the segment those bits start.
CRC	– Last 10 bits of the trailer (for the entire data unit). Also used to correct single bit errors in the data unit.

AAL 3/4

- AAL3 intended to support connection oriented services. AL4 to support connectionless services; Fundamental issues of portocols AAL3 and AAL4 are same. Hence combined – AAL3/4 as a single format.

Convergence sublayer (CS)

- Accepts a data packet of no more than 65, 535 (2^{16}-1) bytes from an upper layer service (eg. SMDS or frame relay) + A header + A trailer; The header and trailer indicates the beginning and end of the message (for reassembling); Also shows how much of the final frame is data and how much is padding.

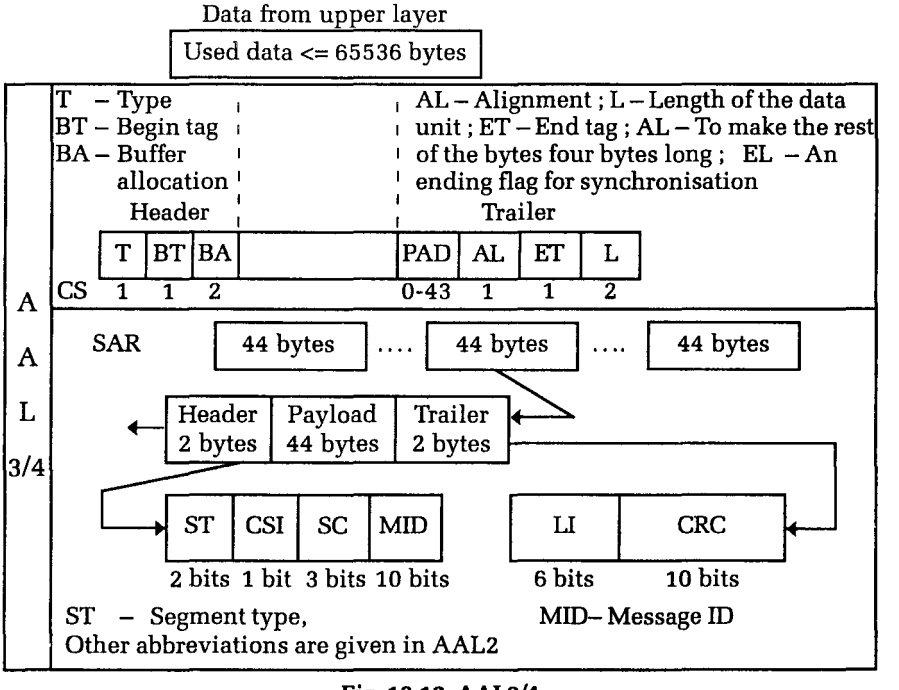


Fig. 18.12 AAL3/4

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

- Packets vary in length; padding is required to ensure that segments are of the same size; Final control fields fall where the receiver expects to find them; If the header trailer and padding in place, CS passes the message in 44 byte segments to the SAR layer, CS header and trailer are added at the beginning and end of the original packet, not to every segment.
- Middle segments are passed to the SAR layer without added overhead; ATM retains the integrity of the original packets; Keeps the ratio of overhead to data bytes low.

T – Hold over from the previous version of AAL3; set to 0 in this format.

BT (1 byte) – A beginning flag; identifies the first cell of a segmented packet and provides synchronisation for the receiving clock.

BA (2 bytes) – Tells the receiver which size buffer is needed for the receiving data .

PAD – Padding is added to fillout the final cells in a segmented packet Total can bet between 0 – 43 bytes; added to the last or last two segments. If the number of data bytes in the final segment is : 40 – No padding; 4 byte trailer is added; 40 + 4 = 44 bytes.

<40 (0 to 39) – Padding bytes (40 to 1); Total 40 bytes.

41 to 43 – Padding bytes (43 to 41) Total is 41 + 43 or 43 + 41 = 84 (First 44 bytes make a complete segment. Next 40 bytes + trailer → last segment).

Segment and reassembly – See explanation below.

Parity P of AAL1 (One bit field)

- Standard parity bit calculated based on the first seven bits of the header.
- A parity bit can detect an odd number of errors (not even numbers)
- Feature can be used for error corrections of the first four bits.
- If one single bit is in error – both CRC and P bit will detect; CRC corrects the bit and the cell is accepted.
- If two bits in error – CRC will detect them (not P bit); CRC correction is invalid; cell is discarded.

Segment and Reassembly of AAL3/4

Figure 18.11 shows AAL3/4 data unit. Functions at this layer accept a 44 byte pay load from the CS and add a 2 byte header and a 2 byte trailer. Total would be 48 byte data unit which is passed on to the ATM layer.

The header and trailer sublayer have 6 fields.

- Segment ST (2 bits) – Tells whether the segment belongs to the beginning, middle or end of a message or a single segment message.
- MID (10 bits) – Multiplexing identification : Identifies cells coming from different flows and multiplexed on the same virtual connection.
- LI (6 bits) : Used in conjunction with the ST to indicate how much of the last segment is message and how much is padding. LI field is used only in frames identified by the ST as being the last in the message (end of packet)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

- CSI
- SC
- CRC

} Functions same as in AAL2

AAL5

- ATM has provided the fifth (AAL5) sublayer for the purposes of :

(i) No addressing
(ii) No sequencing
(iii) No header information at CS or SAR
(iv) Provides only a Pad and a four field trailer.
(v) No comprehensive sequencing and error control mechanisms like that of AAL3/4 which are not required for every application.

- Sequency and elaborate error correction mechanisms are an unnecessary overhead when transmissions are not routed through multiple nodes or multiplexed with other transmissions.
- AAL5 assumes that :

(i) All cells belonging to a single message travel sequentially.
(ii) Rest of the functions usually provided by the CS and SAL headers are already included in the upper layers of the sending application.

Convergence sublayer

- Accepts a data packet of not more than 65, 535 bytes from the upper layer service; Adds an 8 byte trailer + Any padding required (to ensure that the position of the trailer falls where the receiving equipment expects it. (at the last 8 bytes of the last data unit).
- CS then passes the message in 48 bit segments to the SAR layer.
- Here also (like AAL/3/4), the padding and trailer are added to the end of the entire message (not to each segment). Segment consists of 48 bytes of data; In the case of the last segment, 40 bytes of data + 8 bytes of overhead (trailer)

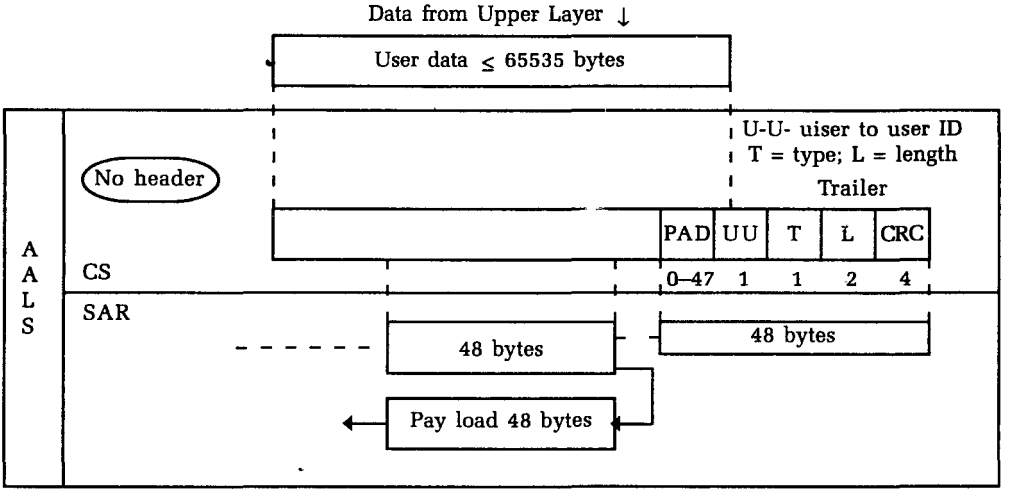


Fig. 18.13 AAL5

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

PAD

- Total padding for a packet is between 0 - 47 bytes.
- Rules for padding same as AAL 3/4 (Body segments in this case = 48 bytes instead of 44 bytes)

UU : UU field is left to the discretion of the user

T : Reserved but not yet defined

L : Indicates how much of the message is data and how much padding.

CRC : Last four bytes are an error check for the entire data unit.

ATM layer

This layer provides (i) Routing (ii) Traffic management (iii) Switching and (iv) Multiplexing services. It processes 48 byte segments outgoing traffic after receiving and accepting the same from the AAL sublayers. It then transforms them into 53 byte cells. An addition of 5 byte header is added.

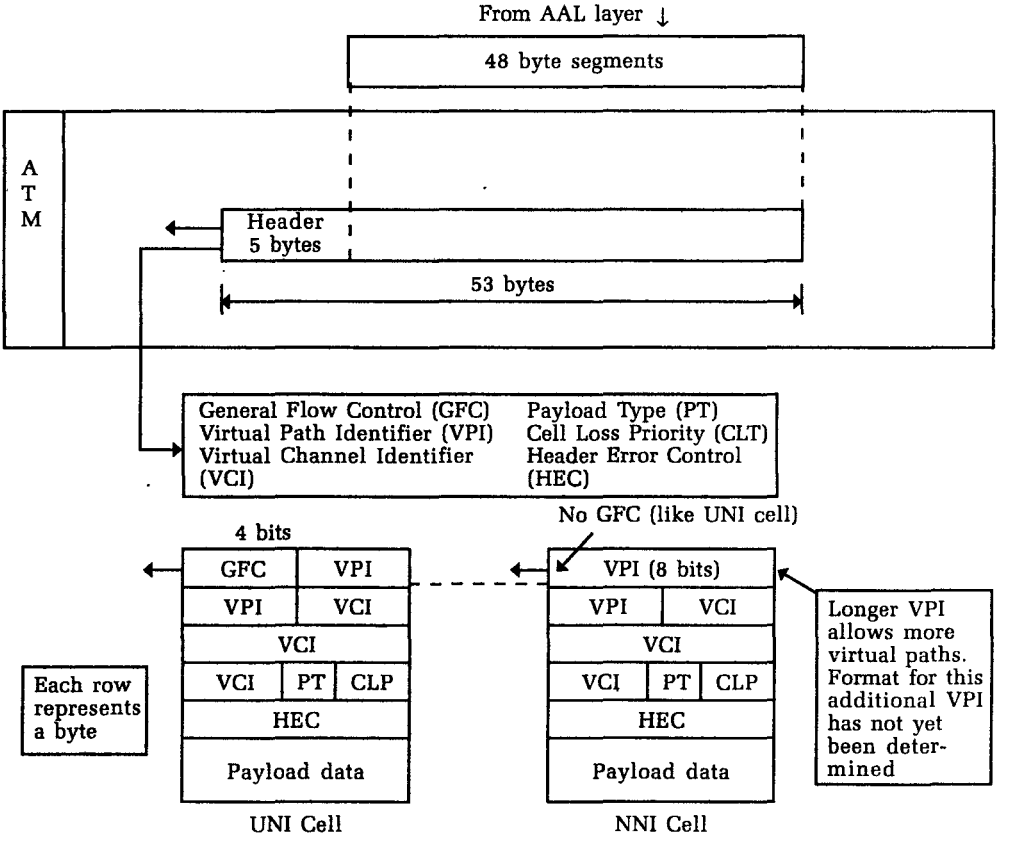


Fig. 18.14 ATM Headers

Header format

ATM uses two formats as shown in the figure :

– one for UNI cells

– Another for NNI cells.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

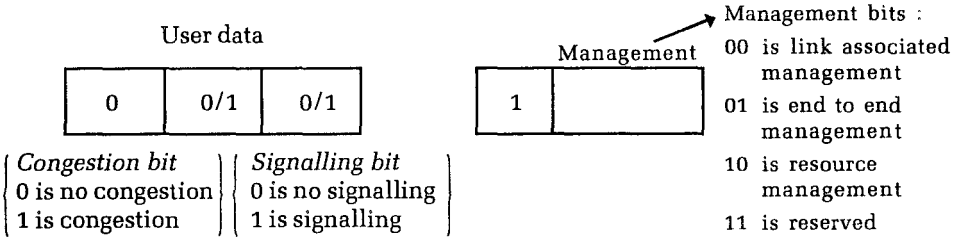
These headers in the byte–by–byte format are preferred by the ITU–T. Each row represents a byte.

GFC (4 bit) : Provides flow control at the UNI level. This is not required at the NNI level. In NNI header, these bits are added to the VPI.

VPI : 8 bit field in the UNI cell and 12 bit field in an NNI cell.

VCI : 16 bit field in both frames.

PT : 3 bit field (1st bit – pay load as user data or managerial information) 2nd and 3rd bit depends on the first bit.



CLP

- 1 bit CLP field is provided for congestion control.
- Low priority cells are discarded to protect the quality of service for higher priority cells, during the time when the link becomes congested. The bit indicates to a switch which cells are to be dropped and which are the ones to be retained.
- A cell with CLP bit set to 1 is retained as long as there are cells with a CLP of 0. This ability to distinguish priority is useful is many circumstance. E.g. If a user is not able to create a required bit rate per second, he can insert certain dummy cells into the data stream to raise the bit rate temporarily. The dummy cells will show a priority 0 and these can be discarded without consequence to the actual data. On the contrary, if the user has to transmit at a higher rate, the network can set this field to 0 in some cells to indicate that they are to be dropped if they are overloaded.

HEC

It is a code computed for the first 4 bytes of the header (a CRC of $x^8 + x^2 + x + 1$ – used to correct single-bit errors and a large class of multiple-bit errors)

ATM Switches

ATM switches provide both switching and multiplexing. Switching is based on a table that is implemented in hardware for PVC (permanent virtual circuit) networking. Then it is stored in RAM for Switched Virtual Circuit (SVS) networking.

Switches are designed for providing : (i) Virtual path (VP) Switching using VPIs, (ii) Combination of virtual path switching and virtual channel switching known as virtual path and channel (VPC) switching and uses both VPIs and VCIs.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Virtual path and channel (VPC) switching and uses both VPIs and VCIs

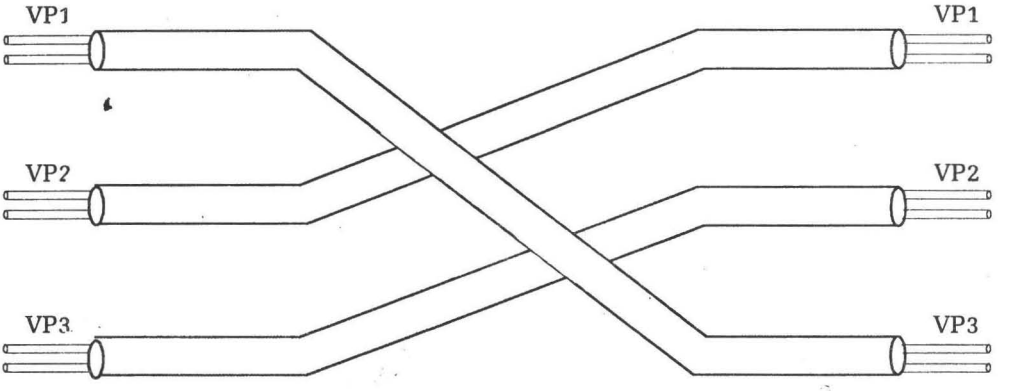


Fig. 18.15 Conceptual view of VP Switching

- VPs cross each other
- Channel with each VP remain with that UP rather than passing into another.

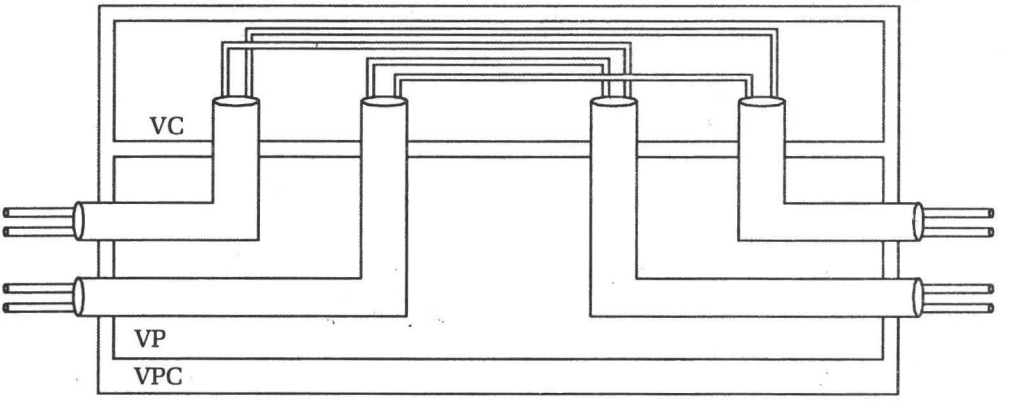


Fig. 18.16 Conceptual view of VPC Switching

- A channel from one VP may pass into another VP.

Physical layer

ATM forum has left the specifications for the level to the implementing agency. E.g. transport medium can be twisted pair, coaxial, or fiber optic cable.

This layer defines :-

(i) Transmission medium,

(ii) Bit transmission,

(iii) Encoding, and

(iv) Electrical to optical transformation

It provides convergence with :

(i) Physical transport protocol (SONET) and T–3

(ii) Mechanisms for transforming the flow of cells into a flow of bits.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

ATM encapsulation

ATM uses a different type of protocol than traditional LANS. It uses 53 byte fixed length packet and is connection oriented (devices typically establish a switched virtual circuit before transmitting). Ethernet and token ring use larger variable length packets and connectionless. In order to use ATM in a backbone network that connects LANs, some translation must be done to enable the LAN packets to flow over the ATM backbone. This is typically done by *encapsulation*. Here an ATM edge switch known as *encapsulation switch* is connected to the LANs. The switch performs the transaction from ethernet (or token ring) to ATM and back again at the other end. The LAN packet is broken into a series of ATM packets transmitted over the ATM backbone and reassembled into the LAN packet at the edge switch at its destination. ATM is transparent to users because the switches do all the required translation.

ATM backbone switches provide point to point full duplex circuits at 155 Mbps (for a total of 310 Mbps). Switches providing 622 Mbps (oc-12, a total of 1.244 Gbps) are not yet widely available. The additional delay imposed by the need to packetise and reassemble the LAN packets will be found. There is extra overhead imposed by using the ATM packets along with LAN packets.

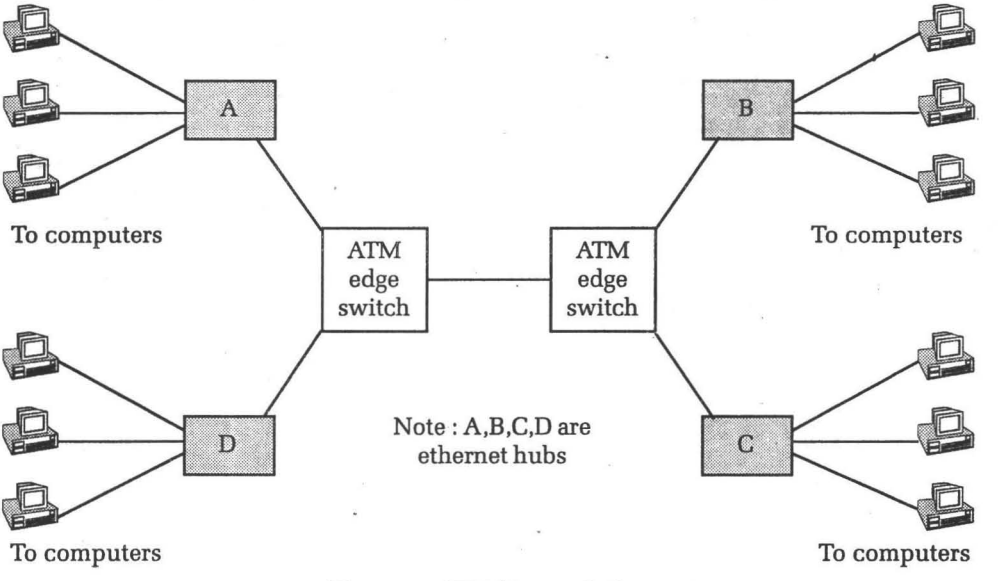


Fig. 18.17 ATM encapsulation

In 1995, ATM forum (the standards body for ATM) accepted a proposal from a consortium of vendors led by IBM for a low speed version of ATM to compete with traditional ethernet and token ring LANs.

ATM 25

- Provides point to point full duplex circuit at 25.6 Mbps in each direction (51.2 Mbps total) from computers to the switch.
- It is an adaptation of token ring that runs over category 3 cable and uses token ring hardware with a chip upgrade.
- Uses a slightly different datalink protocol than wide area ATM's SONET.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

ATM 51

- Designs for the desk top; Developed before ATM 25.
- Provides point to point full duplex circuits at 51.84 Mbps (103.68 Mbps total) from computers to the switch.
- Uses same SONET protocols as wide area ATM.
- Not much Vendor support received as ATM 25.

Both ATM 25 and ATM 51 are choices for desk top connections when ATM backbone networks are used.

- Packet sizes are same
- Protocols same
- No translation or encapsulation required (Switches are simpler, cheaper than edge switches needed for LAN to ATM translation).
- Offers seamless connection to ATM, MANs and WANs
- Simplifying today's multiprotocol mix.

POINTS TO REMEMBER

- Asynchronous transfer mode (ATM) is one of the fastest growing technologies similar to the frame relays. It is a packet switched technology originally designed for use in WAN. It is the cell relay protocol designed by the ATM forum and adopted by the ITU–T.
- ATM uses a fixed length of packets of 53 bytes. (48 bytes payload and 5 bytes of header) more suitable for voice transmissions. ATM data packet is called a cell. Each cell is of the same size. Cells are relatively small, scalable and easy to multiplex basic ATM circuits. Cells are useful to move information from point to point efficiently and with minimal delays.
- Cell network is based on permanent virtual circuit (PVC) routing virtual path identifier indicates the path a cell should take whereas virtual channel identifier indicates the channel a cell should take.
- ATM is a hierarchy of networks connected by associated interfaces. The important interfaces are UNI– user network interface, NNI Network to network interface. The former is between a user and the wide area ATM network. The latter is between two wide area ATM networks. ATM handle or minimise the severity of out of sequences, delay time between packets and bit errors.
- ATM standard defines a series of layers not analogous to those of the OSI model. These are (1) Application adaptation layer (AAL), ATM layer and physical layer.

  AAL allows existing networks to connect to ATM facilities.

  AAL protocols accept transmissions from upper layer services (packet data) and maps them into fixed size ATM cell. ATM layer provides routing, traffic management, switching and multiplexing services. Physical layer defines the transmission medium, bit transmission, encoding and electrical to optical transformations.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

- AAL has a number of groups AL1, AAL2, AAL3/4, AAL5 sub layers. 3 and 4 are combined. AAL2 is part of the ATM design. Each one of the groups are again divided into two sublayers known as convergence sublayer (CS), segmentation and reassembly sublayer (SAR). CS adds overhead and manipulates the data stream at the sending station. At the receiving station, it is vice versa. SAR, at the sending station segments the bit stream into equal sized packets, adds headers/trailers; performs the reverse at the receiving station. AAL1 has a constant bit rate stream, AAL2 is a variable bit rate stream, AAL3/4 is conventional packet switching (Virtual circuit approach / datagram approach); AAL5 are packets needing no information from the SAR layer; No header.
- In the ATM layer, 5 bytes header are added to 48 bytes segment to make it 53 bytes total. ATM switches provide switching and multiplexing.
- Two types of switching found are :

  (i) Virtual path (VP) switching using VPIs

  (ii) Combination of virtual path (VP) switching and virtual channel switching known as Virtual Path and Channel (VPC) switching which uses both VPIs and VCIs – a channel from one VP to another VP.

QUESTIONS

1. What is an ATM? Explain ATM.
2. What were the design goals which stood as a challenge for the designers of ATM?
3. What is the difference between ATM and frame relay.
4. What is packet network ? Explain how it works?
5. What is cell network? Explain how it works?
6. Why should a cell network use a permanent virtual circuit routing strategy?
7. What is VPI? How does the switching done using VPI?
8. If data units are made of same size, How does multiplexing becomes more efficient?
9. Explain the ATM protocol architecture.
10. Discuss the different methods of error detection in each of the AAL types.
11. Compare and contrast different types of AAL.
12. Why AAL 5 has no header added to its SAR layer ?
13. What does ATM layer provides?
14. What is ATM encapsulation? How does it help?
15. Which is the ATM for desktop? Explain.
16. What is multiplexing with different packet sizes? What problems are faced in this?
17. What is the purpose of ATM switches? What are the reasons for designing these switches?

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

FILL IN THE BLANKS

1. ATM is _____ _____ _____.
2. In _____ all data are packet switched, no error control at the intermediate computers within the network.
3. _____ uses fixed length packets of 53 bytes (with 5 bytes overhead and 48 bytes of user data).
4. _____ means that each cell travels independently without being tied to others. However transmission is connection oriented.
5. ATM uses _____ circuit routing.
6. Interface between user and the ATM switch is _____ ____.
7. Interface between two wide area ATM networks is _____.
8. Private and Public UNI does not indicate the _____; they indicate whether the interface is located inside or outside the _____ premises.
9. _____ _____ Interface lies between an ATM switch and wide area ATM network.
10. AAL ____ type process a data stream having a variable bit rate.
11. AAL ____ type process a data stream having a constant bit rate.
12. AAL ___ intended to support connection oriented service and AAL ___ intended to support connectionless services.
13. AAL ____ type is designed to support conventional packet switching that uses the approach of virtual circuit.
14. In the SAR sublayer of _____ the payload is 48 bytes and there is no added header or trailer.
15. In the SAR sublayer of _____ Header 1 byte is added and 2 bytes of trailer are added to 45 byte pay load.
16. In the SAR sublayer of _____ one byte of header is added to 47 bytes of data.
17. In UNI cell header, a _____ _____ _____ field is used for connection purpose.
18. The final product of the SAR will have data packet that is _____ bytes long.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Answers

1. asynchronous transmission mode
2. ATM
3. ATM
4. Asynchronous
5. virtual
6. Private UNI
7. NNI
8. ownership ; users
9. public UNI
10. 2
11. 1
12. 3, 4
13. 5
14. AAL5
15. AAL2
16. AAL1
17. virtual path identifer
18. 48

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

19

SYNCHRONOUS OPTICAL NETWORK SONET/SDH

The *synchronous optical network* has been recently accepted by ANSI as a standard for optical transmission at gigabytes per second speeds. It is a synchronous network.

Fiber optic cable today is occupying the first place because of its :

- High bandwidths to suit highest data rate technologies (e.g. video conferences)
- To carry large number of lower rate technologies at the same time.

Its importance is very much felt and is extensively used in conjunction with the development of technologies because of its advantages over the conventional ones. A need came for standardisation due to internet working among the existing proprietary system. ANSI in USA and ITU-T in Europe have defined standards independently but they are fundamentally similar and compatible.

ANSI standard is called as SONET – Synchronous optical network. ITU (T) standard is called as SDH – Synchronous Digital Hierarchy. Specialities of SONET/SDH are :

- It is a synchronous network.
- Contains recommendations for the standardisation of the fiber optic transmission system (FOTS) equipment sold by different manufacturers.
- SONET/SDH physical specifications and frame design have mechanisms which allows to carry signals from incompatible tributary systems (E.g. Asynchronous services like DS-0, DS-1). It is this flexibility makes SONET popular for universal connectivity.
- It is a multiplexed transport mechanism (no switching) and can be the carrier for broad band services (ATM and B-ISDN).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

A single clock handles the timing of transmissions and equipment across the network. It adds a level of predictability to system, coupling with a powerful frame design. It enables individual channels to be switched for streamlining transmission, speed improvement, cost reduction without demultiplexing the entire signal.

19.1 SYNCHRONOUS TRANSPORT SIGNALS

SONET defines a hierarchy of signalling levels called synchronous transport signals (STSs). The physical links defined to carry each level of STS are called optical carriers (OCs). T_3 and T_4 services are being replaced by SONET services. Its transmission speeds begin at the OC-1 level (optical carrier level) of 51.84 Mbps. OC levels describe the conceptual and physical specifications of the links required to support each level of signalling. Each succeeding rate in the SONET fiber hierarchy is defined as a multiple of OC-1 with SONET rates defined as high as OC-192 or 9.953280 gigabytes per second. The most popular OCs are OC-1, OC-3, OC-12, and OC-48. The implementations of the specification of OCs are left to the manufacturers.

STS	OC	Rate (Mbps)	STM
STS-1	OC-1	51.840	
STS-3	OC-3	155.520	STM-1
STS-9	OC-9	466.560	STM-3
STS-12	OC-12	622.080	STM-4
STS-18	OC-18	933.120	STM-6
STS-24	OC-24	1244.160	STM-8
STS-36	Oc-36	1866.230	STM-12
STS-48	OC-48	2488.320	STM-16
STS-96	OC-96	4976.640	STM-32
STS-192	OC-192	9953.280	STM-64

Note : STS -1 is designed to accommodate data rates equivalent to those of D_3 (44.736 Mbps). The difference in capacity is provided to handle the overhead needs of the optical system.

Fig. 19.1 SONET circuits

Each level above OC-1 is created by multiplexing. OC-1 is the slowest optical transmission rate 51,840,000 bits/second and is slightly faster than D-3 service and line of 44, 376,000 bits/second. Lowest SONET level supports greater bit than the highest T level that is T3. SONET is available in most large cities worldwide (though not fully implemented in all locations). Several telephone companies now use OC-12 circuits at 622.08 Mbps to carry inter-exchange traffic. With these speeds it is easy to see only the telephone companies prefer installing fiber optic cable MANs in most cities and for long distance circuit. It is also seen that even new undersea cables are optical fiber instead of copper.

STS-3 rate is 3 times to the STS-1 rate; STS-9 rate is exactly half the STS-18.

STS-3 rate = 3 x STS-1 rate

STS-9 rate = 9 x STS-1 rate

STS-18 rate = 18 x STS-1 rate or 6 x STS-3 rate
(6 STS-3 channels can be multiplexed into 1 STS-18)

Concept of hierarchy would be similar to that of DS signals and T-lines.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

SDH has a similar system like SONET called *synchronous transport* module (STM). It is intended to be compatible with European hierarchies such as E-lines and with STS levels. Lowest STM level is STM-1 is defined at 155.520 Mbps (equal to STM-3)

Physical configuration

A SONET system is as shown below :

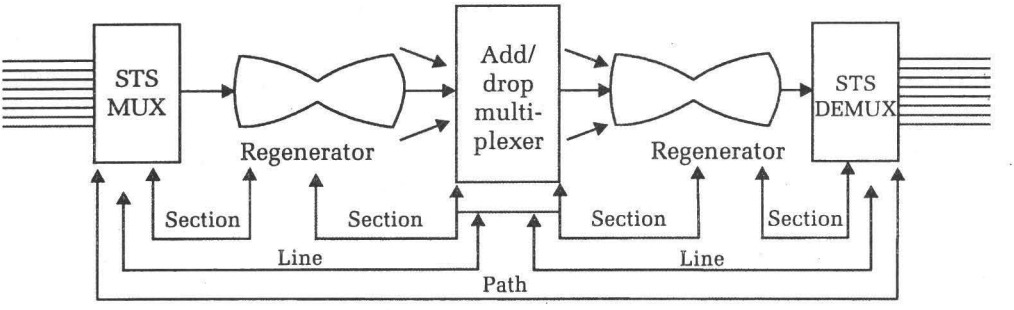


Fig. 19.2 A SONET system

19.2 SONET DEVICES

The most important three basic devices are :

- STS multiplexers : (Converts electronic signals to optical signals; multiplexes the incoming signals to create a single STS signal (STS-1, STS-3 etc)
  - Represents the beginning and end points of a SONET link.
  - Provides the interface between a tributary network and SONET.
  - Devices in between them can be of any number and configuration required by the system.
- Add/drop multiplexers: (Adds signals coming from different sources into a given path or remove a desired signal from the path and redirect it without demultiplexing the entire signal. Instead of relying on timing and bit positions, add/drop multiplexers use header information (addresses and pointers) to identify individual streams).
  - Add/drop multiplexers allow insertion and extraction of SONET paths.
- Regenerators : (STS generator is a repeater; Takes a received optical signal and regenerates it; Adds a function to those of physical layer repeaters. SONET regenerator replaces the existing overhead information (header information) with new information; devices function at the data link layer).
  - Extend the length of the links possible between generator and receiver.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

In figure 19.2, STS multiplexers are fed with a number of electronic signals. These are combined into single optical signal, which is transmitted to a regenerator. It is recreated whatever has been picked up in the transit (without noise).

Regenerated signals from a number of sources are fed into an add/drop multiplexer. This reorganises the signals (if found necessary), sends them out as per the interactions by information in the data frames. These remultiplexed signals are sent to the next regenerator and then to the receiving STS multiplexer. Finally, they are returned to a format usable by the receiving signals. The various levels of SONET connections are shown in the figure :

- Sections– Optical link connecting two neighboring devices (say multiplexer to multiplexer, multiplexer to regenerator, regenerator to regenerator etc.)
- Line – Portion of the network between two multiplexers (say STS multiplexer to add/drop multiplexer, two add/drop multiplexers, two STS multiplexers etc)
- Path – End to end portion of the network (say between two STS multiplexers)

A simple SONET links two STS multiplexers directly to each other (the section, line and path are the same).

19.3 SONET LAYERS

SONET has four functional layers as shown below :

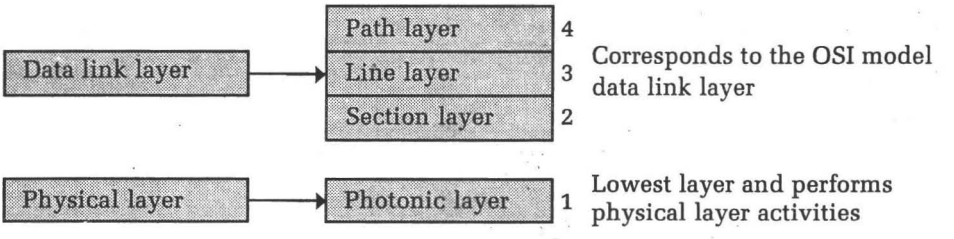


Fig. 19.3 SONET layers

- **Photonic layer** covers i) Physical specifications for the optical fiber channel (ii) Sensitivity of the receiver iii) multiplexing functions etc. SONET uses NRZ encoding – presence of light as 1 and absence of light as 0.
- **Section layer** covers (i) Framing (ii) Scrambling (iii) Error control. It is responsible for the movement of a signal across a physical section. Section layer overhead is added to the frame at this layer.
- **Line layer** responsible for the movement of a signal across a physical line. Overhead of this layer is added to the frame. STS and add/drop multiplexers provide the functions.
- **Path layer** – For the movement of a signal from its optical source to its optical destination. Path layer overhead is added. STS multiplexers provide path layer functions.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Optical source – Here the signal is changed from electronic form into an optical form, multiplexed with other signals, encapsulated in a frame.

Optical destination – Here the received frame is demultiplexed individual optical signals are changed back into their electronic forms.

Device – Layer relationship

Relationship between devices (used in SONET transmission) and the four layers of the standard are as shown below in figure 19.3.

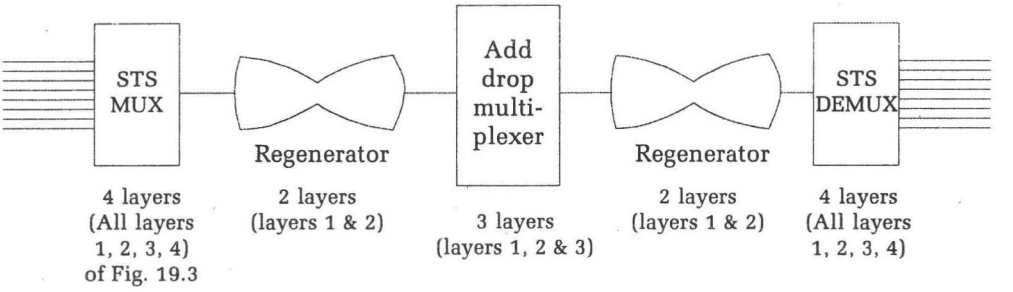


Fig. 19.4 Device-layer relationship

19.4 THE SONET FRAME

Data received from electronic interface (e.g. T_1–line) is encapsulated in a frame at the path layer; overhead is added. After this additional overhead is added to the next two layers (line layer and section layer). Then the frame is passed on to the photonic layer, where it is transformed into an optical signal. As found in other protocols, SONET overhead is not added as headers and trailers. It would be inserted at a variety of locations in the middle of the frame. See the figure 19.5.

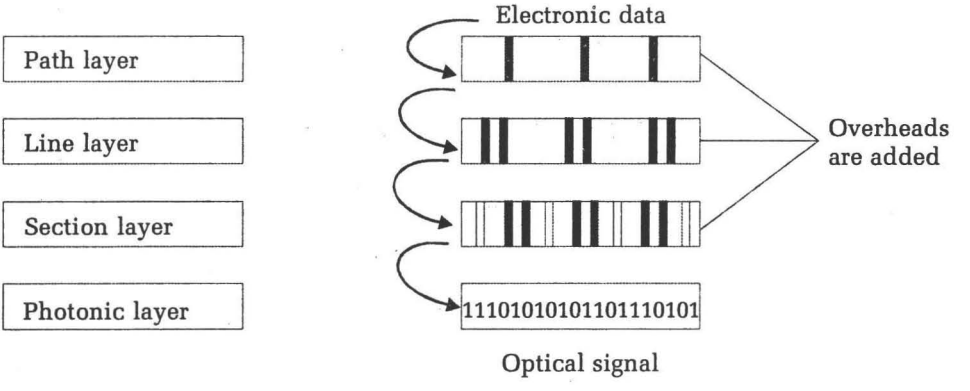


Fig. 19.5 Data encapsulation in SONET

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Frame format

STS-1 frame basic format at the photonic layer is as shown in figure 19.6.

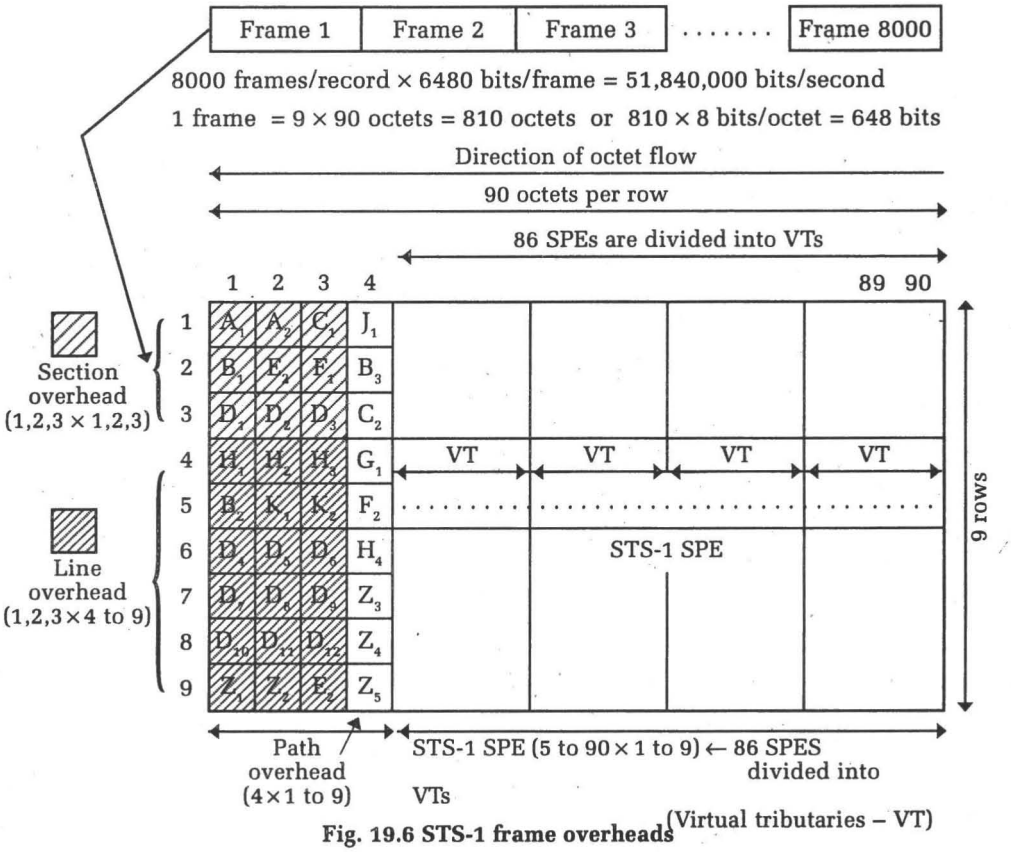


Fig. 19.6 STS-1 frame overheads

Section overhead of STS-1 frame (3 x 3 = 9 octcts): A_1, A_2, C_1, B_1, E_2, F_1, D_1, D_2, D_3

Where A_1 is Alignment 1; A_2 is alignment 2; E_1 orderwise byte; D_1, D_2, D_3 – Management; B_1 Parity byte; F_1 User

Line overhead is (3 x 6 = 18 octcts): H_1, H_2, H_3, B_2, K_1, K_2, D_4, D_5, D_6, D_7, D_8, D_9, D_{10}, D_{11}, D_{12}, Z_1, Z_2, E_2,

Where H_1 H_2 H_3 pointers
K_1, K_2 - Automatic protection switching bytes
D_4 - D_{12}; Data communication channel bytes.
B_2 - Line parity byte
E_2 - Orderwise byte
Z_1, Z_2 - Growth bytes

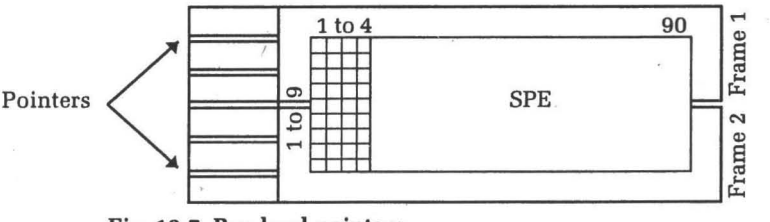


Fig. 19.7 Pay load pointers

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

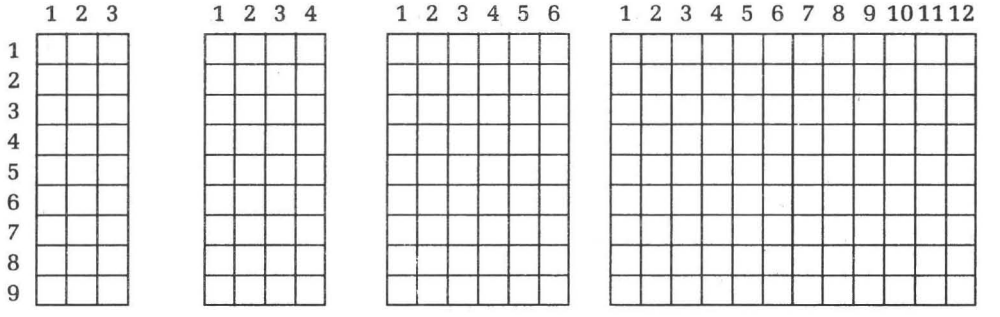
Path Overhead is
9 x 1 = (Nine bytes)

J_1	J_1 = Path trace byte
B_3	B_3 = Path parity byte
C_2	C_2 = Path signal label byte
G_1	G_1 = Path status byte
F_2	F_2 = Path user channel byte
H_4	Z_3, Z_4, Z_5 = Growth bytes (reserved)
Z_3	H_4 = Virtual tributory indicator
Z_4	
Z_5	

Difference between section overhead, line overhead and path overhead is as shown in table 19.1.

Types of VTs

The different types of VTs are shown below :



VT 1.5	VT 2	VT 3	VT 6
8000 Frames/s × 3 columns × 9 rows × 8 bits = 1.728 Mbps	8000 Frames/s x 4 columns x 9 rows x8 bits = 2.304 Mbps	8000 Frames/s x 6 columns x 9 rows x8 bits = 3.456 Mbps	8000 Frames/s x 12 columns x 9 rows x8 bits = 6.912 Mbps

Note :

VT 1.5 means 2 x1.5 columns	= 3 columns	(accomodates US DS-1 service of 1.544 Mbps)
VT 2 means 2 x2 columns	= 4 columns	(accomodates the European CEPT - 1 service of 2.048 Mbps)
VT 3 means 2 x3 columns	= 6 columns	(accomodates DS-1C service fractional DS - 1, 3.152 Mbps)
VT 6 means 2 x6 columns	= 12 columns	(accomodates DS-2 service, 6.312 Mbps)

Fig. 19.8 Types of VTs

When number of tributaries (say two or more) are inserted into STS–1 frame, they are interleaved column by column. SONET uses mechanisms to identify each VT and separating them with demultiplexing the entire stream.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Section overhead	Line overhead	Path overhead
• Consists of nine octcts. • **Alignment bytes** used for framing and synchronisation. These bytes alert a receiver that a frame is arriving and give the receiver a predetermined bit pattern on which to synchronise. The bit patterns are hexadecimal and binary are : F6 → 11110110 (A1) 28 → 00101000 (A2) • **Identification byte C_1** carries a unique identifier for the STS-I frame. This byte is necessary when multiple STS-Is are multiplexed to create a higher rate STS (STS-3, STS-9, STS-12 etc). Information in this byte allows the various signal to be easily recognised upon demultiplexing. • **Parity byte B_1** is for bit interleaved parity (BIP-8); value based on the section header of the previous STS-1; Inserted in the current STS-1; functions as a longitudinal redundancy check. • **Orderwire byte E_1** in consecutive frames form a channel of 64 kbps (8000 frames per second x 8 bits per frame). Channel used for communication between regenerators, or by terminals and regenerators. • **User's byte F_1** in consecutive frames form a 64 Kbps channel reserved for user needs at the section level. • Management bytes D_1, D_2, D_3 together form a 192 Kbps (3 x 8000 x 8) called the data communication channel; required for operation, administration and maintenance (OAM) signalling.	• Consists of nine bytes. • **Pointer bytes** H, H_2, H_3 are pointers; identifying the location of the pay load in the frame when the payload starts somewhere other than at the beginning of the STS envelope. (See fig. 19.6). Pointers are essential in several situations. • SONET is a synchronous protocol frames are built by matching the timing of the data input to the network frame functions. For this reason data collected from asynchronous network inputs may not be synchronised with the SPE and may end up occupying two frames. Pointers enable SONET to a accomodate such framing discrepancies. • Bytes H, H_2, H_3, together form a pointer to the beginning byte of the pay load; More complex uses for pointers also exist. • **Line parity bit B_2** is for bit interleaved parity, similar to B_1. • **Automatic protection switching bytes K_1** and K_2 in consecutive frames form a 128 Kbps channel used for automatic detection of problems in line terminating equipment (multiplexers). **Data Communication Channel bytes D_4 to D_{12}** in consecutive frames form a 376 Kbps channel that provides the same services as the D_1-D_3 bytes (OAM). But at the line rather than the sectional level. **Growth bytes Z_1 & Z_2** are reserved for future use. **Orderwire byte E_2** is consecutive frames form a 64 Kbps channel that provides the same functions as the E_1 order byte, but at the line level.	• Consists of nine bytes. • **Path trace byte J_1** in consecutive frames form a 64 Kbps channel used for tracking the path; It sends a continuous 64 bit string to verify the connection. Choice is left to the application program. • **Path Parity byte B_3** is for bit interleaved parity. Similar to B_1 and B_2; But calculated for the path leader. **Path signal label byte C_2** : It is path identification in byte used to identify different protocols; used at higher levels (DDDI or SMDS) **Path status byte G_1** sent by the receiver to communicate its status to the sender. **Path user channel byte F_2** These bytes in consecutive form like the F_1 form a 64 Kbps channel that is reserved for user needs but at the path level. **Virtual tributary indicator** : It is the multiframe indicator. Indicates payloads that cannot fit into a single frame. **Growth bytes** (Z_3, Z_4 and Z_5) reserved for future use. **Virtual tributaries (VT)** : SONET is designed for carrying broad band pay loads; digital hierarchy rates DS–1 to DS-3 are lower than STS-1. To make SONET compatible with current hierarchy, DS-1 to DS-3, its frame design includes a system of VTs. AVT is (i) a partial load that can be inserted into an STS-1 and combined with other partial pay load to fill out the frame (ii) Instead of using all 86 pay load columns of an STS-1 Frame for data from one source, SPE is sub-divided and each component is called a VT.

Table 19.1

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

Multiplexing STS Frames

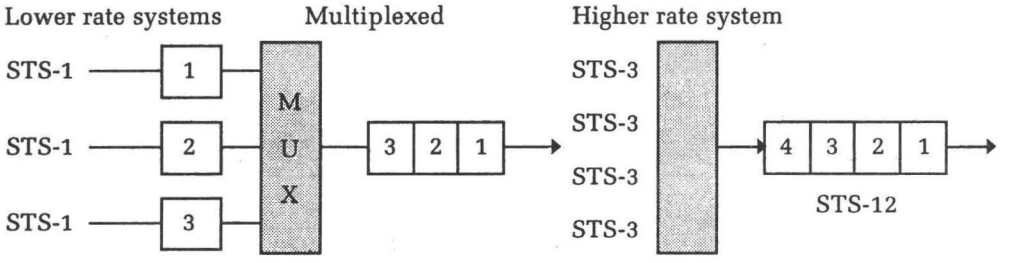


Fig. 19.9 STS Multiplexing

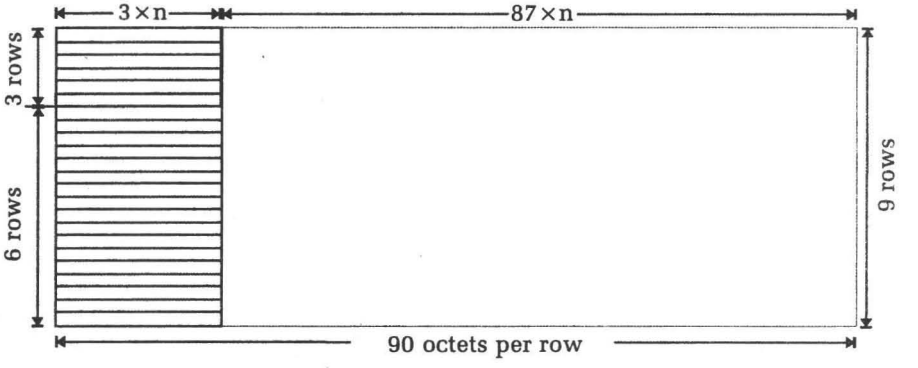


Fig. 19.10 STS-n (made up of lower rate STS-1s)

ATM convergence to SONET/SDH

ATM's most important physical carrier is taken as SONET's STS-3 service (STM-1 in Europe's SDH). ATM provides multiplexing. Hence entire pay load of STS-3 can be used for cell transport without the additional overhead (as required by the other systems.)

- Each row of the frame = 270 octets (3 x 90)
- Nine octets used for section overhead/line over head
- One Octet used for path overhead
- Remaining 260 octets carries 5 cells = (5 x 53) = 265 (pattern as shown in the figure)
- Most rows have partial cells at both ends.

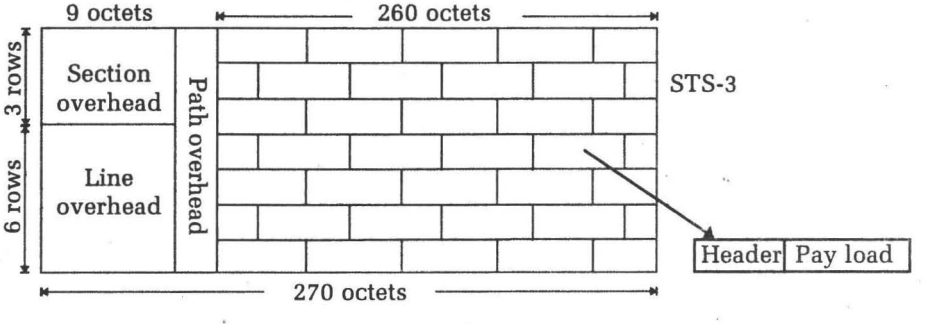


Fig. 19.11 ATM in an STS-3 envelope/one possible mapping

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

POINTS TO REMEMBER

- Synchronous optical network has been accepted by ANSI as a standard for optical transmission at gigabytes per second speeds. Specialities of SONET/SDH are : It is a synchronous net work; it contains recommended actions of the fiber optic. Transmission system (FOTS) equipment are sold by different manufacturers.
- ANSI standard is called as SONET and ITU-T standard is called SDH (Synchronous digital hierarchy).
- SONET has defined a hierarchy of signals (similar to DS) called synchronous transport signals (STSs). The physical link defined to carry each level of STS are called optical carriers (implementation of STSs). STS, OC and STMs are comparable.
- SONET has four distinctive layers; data layer, line layer, section layer. These are similar to OSIs data link layer, whereas photonic layer is similar to physical layer. It is the lowest layer each of these layers is responsible for signal transfer across a specific portion of the transmission path.
- The various devices and the layer relationship of the SONET system are :
  - (i) STS Multiplexer combines several optical signals to make an STS signal (four layers 1, 2, 3, 4 layers)
  - (ii) Regenerator (2 layers 1, 2 layers) Removes noise from an optical signal.
  - (iii) Add/drop multiplexer (3 layers 1, 2, 3 layers) – Adds STS signals from different paths and removes STS signals from a path.
  - (iv) STS Demultiplexer – (4 layers 1, 2, 3, 4, layers)

    [Layer 1 – Photonic layer; 2 – Section layer; 3 – line layer; 4 – path layer]
- STS-1 frame uses 810 octets (9 rows and 90 columns) and transmit at a rate of 51,840 Mbps. It has a section overhead of nine octets. Line overhead of 18 bytes and a path overhead of 9 bytes. SONET is designed to carry broad band pay loads. Overhead and data (pay load) in a STS-1 are arranged in a matrix configuration of 810 octets.
- SONET is backward compatible with the recent DS hierarchy through the virtual tributary (VT) concept. An STS pay load is a combination of several VTs and lower rate STS can be multiplexed to get new STSs with higher data rates.

QUESTIONS

1. What is SONET/SDH? What are the specialities of SONET/SDH?
2. Explain synchronous transport signals (STSs) in SONET?
3. What are optical carriers?
4. How is an STS multiplexer differs from an add/drop multiplexer?
5. How does STS levels, OC levels and STM levels compare ?

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

6. Explain the SONET system? What are the basic devices of SONET? Explain each one of them.
7. Explain the purpose of the pointer in the line overhead.
8. Explain the functional layers of the SONET.
9. Compare the STS hierarchy with DS hierarchy.
10. Explain the SONET frames and SONET formats.
11. How the data encapsulation takes place in SONET? Explain.
12. Compare and contrast the different types of overheads found in SONET.
13. What are virtual tributaries? What are the types?
14. Explain multiplexing of STS frames.
15. How does the ATM convergence takes place to SONET/SDH?

FILL IN THE BLANKS

1. SONET is _____ _____ network.
2. SDH is _____ _____ _____.
3. The optical link between any two SONET devices is known as a _____.
4. SONET's _____ layer transfers a signal across a physical line.
5. SONET is a standard developed by _____; SDH is a standard developed by _____.
6. An _____ _____ remove signals from a path in a SONET system.
7. _____ layer transfer's data from its optical source to its optical destination in a SONET.
8. Framing, scrambling and error handling are done in _____ layer in a SONET.
9. _____ layer of SONET corresponds to the OSI model's physical layer
10. A _____ removes noise from a signal, can also add or remove headers in SONET.
11. AN STS multiplexer operates in _____ layers.
12. A regenerator operates in _____ and _____ layers.
13. An add/drop multiplexer operates in _____, _____ and _____ layers.
14. An STS demultiplexer operates in _____ layers.
15. The synchronous pay load envelope (SPE) of an STS-1 frame contains _____ _____ and _____ _____ .
16. The maximum number of VT6 that STS -1 can accommodate is ____; VT 1.5 is ____; VT 3 is ____.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

17. SONET is a standard for _____ _____ cable.
18. _____ overhead contains the pointers to the payload.
19. ATM's most important physical carrier is SONET's _____ service.
20. During multiplexing of STS frames, 3 lower rates of STS-1s can be combined into one _____; and 4 _____ can be combined to form one STS-12 of higher rate systems.

Answers

1. synchronous optical
2. synchronous digital hierarchy
3. section
4. path
5. ANSI, ITU(T)
6. Add/drop multiplexer
7. Path
8. section
9. Photonic
10. regenerator
11. all (path, line, section & photonic)
12. section ; photonic
13. line, section and photonic
14. all (path, line, section, photonic)
15. user data ; path overhead
16. 12, 3, 6
17. fiber optic
18. Path
19. STS-3
20. STS-3, STS-3s

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-12 22:04:12.

UNIT 5

CHAPTER 20

NETWORKING AND INTERNETWORKING DEVICES

CHAPTER 21

TRANSPORT LAYER

CHAPTER 22

UPPER OSI LAYER

CHAPTER 23

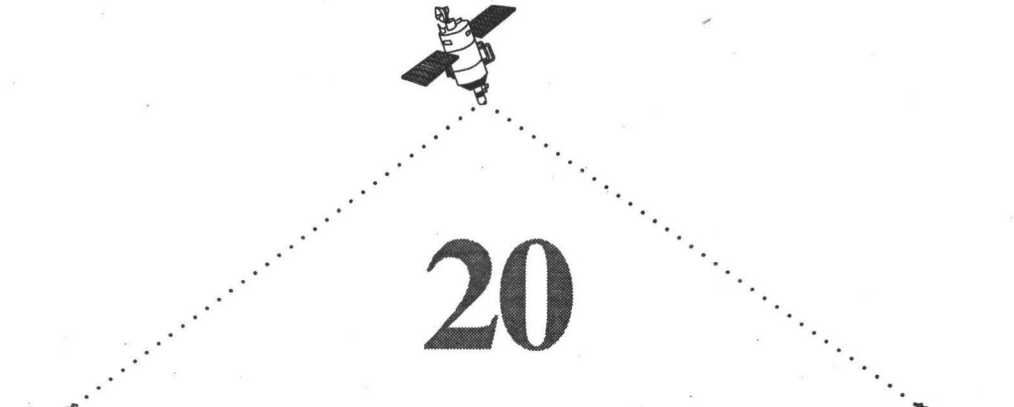
TRANSMISSION CONTROL PROTOCOL (TCP)/ INTERNET PROTOCOL

CHAPTER 24

EMERGING TECHNOLOGIES COMPUTER TELEPHONY AND IP TELEPHONY

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.



20

NETWORKING AND INTERNETWORKING DEVICES

In a network, a number of devices say two or more are connected for the purposes of sharing the data or resources. A LAN can cover much more distance than its media can handle effectively. Alternatively, the number of stations are many for efficient frame delivery or management of the network and the network may need to be subdivided. Repeater or Regenerator is used into the network to increase the coverable distance in the former case. In the latter case, a device called a bridge is inserted for traffic management. Internet or internetworking is an interconnection of individual networks. If an internet is to be created, internet working devices called routers and gateways are to be used. These devices are designed to overcome

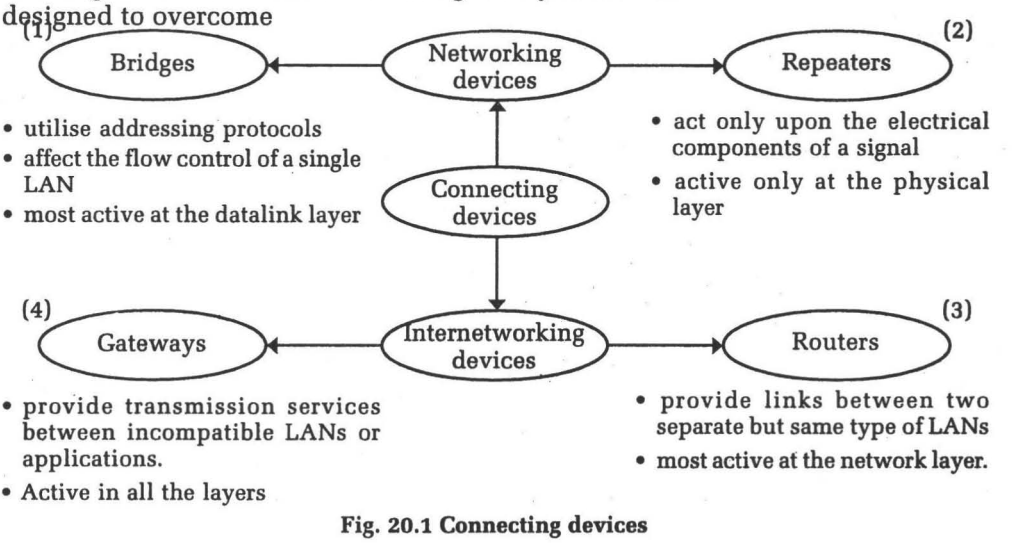


Fig. 20.1 Connecting devices

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

obstacles to interconnection without disrupting the independent functioning of the networks. Terms internet and Internet are used in separate contexts (small *i* is used to mean interconnection of networks; capital I is used to mean a world wide network). An internet is not the same as Internet.

The above four device types interact with protocols at different layers of the OSI models.

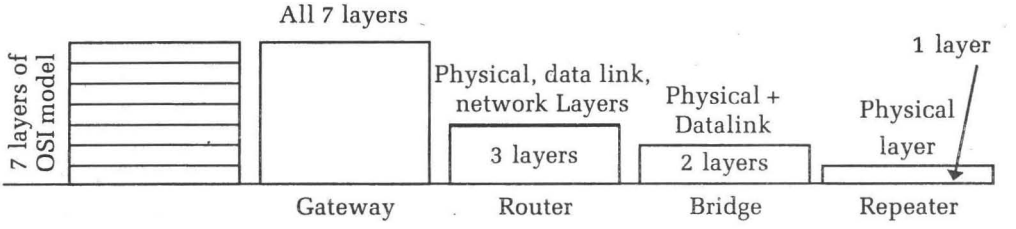


Fig. 20.2 Connecting devices with the OSI model

Repeaters

Repeater or Regenerator is an electronic device used on the networking devices and is active only at the physical layer of the OSI model (See figure 20.2). The information which is carried on signals within a network can travel a fixed distance before attenuation (that is weakening of the signal due to fiction) or interference from noise endangers the integrity of the data. To avoid attenuation, telephone lines have repeaters or amplifiers spaced throughout their length. The distance between them depends on the amount of power lost per unit length of the transmission line. Amplifier takes the incoming signal and increases its strength, and retransmits it on the next section of the circuit. They are typically based on analog circuits such as the telephone company's voice circuits. Attenuation is the deciding factor for deciding the distance between the repeaters, though one to ten mile intervals are common.

One thing is to be noticed is that on analog circuits, it is important to recognise that the noise and distortion present are also amplified, along with the signal. This shows some noise existing from a previous circuit is regenerated and amplified each time the signal is amplified. Repeaters are commonly used on digital circuits. The incoming signal received from a repeater translates it into a digital message and retransmits the same. Since the message is recreated at each repeater, noise and distortion from the previous circuit are not amplified, thus providing a cleaner signal and resulting in a lower error rate for digital circuits. A repeater installed receives the signal before it becomes too local or get corrupted, regenerate the original bit pattern, and puts the refreshed copy back on to the link. The signal, with the corruption removed, is transmitted a second time from a location closer to the transmission.

Many of the experts compare repeater to an amplifier. Some do not agree since the amplifier cannot discriminate between intended signal and noise. Amplifier amplifies everything in the same proportion of whatever is fed. But a repeater does not amplifies the signal. But it regenerates it. When it receives a weekend/corrupted signal, it creates a copy bit for bit, at the original strength.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

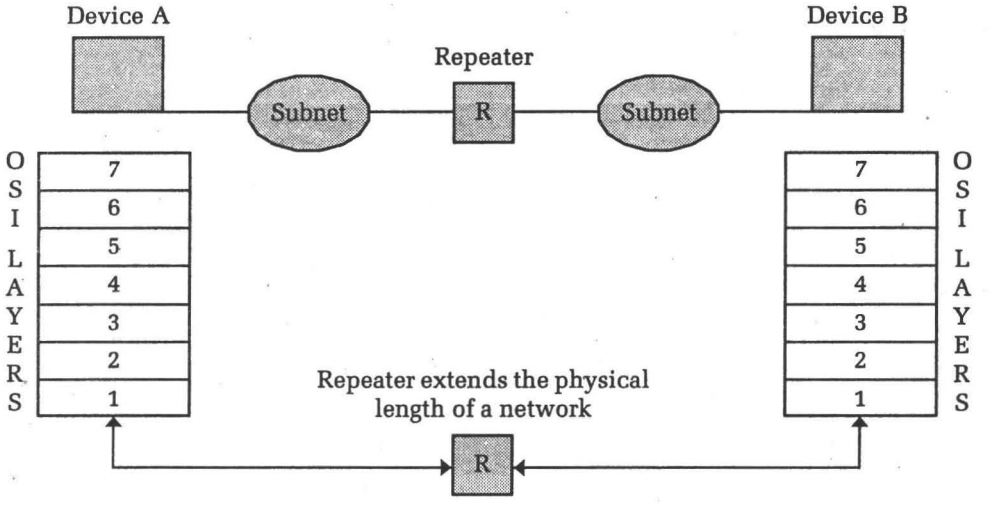


Fig. 20.3 A repeater in the OSI model

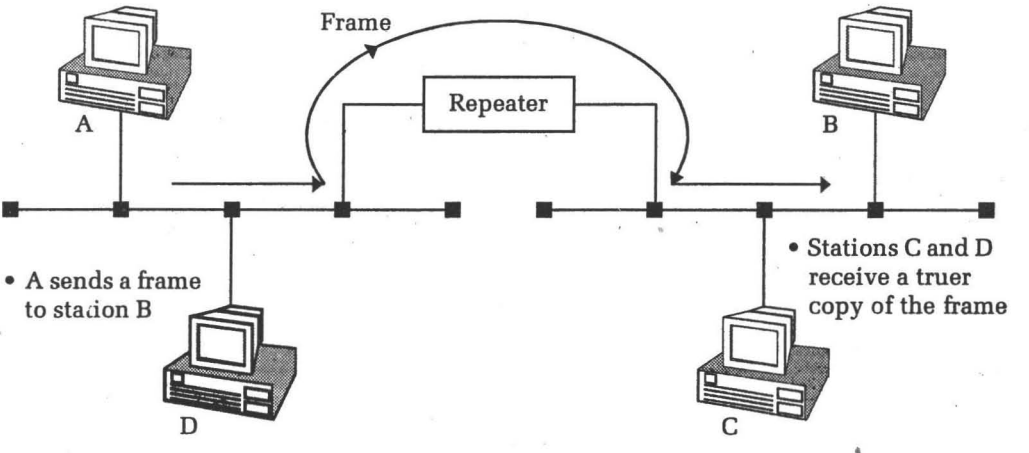


Fig. 20.4 A repeater

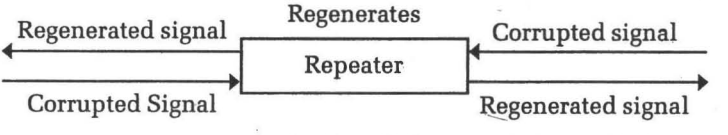


Fig. 20.5 Repeater Functions (Right to left transmission and vice versa)

Bridges

Bridges are used to connect two LAN segments :

- Using the same data link and network protocol
- Operates at the physical and data link layers of the OSI Model.
- Connects the same or different types of cable.

Bridges are more sophisticated than hubs because they only forward those messages that need to go to the other network segments.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

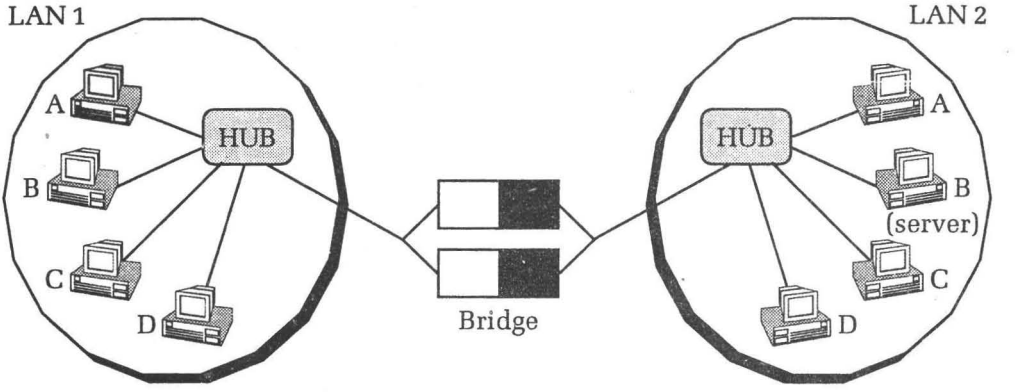


Fig. 20.6 Bridge to connect two LANs

Bridges divide a large network into smaller segments. It contain logic that allows them to keep the traffic for each segment separate (unlike repeaters). Bridges are repeaters that are smart enough to relay a frame only to the side of the segment containing the intended recipient.

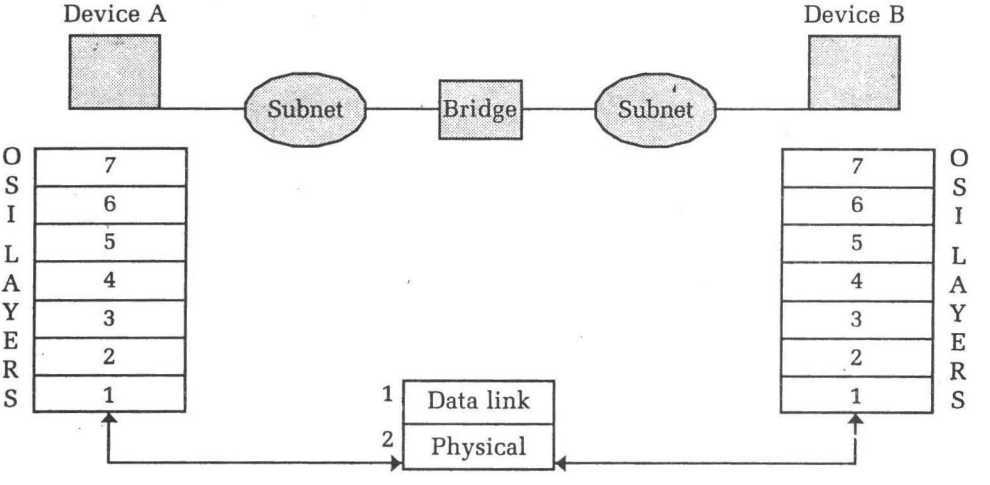


Fig. 20.7 A Bride in the OSI model

Bridges filter traffic; makes them useful for controlling congestion; isolating problem links, provide security through partitioning of traffic. They do not modify the structure or contents of a packet in any way, hence used only between segments that use the same protocol.

Bridges 'learn' whether to forward packets. When a bridge receiver packet, it reads the packet source address; compares this address to its own internal routing table; If source address is not in the routing table, the bridge adds it. The bridge is set to learn the address of the devices on the network. If destination address is not in the routing table, the bridge forwards the packet to all networks or network segments except the one on which it was received. If the destination address is on the routing table and as well as on the same network segment as the source address the bridge automatically discards the packet, a process known as

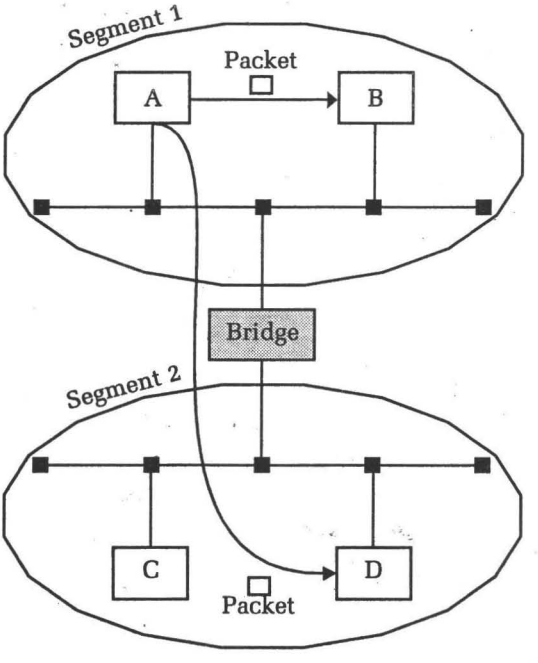
Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

filtering. The bridge can discard the packet because the station to which it is addressed will already have been received and copied it. If the destination address in the routing table but not on the same network segment, the bridge determines the port associated with the address and forwards the packet to that port. Some bridges check packets for errors and forward only the error-free ones.

Bridges are both hardware and software combination. A typical bridge is a block box; sets between the two networks; has its own processor, memory and software; operations are transparent to the network user. A bridge can also be regular computer with two or more NICs and special bridging software. A simple bridge as shown in figure 20.8 can connect two LAN segments in the same building and also useful if a LAN cable gets too long or too busy. One LAN can be broken into two segments and bridge them.

A bridge operates at the datalink layer accesses the physical addresses of all stations connected to it. If the frame enters a bridge, the bridge not only regenerates the signal and also checks the addresses of destination and forwards the new copy only to the segment to which the address belongs. A bridge encounters a packet, it reads the address contained in the frame, compares that address with a table of all stations on both segments. If it hits (find a match), it discovers to which segment the station belongs and relays the packet only to that segment.



- Segment 1 and segment 2 are connected by a bridge.
- A packet from station A to Station B is blocked from crossing into segment 2.
- A packet from station A to station D is allowed by the bridge to cross, relays it to the segment 2, where it is received by station D.

Fig. 20.8 Functions of a bridge

The selection of a bridge depends on a look up table containing the physical addresses of every station connected to it. The table indicates to which segment it belongs. The table generation and the segments connected by a single bridge determines the type and cost of the bridge.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Three types of bridges

These are :

(i) Simple bridges, (ii) Learning bridges, (iii) Multiport bridges

Simple bridge

- Old time (most primitive) type
- Least expensive
- Links two segments
- Contains a table that lists the addresses of all the stations in each of them.
- Addresses are to be entered manually
- Before functioning, the operator must set down and program the addresses of every station.
- If a new station is added, the table must be modified.
- For removal of a station, the invalid address must be deleted.
- Logic is pass/no pass variety, a configuration that makes a simple bridge straight forward and inexpensive to manufacture.
- Installation and maintenance are time consuming.
- Potentially more trouble than the cost savings are worth.

Learning bridges

- Builds its table of station addresses on its own as it performs functions.
- When first installed, its table is empty.
- When it encounters each packet, it looks at destination/source addresses.
- Checks the destination to decide where to send the packet.
- If not able to recognise the destination address, it relays the packet to all of the stations on both segments.
- Uses the source address to build its table.
- When it reads the source address, it notes which side the packet came from, associates that address with the segment to which it belongs.
- When the first packet transmitted by each station, bridge learns the segment associated with that station.
- Finally it would develop a complete table of address/segment stored in its memory.
- Process continues even after the formation of table for self-updating e.g. a packet from A to D stations, they include NICs on the computer's and suppose the stored segment locations for both stations are wrong. The bridge corrects since it is constantly checking the source address of received packets. It updates its table noticing that A is in the lower segment (packet is coming from A) and D is in upper segment.

The logic required to achieve this type of automation makes a learning bridge expensive than simple bridge. Occasions are there where the cost is worth.

Multiport bridges

It can be of (i) simple or (ii) learning. It is used to interconnect for more than two same time segments.

One vendor's bridge may actually provide the functions of a router.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Multiprotocol bridges

- Translate between different data link layer protocols.
- Receives data from one network using one datalink protocol (Ethernet) and translates it into another protocol (token ring) for use on another network.
- Most common type of this bridge translates between ethernet and token ring.

Protocol filtering bridges

- Multiprotocol bridges wherein it forwards only packet of a certain type (e.g. understands ethernet and token ring and forwards only ethernet packets)

Encapsulating bridges

- To connect networks with different datalink protocols.
- Simply surrounds a packet using one protocol with a packet of a different protocol for transmission over a backbone network, which uses yet another protocol.
- When message is received at destination LAN, the encapsulating bridge at the other end removes the encapsulating packet and transmits the original packet.

Routers

Routers connect two or more LANs that use the same or different (usually different) data link protocols but the same network protocol. Routers and bridges are simple hardware devices capable of executing specific tasks. Routers are more sophisticated; have access to network layer addresses and contain software to determine which of several possible paths between those addresses best for a particular transmission. They operate in three layers of OSI model i.e. physical, datalink and network.

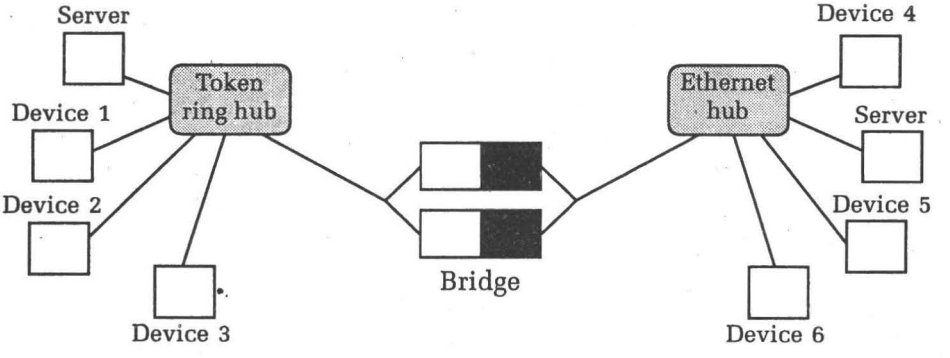


Fig. 20.9 Use of routers to connect LANs

- Routers only forward those messages that need to go to other networks.
- It chooses the best route between networks out of the several possible routes.
- Knows its own location and packets final destination; it looks in a routing table to identify the best route or path.
- Posses a high level of software intelligence than either repeaters or bridges as they operate at the network layer.
- May be black boxes or computers with several NICs.

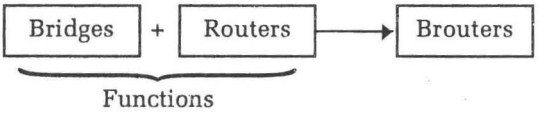
Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Performs more processing than bridges, hence operates slowly.
- Allows the logical separation of an internetwork into many networks using addressing scheme which distinguishes between device addresses at the data link layer and internetwork addresses at the network layer.
- Routing systems use the internet work address specified in the network protocol packet and their routing tables for routing decisions.
- Router only processes messages that are specifically addressed to it unlike a bridge. To send a message to a computer on another network the sender must specify the internetwork address of the destination computer in the network layer packet, send the packet to the router, which will process the packet by building new datalink layer packet, then transmits that on the other network.
- It attempts to make no changes the network packet and user data it receives. If changes needed (when the maximum datalink layer packet size on one network is different from another), it splits a message into several messages for transmission.

Brouters

These are devices which combine the functions of both bridges and routers operating at both the datalink and network layers. A brouter connects both same datalink type network LAN segments and different datalink ones.



Like a bridge, it examines the datalink layer addresses of all packets on the network and forwards them to any other network of the same type. At the same time, it processes any messages addressed to it by looking at the network layer protocol to see if the messages needs to be forwarded to a different datalink layer type network. The advantage of brouters is that they are as fast as bridges for same datalink type networks. It can also connect different datalink type networks.

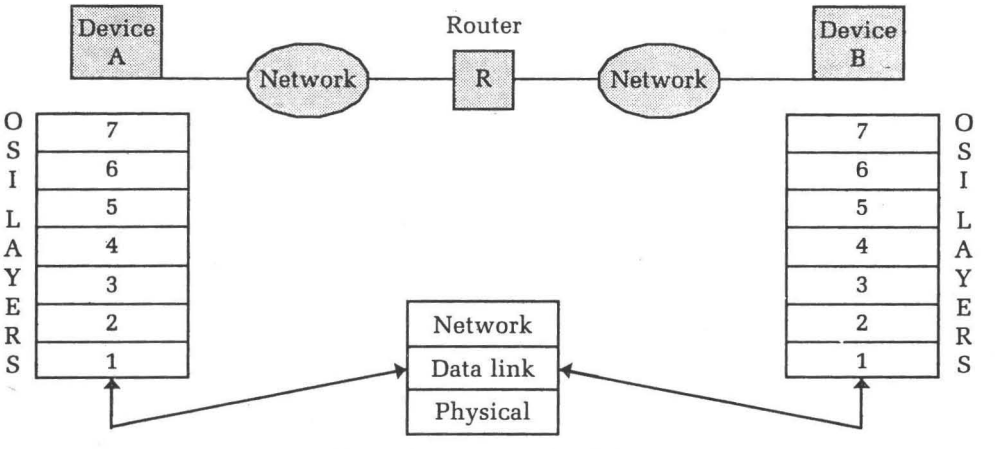


Fig. 20.10 A Router in the OSI Model

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Routers act like stations on a network. Routers have addresses on, and links to, two or more networks at the same time (unlike most stations which are members of only one network).
- Receive packets from one connected network, pass them to a second connected network.
- If a received packet is addressed to a node on a network of which the router is not a member, still it is capable of determining which of its connected networks is the best next relay point for the packet.
- Once a router identifies the best route for a packet to travel, it passes the packet along the appropriate network to another router.
- Router checks the destination address; finds what it considers the best route for the packet; passes it to the destination network or across a neighbouring network to the next router on the chosen path.

Routing concepts

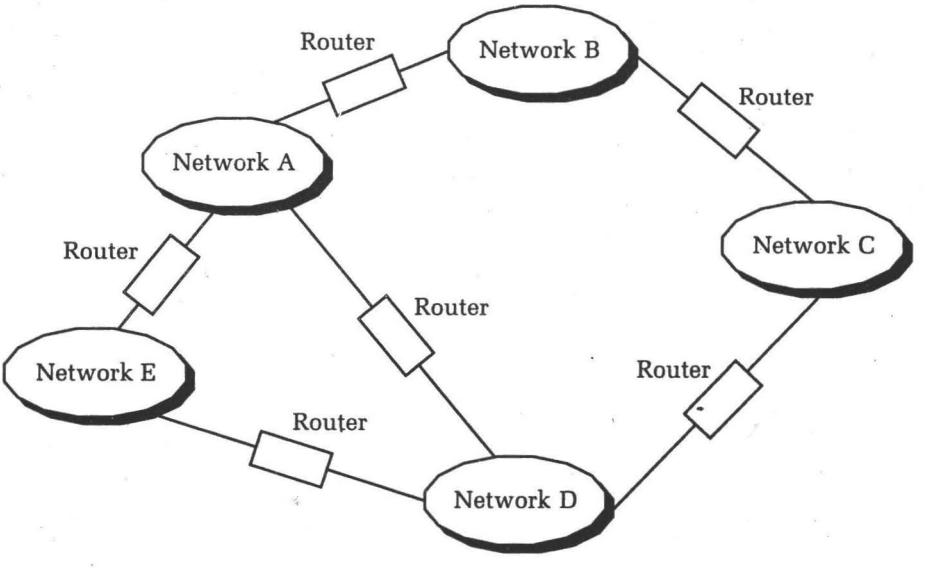


Fig. 20.11 Routers in an internet

- Job of router is to forward packets through an internet work of compatible networks.
- Packet is to moved from network A to network C via router (network) B. More than one pathway exists. Packet could reach network by going through router D instead of Router B or even directly from A to C.
- With multiple options, the router choose, the best pathway.
- Decision is based on efficiency which of the available pathways is the cheapest (shortest); value is assigned to each link.

  The length of a particular route = Total of the value of the component links; shortest means (depending on the protocol) the route requiring the smallest number of relays/hops. (E.g. A to D is considered shorter than the route

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

A–B–C–D even if the actual distance covered by the latter is same or less). In other cases, shortest means (i) fastest (ii) cheapest (iii) most reliable (iv) most secure (v) best of any other equality that makes one particular link (or combination of links) more attractive than other. Shortest means a combination of the above.

- Shortest means smallest number of relays needed; also called *hop-count routing* (every link is considered to be of equal length given the value 1). Equal link values make hop count routing simple.
  (i) one hop route = 1
  (ii) two-hop routes = 2 & so on.
- Routers need updating only when a link becomes unavailable. Value of the link here becomes infinite and alternatives found. Hopcount algorithms usually limit the routes known by a single router to those within fifteen hops. Novell, Apple talk, OSI, TCP/IP protocols all use hop count as the basis for their routing algorithms.
- Some other protocols factor a number of qualities relevant to the functioning of a link before giving a value to the link based on :
  – Speed
  – Traffic congestion
  – Link medium etc.

  When all relevant factors for a particular link are combined, a number representing the value or length of the link is issued, which represents an assessment of efficiency, not a physical distance, known as symbolic length of the link.
- In some protocols, each link in a network is assigned a length based on the qualities considered important for that network. Eg. Half-duplex or full-duplex, direction of a particular length of the link is differing from other, traffic load, quality of the cable (though the physical distance the signal has to travel is not changed) difference etc. As with hop-count routing, the decision of which route is best depends on shortest distance (totalling the lengths of every link used by a given path). Routing all three hop paths = 3 lengths are longer than two hop paths. Different links if assigned different lengths three hop link may be even shorter than two hop-link.

Distributed routing

In certain routing protocols, if a pathway to the destination is decided, the router sends all packets in that route to reach the destination. In other routing protocols, a technique is employed known as *distributed routing* wherein a router may select a new route for each packet (even packets belonging to the same transmission) in response to the changes in the relative lengths of the links.

Router for the packets from Network A to Network D

(i) Via network B

(ii) Via network C

(iii) Via network Q etc, *which route is the most efficient is to be decided.*

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

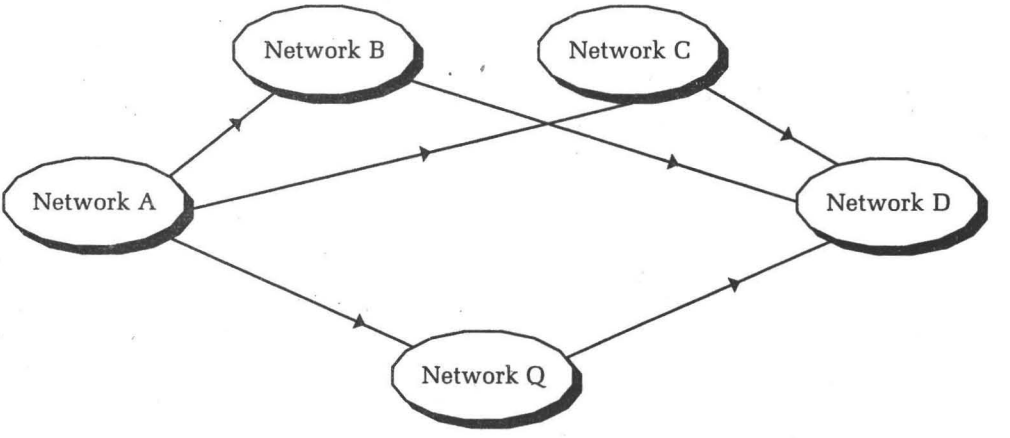
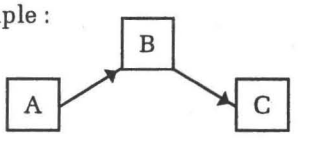


Fig. 20.12 Route for the packets from network A to network D

Packet life time	Loops and bouncing
• Router decides the pathway • Packets are passed on to the next router on that path; router forgets about it. • Next router may choose the same path way or different pathway if shorter. • Relay the packet to the next router in that direction. • Handing-off responsibility like this allows each router to contain minimal logic. Keeps the amount of information that must be contained in the frame to a minimum. • Allows for route adjustment based on upto the minute appraisals of each link. • Creates the potential for a packet getting stuck in a never ending loop or bounce in which a packet is passed a round from router to router without ever actually reaching its destination.	• Occurs when a router updates its routing table; relays packet based on new pathways before the receiving router has updated its own vector. Example :  • A believes short route to C is via B. • Relays a packet to B • Before B receives the packet, comes to know that its link to C is disabled. • B updates its sector and finds that current shortest route is via A. • A has not received the information about B-C link, still believes best route to C is through B. • Packet is relayed back to B; B relays it back to A. Problems of this sort are more likely on systems using distance vector algorithms than on those using link state algorithms.

Problems created by looping and bouncing is not primarily one of lost packets. (The data link functions of the transmissions originator and receiver report lost frames and replace with new copies).

Problem is processing eternally. *Looping packets* uses network resources and increases congestion. *Looping packets* are to be identified and destroyed to make the links free for legitimate traffic.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

The solution is an added packet field called *packet life time*. Each packet is marked with a lifetime, usually the number of hops that are allowed before a packet is considered lost and accordingly destroyed.

Each router to encounter the packet subtracts 1 from the total before passing it on. When the life time total reaches 0, the packet is destroyed.

Gateways

These are more complex than bridges or routers because these are the interface between two or more dissimilar networks. It connects two or more LANs which uses same or different (usually different) data link and network protocols. It operates in all seven layers of the OSI model. A *gateway* is a protocol converter.

A router by itself :

- transfers
- accepts
- relays packets only across networks using similar protocols

A gateway :

- accepts a packet formatted for one protocol (Apple talk)
- convert it to a packet formatted for another protocol (TCP/IP) before forwarding it.
- a software installed within a router
- understands the protocols used by each network linked into the router and is therefore able to translate from one to another (only modifications required are the header (trailer of the packet).
- The gateway must adjust the data rate, size an format in other cases.

Gateways (i) translate one network protocol into another (ii) translate data formats and (iii) open sessions between application programs, thus overcoming both hardware and software incompatibilities.

In micro to mainframe communications, for example, the gateways convert the microcomputer LAN transmissions into a transmission that looks like it came from a smart terminal.

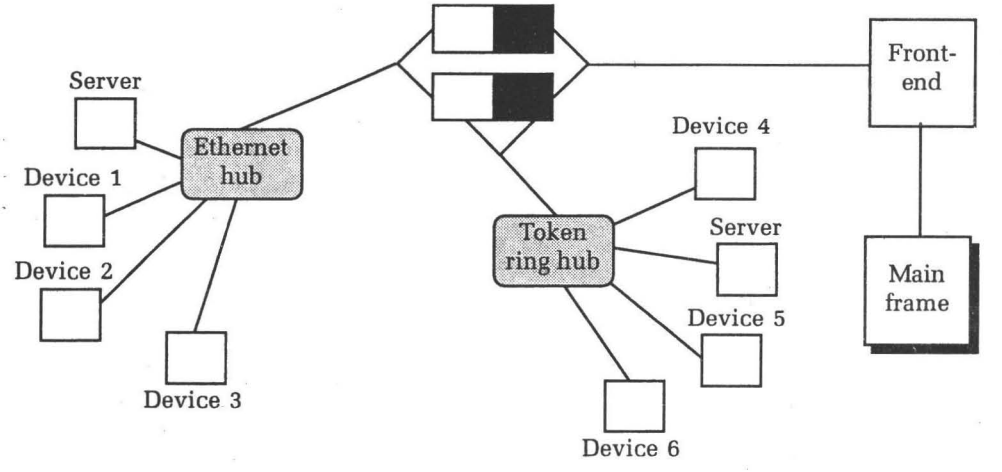


Fig. 20.13 Use of gateways (connecting LANs and Mainframe)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

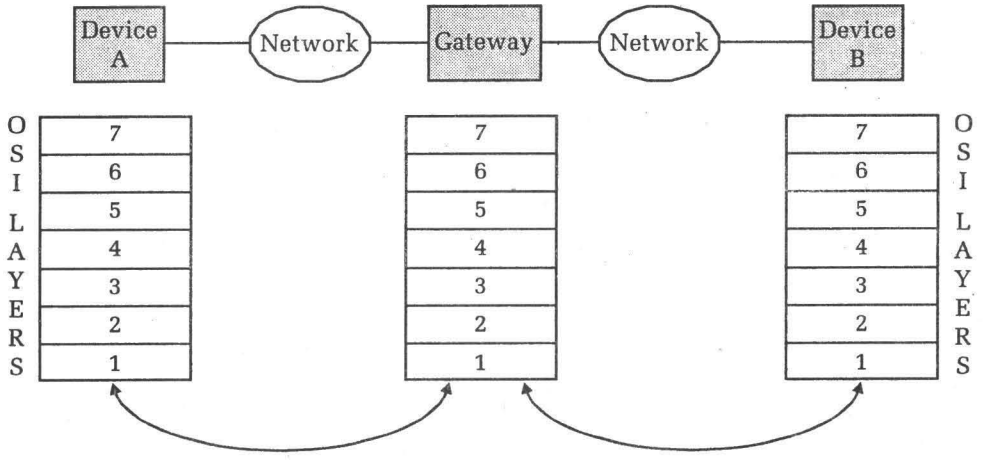


Fig. 20.14 A gateway in the OSI model

Routing algorithms

- Routing the pathway with the lowest cost is the best solution.
- Optimal combination for any transmission is foundout knowing the cost of each link. Several algorithms are used for making the calculations.
- The most popular ones are :
  - Distance vector routing
  - Link state routing

Distance vector routing

- Each router periodically shares its knowledge about the entire network with its neighbours.

  Algorithms work as follows :
- Knowledge about the whole network : Every router shares its knowledge about the network to the neighbours. It sends all of its collected knowledge about the network to the neighbours. A router's knowledge of the network may be sparse (How much it knows, is important? It sends whatever it has)
- Routing only to neighbours : Every router sends its knowledge periodically about the network to the other routers with whom they have links. Through its ports, it sends whatever information (knowledge) it has about the whole network which is received and kept by its each neighbouring router and used to update that router's own information about the network.

Information sharing at regular intervals

Once in 30 seconds, each router sends its information about the whole network to its neighbours. Sharing of information occurs whether or the network has changed since the last time information has been exchanged.

Sharing of information

Figure 20.15 shows how distance vector routing works.

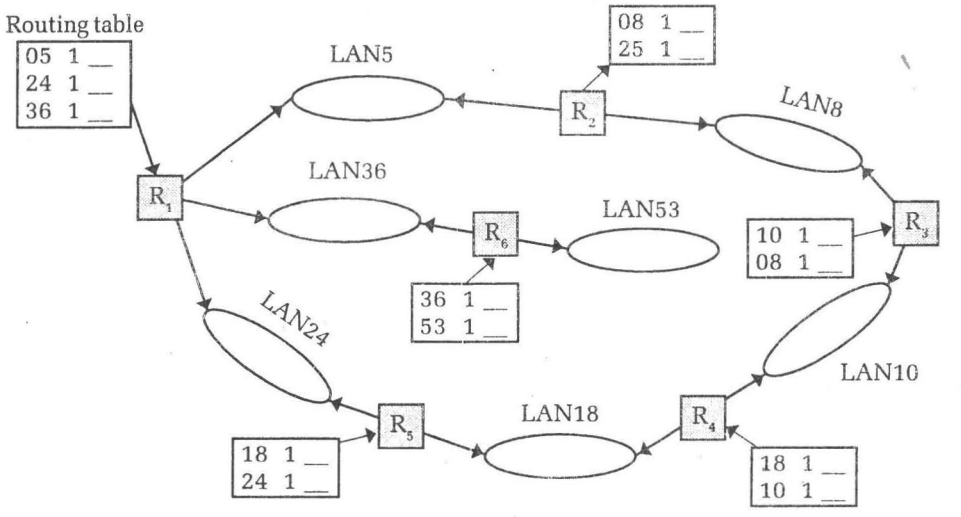
Distance vector routing indicates the routing process measured by a cost of 1 unit for every link. The efficiency of transmission is a function of the number of

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

links required to reach a destination. Hence distance vector routing is based not on cost but on hop count.

η transmission = f (number of links)



Note : R_1 to R_5 are routers or gateways

LANs may be Ethernet type, Token ring type, FDII Type

(LAN number are indicated)

Fig. 20.15 An internet

In the figure 20.15, information about the internet work is sent by each router to its immediate neighbours eg. R_1 sends periodically its knowledge about the whole internetwork to immediate routers R_2, R_5 and R_6. Similarly R_2 sends information to R_1 and R_3. In this way R_1 also gets back its own information and also information from other immediate neighbours after adding further knowledge to their own knowledge. Each of these neighbours adds its knowledge and sends the updated table to its neighbours. Finally, every router have updated knowledge about other routers in the network. This is the concept.

Routing table

The question is how each router gets its initial knowledge about the whole network (internet work) and how shared information is used to update the knowledge?

Table creation

At the start, a routers knowledge of the internet work is sparse. What it knows is that it has been connected to some LAN numbers (two or more). A router knows the ID of each station. A station port ID and a network ID share the same prefix. A router can find out to which network it is connected studying its own logical addresses (it has many logical addresses and ports). With this information, it can construct its own original routing table.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Routing table has three information as under :

Network_ID	Cost	Next router

Network ID – Final destination of the packet

Cost – Number of hops a packet must make to get there.

Next Router – Router to which a packet must be delivered on its way to a particular destination.

A sample table has been put at six of the routers in figure 20.15. Routing table distribution in distance vector routing is shown in figure 20.15. No multiple hop destinations and no next routers have been identified. The basic tables as shown in the figure are sent to neighbours (as shown by arrows) eg. R_1 sends its routing table to routers R_2, R_5, R_6; R_2 send its routing table to routers R_1 and R_3.

Updating the table : When R_1 receives a routing table from R_2 it uses the information to update its own table.

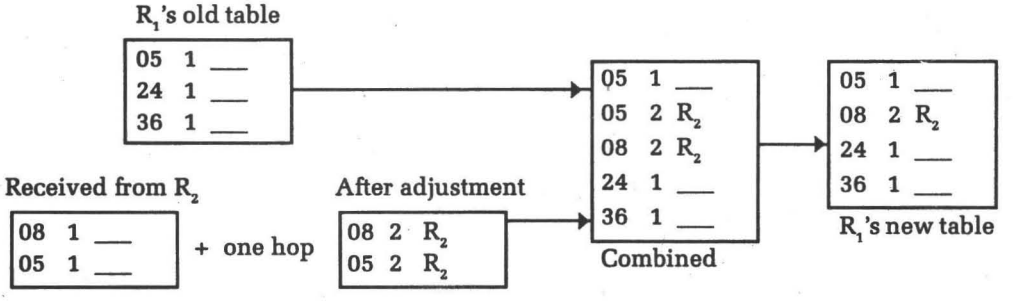


Fig. 20.16 Updating the table

In the above case, R_1's old table and the one received from 2 (after the hop) both are combined. The combined table may contain duplicate data for some network destinations. In the above case we find 05 1 – and 05 2 R_2 have emerged as duplicate data for network 5 (Received from R_1's old table and from R_2). If we consider the cost 05 2 R_2 is costlier than 05 1 – as there is a hop. Hence the duplications are avoided. Costly duplications are first removed. Here we are eliminating 05 2 R_2. Hence, the R_1's new table is as shown above in figure 20.16.

Similarly let us examine router R_3 which receives a copy of R_4's routing table.

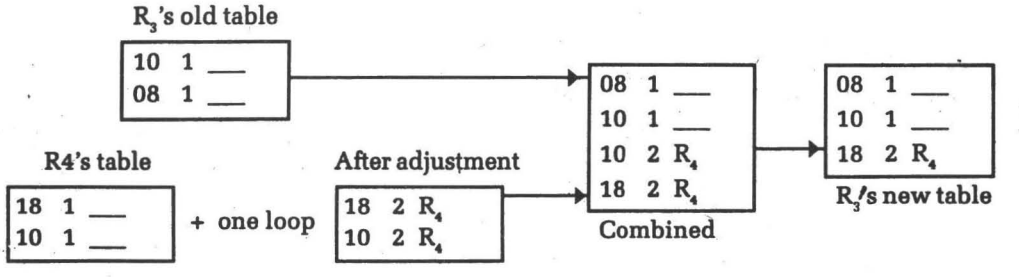


Fig. 20.17 Updating the table

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

In this case also if we work out R_3's new table similar to R_1's new table, the duplication of 10 2 R_4 in the combined table can be eliminated as it is costly. It is also possible to consider R_5 and to deliver a packet to network 10 requires two hops the next of which is to router R_3. This would work out costly. Here the responsibility ceases if R_5 relays the packet to R_4. R_4 receives the packet, looks at its own table and finds that it is connected directly to LAN 10 (one hop, to next router). Network 10 delivers the packet to its final destination.

The updated routing table are shown in figure 20.18. at points R_1 and R_3. Rest of the routers, the table remains same.

If we consider R_6 in a similar way for a new table.

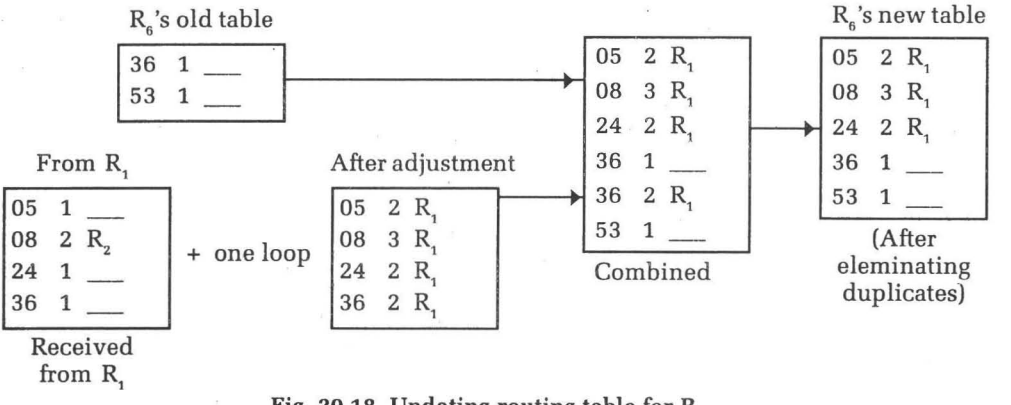


Fig. 20.18 Updating routing table for R_6

New updated routing tables :

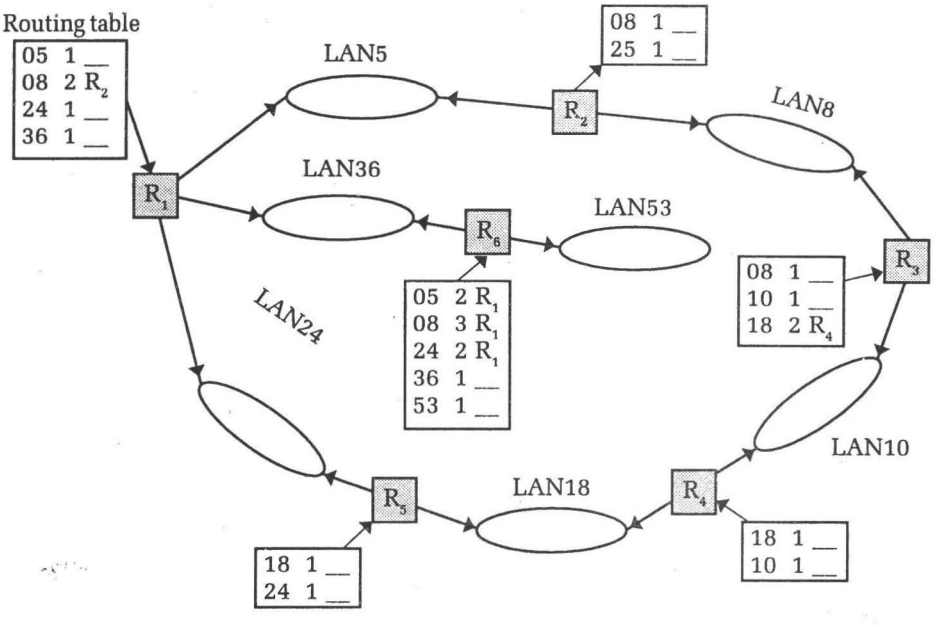


Fig. 20.19 Updated routing tables for R_1, R_3 & R_6

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Final routing tables :

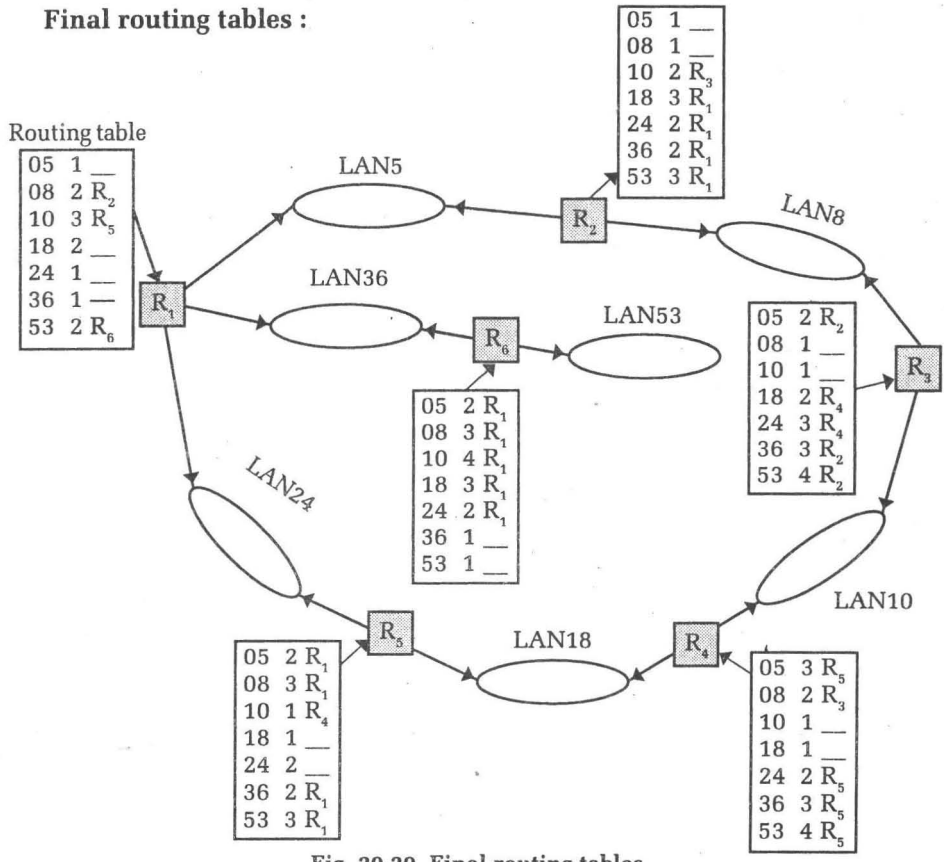


Fig. 20.20 Final routing tables

Link state routing

Here each router shares its knowledge of the neighbourhood with every other router in the network unlike distance vector routing.

The router sends information only about its neighbourhood (not by sending the entire routing table). A process called flooding is used wherein a router sends its information to all of its neighbours through its output ports. Each router sends information to every other router on the internetwork (not just to its neighbours). Each router sends the packet to all of its neighbours. Same information received by all periodically. The interval in this case is longer (Eg. 30 minutes Vs 30 seconds as compared to distance vector routing).

Information sharing

Details	Distance vector routing	Link state routing
1. Router sending its knowledge to other routers.	Router sends its knowledge to neighbours. Neighbours add this knowledge to their own knowledge; send the whole table to their own neighbours.	Each router sends its knowledge about its neighbourhood to every other router in the internet work.
2. Cost algorithms	Lowest	Lowest

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

	Cost refers to hopcount	Cost is weighted values based on security level, traffic, state of the link (Cost is different from R_1 to network 5 is different from R_1 to network 24). Cost does'nt depend on transmission fees paid by the sender/receiver. Cost is an outbound cost.
3. Information sharing	Takes less period	Longer period.

Packet cost: Cost is based on outbound cost. (When a packet leaves the router)

- Cost is applied only by routers and not by any other stations in a network. Link from one router to the next is a network, not a point to point cable. Every station on the network examines the header of every packet that passes. If cost of this is added for each station, instead of routers alone, the cost would go high (unpredictably); the number of stations in a network would change for variety of reasons, many of them unpredictable.
- Cost is calculated as a packet leaves the router, not at the entry. Most of the networks are broadcast networks. When a packet is in the network, each station including the router can pick it up. Since the packet goes from a network to a router, cost cannot be assigned to a packet. Figure 20.21 below shows our sample internet as it appears to the link state routing algorithm. The costs reflect attributes of each network; the cost shown here is arbitrary.

When a router floods the network with its neighbourhood with information, it is said to be *advertising*. The basis of which is short packet called a *link state packet (LSP)* which contain fields like ID of the advertiser, ID of the destination work affected, cost and ID of the neighbour router.

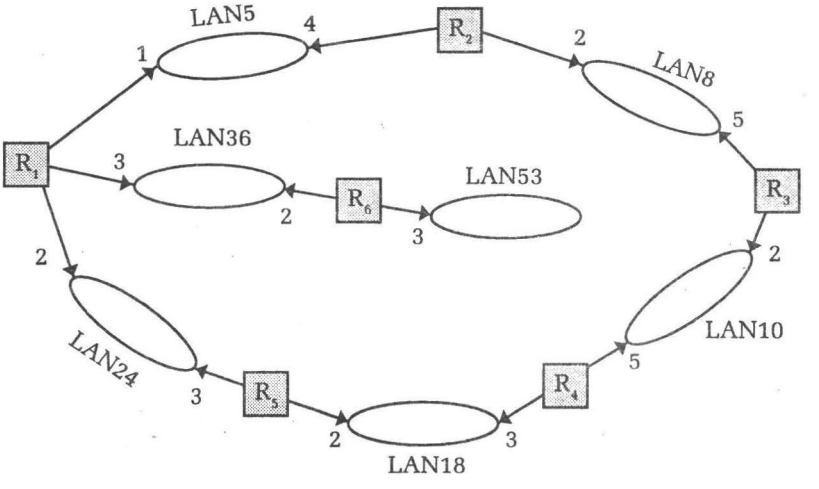


Fig. 20.21 Cost in link state routing

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Getting information about neighbours

A short greeting packet is sent by the router periodically to get its information about its neighbours. If neighbour responds to the greeting, it is considered as alive and functioning. If not, a change is assumed to have occurred and the sending router alerts the rest of the network in its next LSP. The greeting packets are small. They do not occupy network resources to a significant degree.

The flooding of R_1's LSP

This is shown as per the figure 20.22 below.

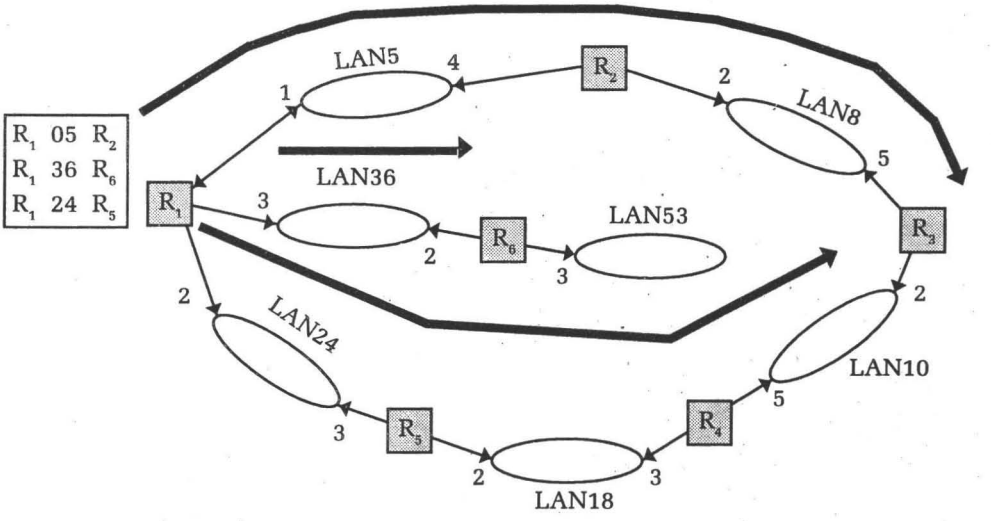


Fig. 20.22 R_1's LSP

Flooding of R_2's LSP

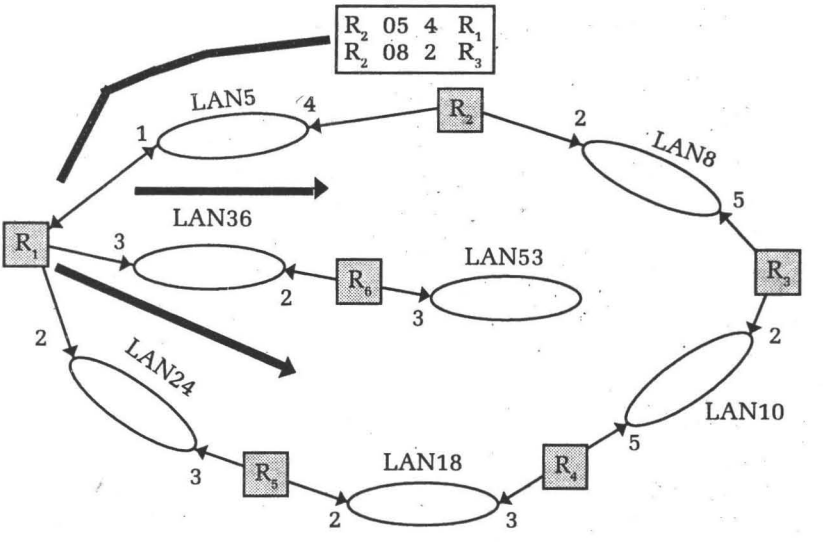


Fig. 20.23 R_2's LSP

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Dijkstra algorithm

This algorithm is used by each router to calculate it routing table. This calculates the shortest path between two points on a network using a graph made up of nodes and arcs. Nodes are of two types :

- Networks
- Routers

Arcs are connections between a router and a network (router-to-network and vice versa). Cost is applied only to the arc from router to network where as from network to router it is zero. See the figure below :

Advertiser	Network	Cost	Neighbour
R_1	5	1	R_2
R_1	36	3	R_6
R_1	24	2	R_5
R_2	5	4	R_1
R_2	8	2	R_3
R_3	8	5	R_2
R_3	10	2	R_4
R_4	10	5	R_3
R_4	18	3	R_5
R_5	24	3	R_1
R_5	18	2	R_4
R_6	36	2	R_1
R_6	53	3	–

Fig. 20.24 Link state database

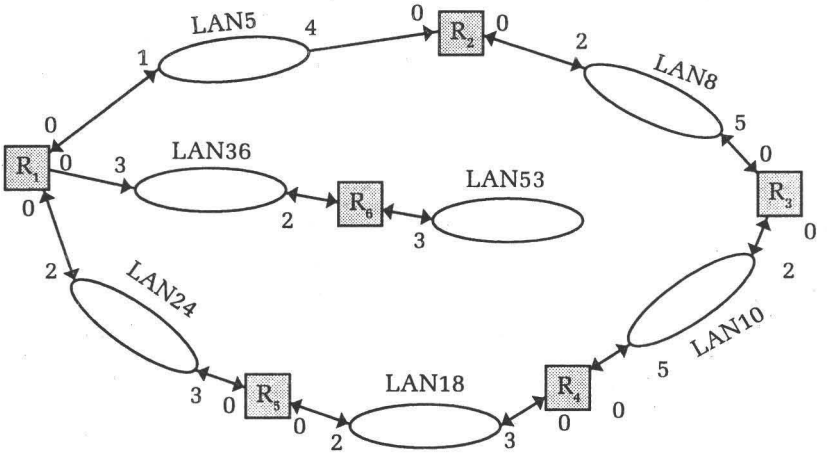


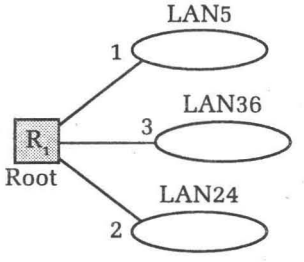
Fig. 20.25 Costs in the Dijkstra algorithm

The Algorithm follows 4 steps to discover shortest path tree (routing table) for each router.

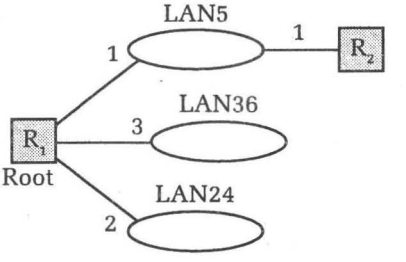
Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

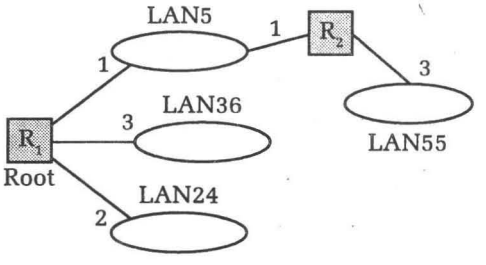
- The algorithm begins to build the tree by identifying its root. The root of each router's tree is itself. Algorithm connect, all nodes that can be reached from this root (all other neighbour nodes) Nodes and arcs are temporary.
- The algorithm examines the database; it identifies every node which can be reached from the selected node. These nodes and their arcs are added temporarily to the tree.
- Last two steps are repeated till every node in the network is attached permanently to the tree. The only permanent arcs are those that represent the shortest (lowest cost) route to every node.



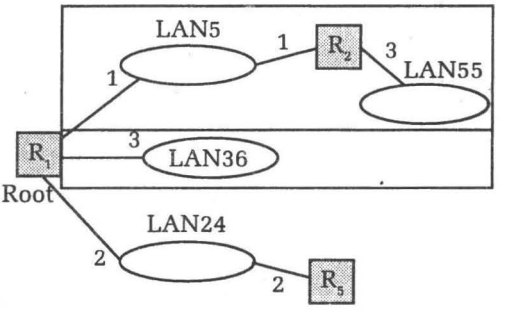
(i) Networks 5, 36, 24 added



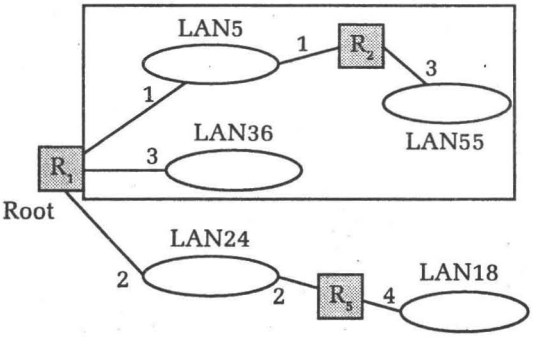
(ii) R_2 added; 5 permanent



(iii) R_2 permanent, 55 added



(iv) 24 permanent, R_5 added

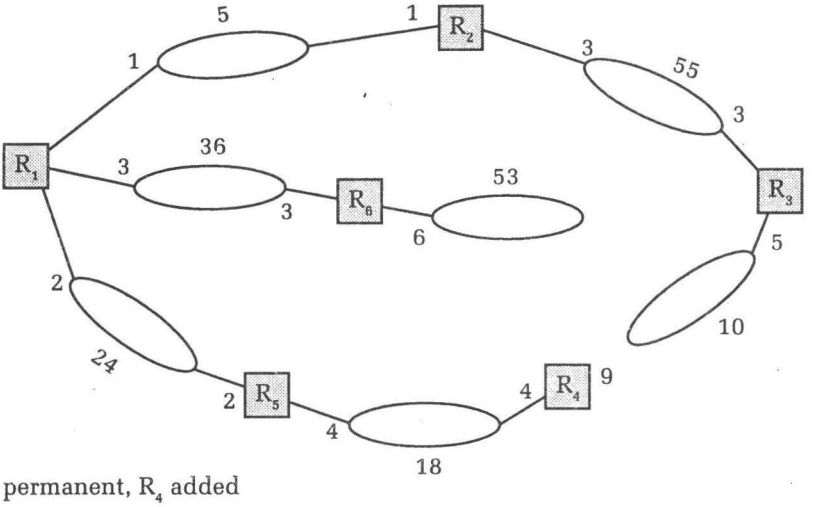


(v) R_5 permanent, 18 added

Like this continue (vi), (vii), (viii) not shown

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.



(ix) 18 permanent, R_4 added

(x) R_4 permanent, 10 added But 9>5 so that link deleted

(xi) 10 permanent

(xii) 55 permanent

In link state routing, it may be noted that the link state database is the same for all routers. The shortest path trees and the routing tables are different for each router.

POINTS TO REMEMBER

- Internet or internet working is an inter connection of individual networks. I means a worldwide network; (small *i*) *i* is used to mean interconnection of networks.
- There are four categories in networking and internetworking devices : (i) repeaters (ii) bridges (iii) routers and (iv) gateways. Repeater or regenerator is an electronic device used on the networking devices and is active only at the physical layer of the OSI model. The purpose is to regenerate the signal.
- Bridges are used to connect the two LAN segments. Bridges are more sophisticated than hubs because they only forward those messages that need to go to the other network segments. They divide a large network into smaller segments. They operate in the physical and data link layers of the OSI model. It filters traffic, makes them useful for controlling congestion, isolating problem links, provides security through partitioning of traffic. Three types of bridges are (i) simple bridges (ii) learning bridges (iii) multiport bridges.
- Routers connect two or more LANs that use the same or different data link protocols but the same network protocol. Routers and bridges are simple hardware devices capable of executive specific tasks. These operate in the physical, datalink and network layers of the OSI model. They decide the path a packet should take.
- Gateways operate in all the seven layers of the OSI model. They are more complex than bridges or routers because these are the interface between two

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

or more dissimilar networks. It connects two or more LANs which uses same or different (usually different) data link and network protocols. A gateway is a protocol converter.

- Brouters are devices which combine the functions of both bridge and routers operating at both the data link and network layers.
- Two methods of calculating the shortest path between two routers are (i) Distance vector routing and (ii) Link state routing.
- In distance vector routing, each router periodically shares its own knowledge about the network with its immediate neighbour routers. Here each router provides a table with information about networks (ID, Cost and the router to access the particular network)
- In link state routing each router creates LSP. Every other router receives the LSP through the flooding process. From the same common data base (All routers have same information). Each router finds its own shortest paths to the other routers using the Dijkstra algorithm. A cost is assigned to a packet soon after it leaves the router in link state routing and every router has its own unique routing table.

QUESTIONS

1. What is a networking device ? Compare networking with an internetworking device?
2. Explain the functions of the four connecting devices in which OSI layers they operate?
3. Compare an contrast a repeater and an amplifier.
4. What are the different types of bridges? Compare and contrast different types of bridges.
5. What is a brouter ? What are its functions?
6. Compare and contrast the four connecting devices.
7. Explain the routing concept.
8. What do you mean by distributed routing?
9. Explain packet life time, loops and bouncing.
10. Explain two most popular routing algorithms?
11. What is LSP database? How is it created?
12. What are the factors to be considered in connecting network?

FILL IN THE BLANKS

1. _____ are most active at the data link layer.
2. _____ utilise addressing protocols.
3. _____ act only upon the electrical components of a signal.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

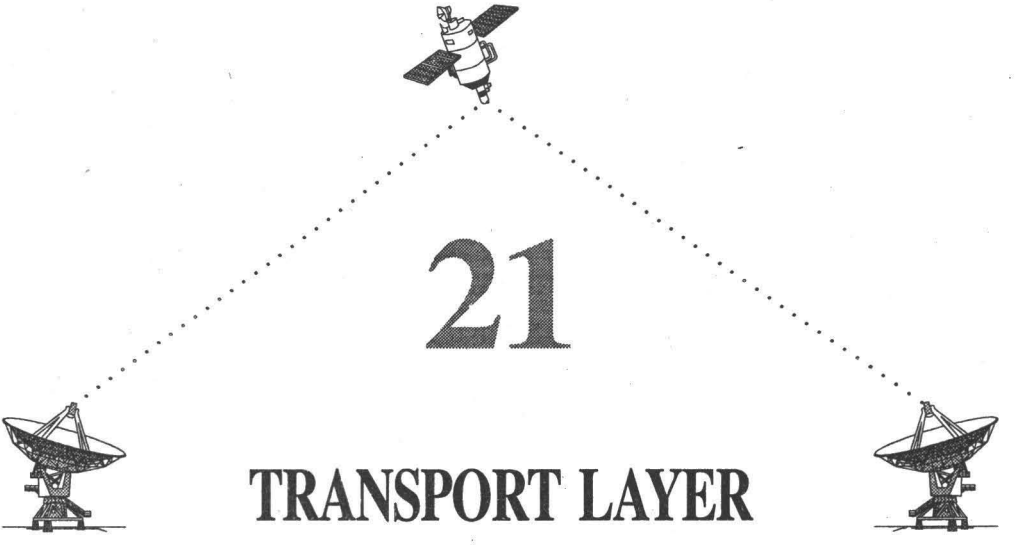
4. _____ are active only at the physical layer.
5. _____ is used for the purposes of a regeneration of signal.
6. _____ uses the first 3 layers of the OSI model.
7. Function of bridges + Function of router → Function of a _____.
8. Out of the four connecting devices _____ is not considered an internet working device.
9. _____ _____ routing algorithm requires more traffic between routers for updating.
10. In an LSP, we find the advertiser as a _____.
11. Routers have a common data base in _____ _____ routing.
12. A repeater takes the corrupted/weakened signal and _____ the same.
13. _____ bridge must have its address table manually entered.
14. _____ function in all layers of OSI model.
15. In _____ routing, each router receives vectors from its neighbours.
16. A packet travelling from one token ring network to another uses the service of a _____.
17. The bridge types are simple, learning and _____.
18. The _____ path in routing can refer to paths of least expensive/distant/ number of hops (any or a combination).
19. A _____ bridge filters / forward data packets, extend LANs .
20. _____ bridges are to connect networks with different datalink protocols.

Answers

1. Bridges
2. Bridges
3. Repeaters
4. Repeaters
5. Repeater
6. Router
7. Brouter
8. bridge
9. Distance vector
10. router
11. link vector
12. regenerates
13. Simple
14. Gateways
15. distance vector
16. router
17. multiport
18. shortest
19. simple
20. Encapsulating

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.



21

TRANSPORT LAYER

It is the fourth layer and is the core of the OSI Model. It is also known as host-to-host layer or end-to-end layer, because it :

(i) Establishes, maintains and terminates logical connections for the transfer of data between end users.

(ii) Responsible for generating the address of the end user.

(iii) Breaking a large data transmission into smaller packets (if required); ensuring that all the packets have been received; eliminating duplication packets.

(iv) Deals with end-to-end issues (viz procedures for entering and departing from the network).

(v) Can multiplex several streams of messages into one physical circuit; use inverse multiplexing to create one fast circuit from several slower ones.

(vi) Performs flow control by controlling the movement of messages, layers 1 and 2 control the physical flow of packets or frames.

(vii) Act as a liaison between upper layer protocols (session, presentation and application) and the services provided by the lower layers (network, data link and physical). The upper layers use the services of this layer to interact with the network without interacting directly with lower layers (or need not be even aware of it).

Examples of transport layer protocols are :

- Transmission control protocol (TCP)
- User diagram protocol (UDP)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Suppose an internet is made up of a variety of different physical networks such as LANs, MANs and WANs. A transmission moves from network to network. The data may be encapsulated in different types and lengths of packets. One network's network (data link functions) may break into smaller segments to fit a restricted packet or frame size; another network's peer functions may link several segments to a large segment.

If an ethernet in the internet is replaced by a token ring, the upper layers remain unaware of it. For the upper layers, the internet is a single and unchanging network. The transport layer provides this transparency.

21.1 DUTIES OF THE TRANSPORT LAYER

Transport protocol (peer to peer) implements transport layer services between two transport entities as shown in figure 20.1.

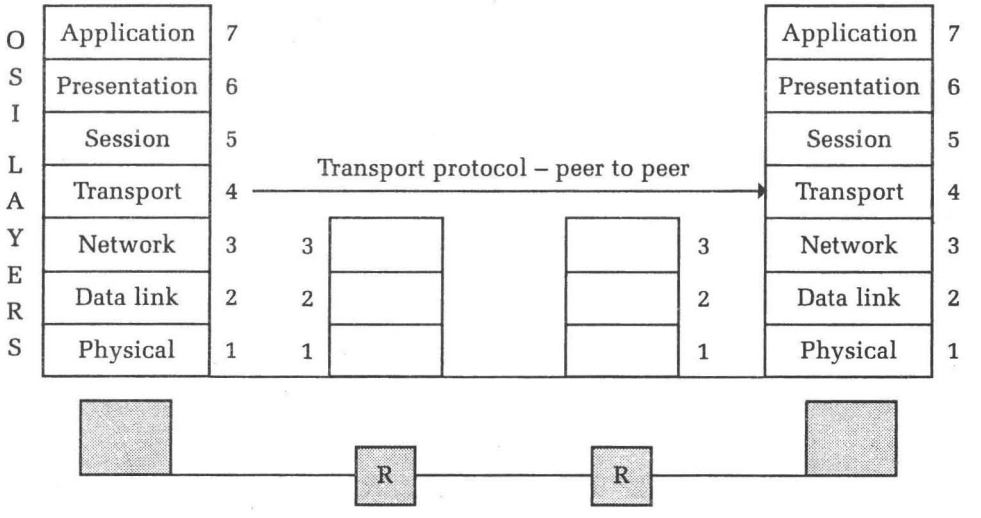


Fig. 21.1 Transport layer services

- The services provided are similar to the data link layer.
- Data link layer is designed to provide its services within a single network.
- Transport layer provides services across an internetwork (made of many networks)
- Data link layer controls the physical layer.
- Transport layer controls all three lower layers (1, 2, 3)

Services provided by transport layer protocols, are divided into :

(i) End to end delivery – Networking layer oversees the end to end delivery of end packets; does not see any relationship between those packets.

(ii) Addressing

(iii) Reliable delivery

(iv) Flow control

(v) Multiplexing

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

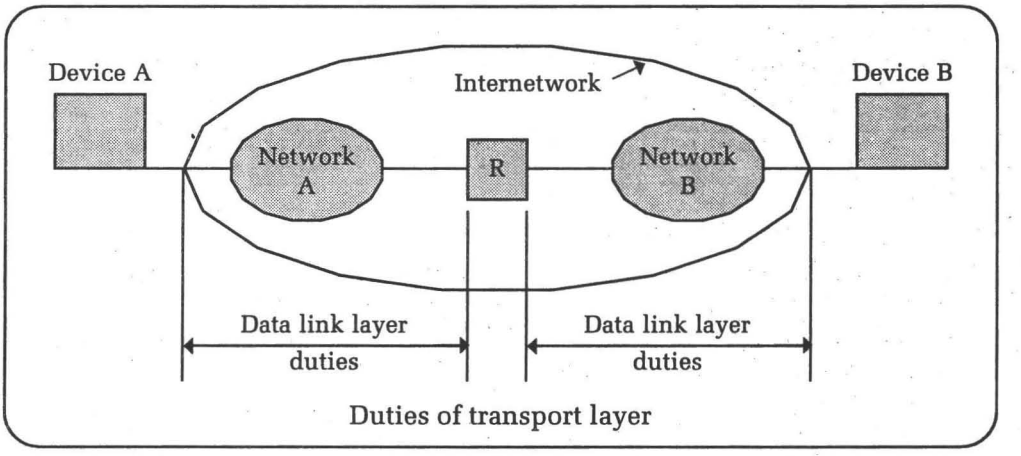


Fig. 21.2 Transport layer

(i) End to end delivery

- Network layer oversees :
  - (i) End to end delivery of individual packets; does not see any relationship between those packets (even those belonging to a single message)
  - (ii) Treats as an independent entity.
- Transport layer oversees :
  - (i) The entire message arrives intact (not just a single packet)
  - (ii) End to end (source-to-destination) delivery of an entire message.

(ii) Addressing

Protocol stacks (groups of protocols) interact at different levels. There are many protocols coming under this combines :

- Session Level
- Presentation Level
- Application Level

into a single package called an *application*.

Transport layer interacts with the functions of the session layer. Delivery to the session layer functions is effectively delivery to the application. Communication occurs not from end machine to end machine but occurs from end application to end application. Data generated by an application of one machine should be received by the correct application on the other machine. Communication is ended between many to many entities known as service ports. How the network identifies the service point on one host communicating with the service point on the other host. Addressing is very much required in this context for accurate delivery from one service point to another service point. Another level of addressing apart from the ones which are used in the data link and network levels is needed. Network level protocols need to know about this. At the transport layer, the protocol should be aware of which upper layer, protocols need communication.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

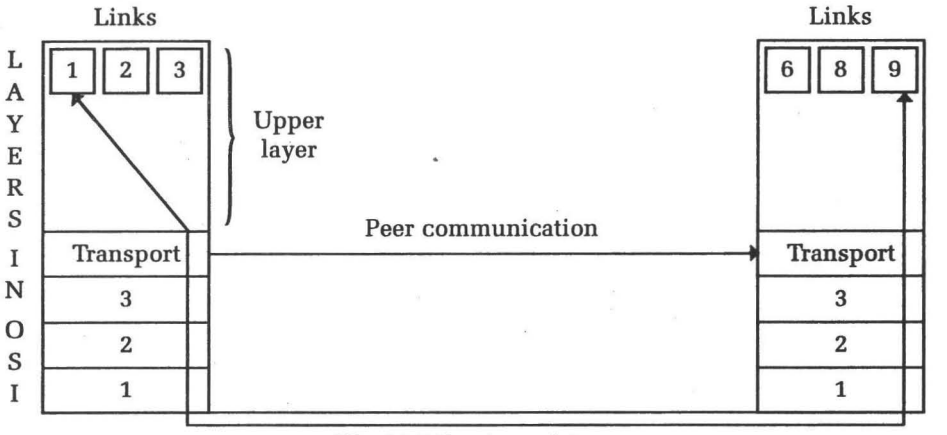


Fig. 21.3 Service points

(iii) Reliable delivery

Reliable delivery is to be checked for four controls at the transport layer.

- Error control
- Sequence control
- Loss control
- Duplication control.

(a) Error control

Data is to be delivered to the destination exactly as they originated from the source. Error control is the primary goal of reliability which is to be taken care off while transferring the data. As we are aware 100% error free delivery is not possible. But to the possible extent error free delivery, the transport layer protocols are designed.

Mechanism for this are based on :

- Error detection
- Retransmission with the error handling usually performed (using algorithms implementation in software e.g. checksum)

The question to be answered is: when error handling is there at the data link layer? why should this be there again at the transport layer?

In the data link layer function, it guarantees error free delivery node to node for each link. Node to node reliability will not ensure end-to-end reliability. See the figure 21.4.

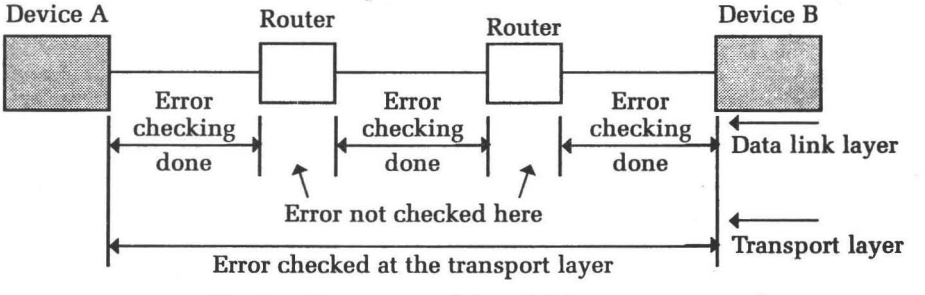


Fig. 21.4 Transport and data link layer error control

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

It may be noted from the above figure that though error checking is done at the data link layer errors are introduced as the packet is processed inside the routers and this has to be checked at the transport layer by its own checking to ensure that end-to-end (beginning to the end of the link) is intact and packet has arrived as intended by the source.

(b) Sequence Control

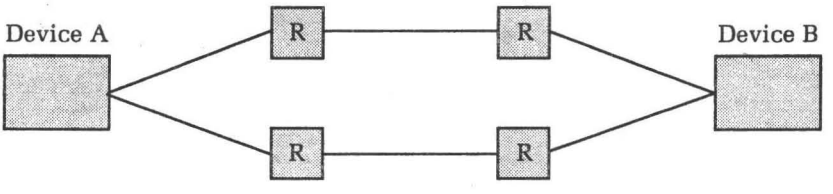
- Second aspect of reliability which is implemented at the transport layer.
- Transport layer is responsible for ensuring that data units received from upper layers are useable by the lower layers at the sending end.
- Similarly, at the receiving end, it is responsible for ensuring that various pieces of a transmission arrive in the order intended.

Segmentation and concatenation

If the data unit received from the upper layers is too long for the network layer diagram or data link layer frame to handle, the transport protocol reduces the size into small usable blocks. This is called *segmentation*. Alternatively, the size of the data unit, are small (belonging to a single session), then several can fit together into single datagram or frame, the transport protocol combines them into a single data unit. This is called *concatenation*.

Sequence numbers

Transport layer services add a sequence number at the end of each segment, if a longer data unit has been segmented. If the data unit is longer and has been segmented, the numbers indicate the order for reassembly. Alternatively, if several shorter units have been concatenated, the numbers indicate the end of each sub unit and allow then to be separated accurately at the destination. Further, each segment carries a field indicating whether it is the final segment or middle segment of the transmission.



- Father puts a cheque to his own account. } Packet 1
- Simultaneously he issues a cheque to the university for examination fees of his son from the same account (requesting the bank to hasten up immediately } Packet 2

- It is not important which order the transmission travel.
- Important is that they are to be reassembled at the destination.

This is something like you need not know how the various parts of the product reaching the assembly and assembled what you are interested is receiving of final product.

If the message is out of order, the effect is lost.

Fig. 21.5 Sequence control

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

(c) Loss control

This is the third aspect of reliability where in the transport layer ensures that all pieces of a transmission arrive at the destination, not just some of them. Some segments of the data may be lost in transmit, when data are segmented for delivery. For this, sequence numbers are provided which allow the receiver's transport layer protocol to identify any missing segments to enable them to request for redelivery.

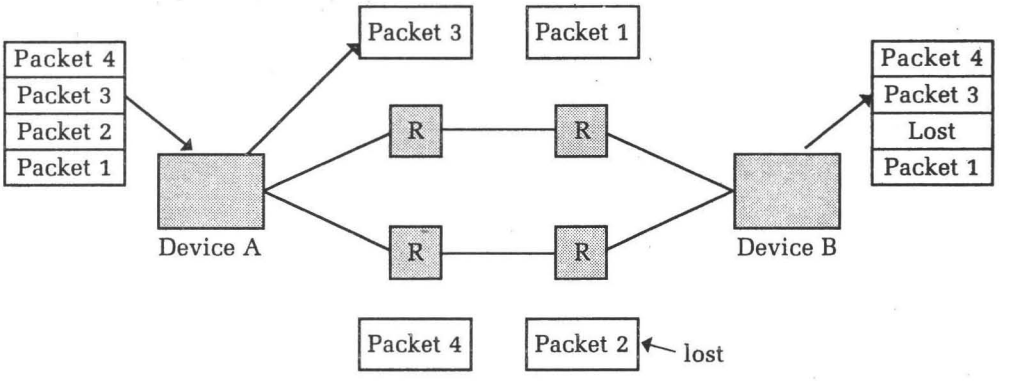


Fig. 21.6 Loss control

(d) Duplication control

This is the fourth aspect of reliability wherein the transport layer functions must guarantee that none of the pieces received at the destination are duplicated. Similar to identification of lost packets also, here also sequence numbers would help the receiver to identify and discard duplicate segments. Duplication is a severe problem, with major consequences. If the amount is paid twice from a bank to the customer, it would be a problem. Refer figure of sequence control. Father issues a cheque to the university for his son's examination fees. If the above is duplicated, the cheque will go twice to the university account.

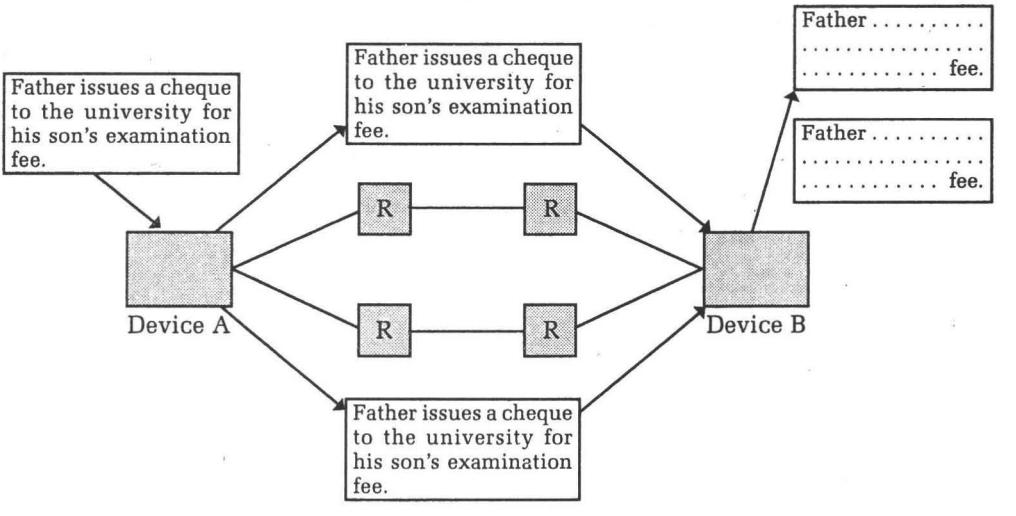


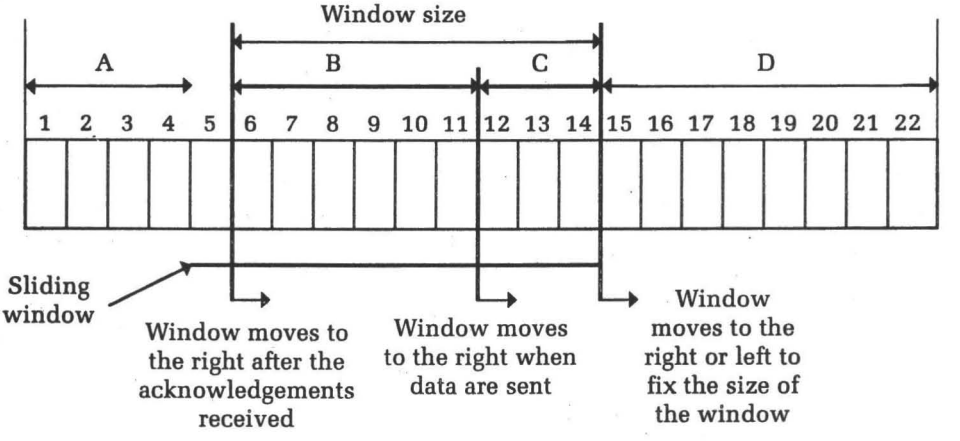
Fig. 21.7 Duplication control

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

(iv) Flow control

The transport layer is responsible for flow control in a similar way to the data link layer, which is performed end-to-end instead of across a single link. It uses a sliding window protocol. The window varies in size to accommodate buffer occupancy. The amount of data, the window can hold is negotiable. Window's *size control* is left to the receiver which specifies the size of the window to be increased or decreased in its acknowledgement packet. In majority of the cases, sliding windows are based on the number of bytes that the receiver can accommodate instead of the number of frames. A pair of communicating entities will use a buffer of *x* bytes that would accommodate *y* frames. The sender need not send a full window's worth of data; an acknowledgement expands the size of the window based on the sequence number of the acknowledged data segment; size of the window can be increased or decreased by the receiver; Receiver can send an acknowledgement any time it intends to do. To cope up with the variability in size, transport layer windows uses three pointers (acts like virtual walls) to identify the buffer.



A. Sent and acknowledged
B. Sent but not acknowledged
C. Can be sent
D. Cannot be sent

Fig. 21.8 Sliding window

(v) Multiplexing

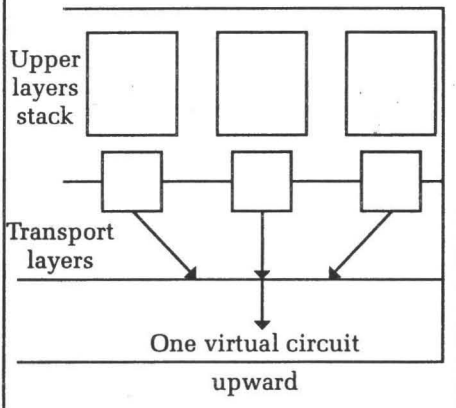
In order to better the transmission efficiency, the transport layer has the option of multiplexing in two ways :

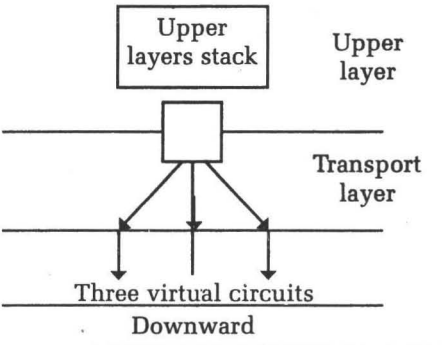
- Upward – many transport layers use the same network connection.
- Downward – one transport layer uses many network connections.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Upward	Downward
• Uses virtual circuits based on the services of the lower three layers. • The underlying networks charge for each virtual circuit connection. • Transport layer can send several transmission bound for the same destination along the same path by multiplexing, to make more cost effective of an established circuit	• Transport layer allows the splitting of a single transmission among a number of different paths to improve speed of delivery (throughput). This is useful when the underlying networks have low/slow capacity eg. some network layer protocols have restrictions on the size of packet sequence numbers which are handled. X.25 uses a three bit numbering code; sequence numbers are restricted to the range of 0 to 7 (only eight packets could be sent before acknowledgement needed). Throughput is low. Therefore, the transport layer can opt to use more than one virtual circuit at the network layer to improve throughput. The speed of delivery is made faster by sending several data segments.





21.2 CONNECTION

End-to-end delivery can be accomplished in the two modes :

- Connection-oriented
- Connectionless

Connection oriented mode

(i) Commonly used is connection oriented. Protocol establishes a virtual circuit or pathway through the internet between the sender and receiver. All the packets related to a message are then sent over this same path. Using a single path way for the entire message (a) facilitates the acknowledgement process (b) retransmission of damaged or lost frames.

(ii) Considered generally reliable.

(iii) This transmission has three stages :

(a) Connection establishment

(b) Data transfer

(c) Connection termination

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

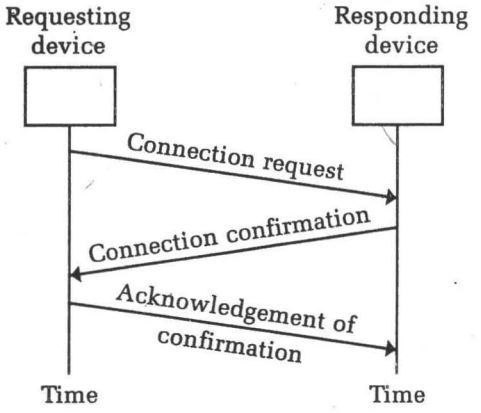


Fig. 21.9 Connection establishment

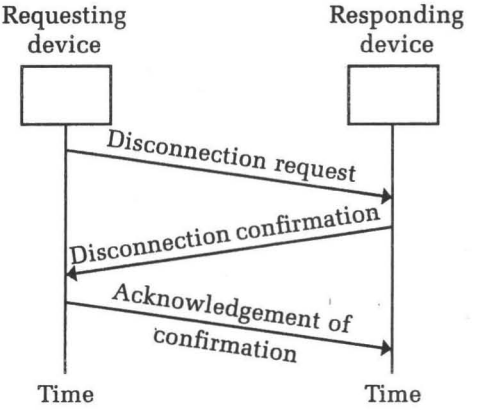


Fig. 21.10 Connection termination

Connection establishment (Fig. 21.9)

- Either communicating device can send data to another.
- Before data is sent, the requesting device would first determine the availability of the other to exchange data and a pathway must be found through the network, known as *connection establishment* which needs *three way handshake* as below :
  - Requesting computer sends a connection request packet to the intended receiver.
  - Responding computer returns a confirmation packet to the requesting computer.
  - The requesting computer returns a packet acknowledging the confirmation.

Connection termination (Fig. 21.10)

- This happens all the data have been transferred. It request a three way handshake as below :
  - Requesting computer sends a disconnection request packet.
  - Responding computer confirm the disconnection request.
  - Requesting computer acknowledges the confirmation.

21.3 OSI TRANSPORT PROTOCOL

The redundant services are avoided in the OSI by means of five transport classes. These classes are used depending on the services required by the upper layers.

(i) TP0 – Simple Class

(ii) TP1 – Basic error recovery class

(iii) TP2 – Multiplexing class

(iv) TP3 – Error recovery and multiplexing class

(v) TP4 – Error detection and recovery class.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Application

- The *transport layers* relates the requests to the available networking services.
  - TP0 and TP2 – used with perfect network layers
  - TP1 and TP3 – used with residual error network layers.
  - TP4 – used with unreliable network layers.

A *perfect network layer* is one in which the number of packets that are lost or damaged is almost zero.

A *residual error network layer* is one in which some percentage of errors are never corrected.

A *unreliable network layer* – TP4 provides fully reliable, full duplex, connection oriented services similar to TCP in the TCP/IP protocol suite.

Transport protocol data unit (TPDU)

Each TPDU consists of four fields :

Length	Fixed parameters	Variable parameters	Data

Fig. 2.11 TPDU

Length

1. It is first byte
2. Indicates the total number of bytes (excluding the length field).

Fixed parameters

1. Contains parameters or control fields (which are commonly present in all transport layer packets)
2. It consists of four parts :

(a) *Code* – Identifies the type of the data unit. ISO & ITU–T have recognised the following codes.

CR – Connection request	ED – Expected data
CC – Connection confirm	AK – Data acknowledge
DR – Disconnect request	EA – Expected data acknowledge
DC – Disconnect confirm	RJ – Reject
DT – Data	ER – Error

(b) *Source and destination reference* : These fields contain the addresses of the original sender and the ultimate destination of the packet.

(c) *Sequence number* : Transmission is divided into smaller packets for transporting purpose. Each segment is given a number for identification of its place on the sequence.

Sequence numbers are used for acknowledgement, flow control, reordering of packets at the destination.

(d) *Credit allocation*

- It enables a receiving station to inform the sender how many more data unit, may be sent before the sender has to wait for an acknowledgement. It allows the receiver to :

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

(i) Supersede existing sliding window or flow control restrictions.

(ii) To change the allocation at any time based on its processing needs.

- It separates flow control from acknowledgements (sender and receiver need not have the same sliding window size)

Variable parameters

This section of a TPDU contains infrequently occurring parameters (used mostly for management, like testing the reliability of a remoter etc.)

Data

This section of a TPDU contains regular/expedited data coming from the upper layers. Expedited data consists of a high priority message that must be handled out of sequence. An urgent request can supersede the incoming queue of the receiver and is processed ahead of packets that have been received earlier to it.

Connection oriented transport service (COTS) and connectionless transport service (CLTS)

OSI model supports the COTS and CLTS services, out of which COTS are commonly used.

COTS

- Creates a virtual circuit between two remote entities.
- COTS makes four different kinds of services available to the upper layers.

(i) *T-connect (T means transfer)* : This is first used service by the upper layer user of COTS to setup full duplex transport connection with a peer function on a remote device. During the establishment of the transport connection, the user can negotiate the quality of services desired and decide between normal and expedited data transfer modes.

(ii) *T-data* provides nonconfirmed service (but reliable). Successfully delivered packets are not acknowledged.

(iii) *T-expedited data* : After the connection is established, the two peers (T–Data or T– expedited data) services are taken for transfer of data. The amount of expedited data that can be carried is limited to 16 octets (bytes) by common agreement.

(iv) *T-disconnect* : User or transport service provider deploys this service to terminate a transport connection at any time during the data transfer. It is destructive. Any data still in transit when it is invoked may be lost. It can also be used by the transport service provider/called user, to reject a connection request.

CLTS

- Provides only one kind of service to the upper layer : T–UNIT–DATA.

  T–UNIT_DATA provides a single free standing data unit for all transmissions.

  Each unit contains :

  – all of the protocol control information necessary for delivery

  – no provisions for sequencing or flow control.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

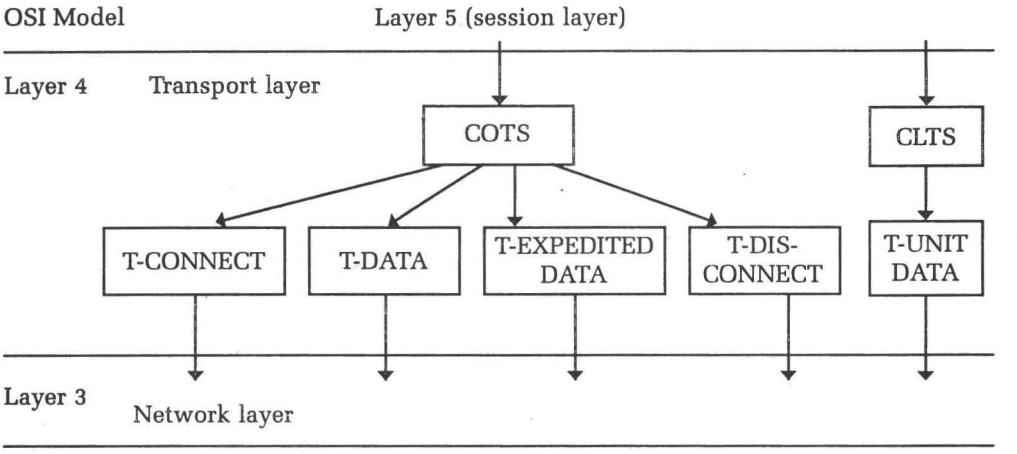


Fig. 2.12 Transport layer protocols in the OSI model

POINTS TO REMEMBER

- Transport layer is the fourth layer and is the core of the OSI model. Also known as hot-to-host layer and end-to-end layer. It makes data transmission transparent to the upper layers. It hides all of the manipulations in moving a message from source to destination. Certain common duties exist between transport layer and data link layer. The difference is data link layer functions in a single network, while the transport layer operates across an internet.
- Transport protocol peer to peer implements transport layer services between two transport entities. Services are divided into : (i) End to End delivery ii) Addressing (iii) Reliable delivery (iv) Flow control (v) Multiplexing Transport layer needs port / service point addresses.
- Reliable delivery requires (i) error control (ii) sequence control (iii) lost control and (iv) duplication control. Reliable delivery is to be checked for control at the transport layer.
- Flow control is handled by a three walled sliding window.
- Multiplexing can be a downward or upward in the transport layer.
- Loss control is the third aspect of reliability wherein the transport layer ensures that all pieces of a transmission arrive at the destination. Some segments of the data many be lost in transit, when data are segmented for delivery.
- Duplication control – fourth aspect wherein the functions must guarantee that none of the pieces received at the destination are duplicated.
- End-to-end delivery can be accomplished in two modes : Connection oriented transport services (COTS); connectionless transport services (CLTS).
- Connection establishment and connection termination are accomplished through three way handshakes.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- The transport layer is responsible for end to end delivery, segmentation, and concatenation.
- The transport protocol data unit (TPDU) format has four fields (i) Length (ii) Fixed parameters (iii) Variable parameters (iv) Data.
- The five types of transport classes are based on the reliability of the lower layers.

QUESTIONS

1. What are the functions of transport layer?
2. 'Some of the duties of data link layer and transport layer are common'. Is this a duplication? Give your comments.
3. How are the services provided by transport layer protocols are divided ?
4. Explain the terms : End to end delivery, Addressing, Reliable delivery, Flow control.
5. What are the controls to be checked in reliable delivery? Explain each of them.
6. What is segmentation and concatenation?
7. Explain loss control and duplication control.
8. Compare the sliding window walls of the sender in the data link layer with that of the ones in the transport layer.
9. What are the three phases a connection oriented transport service (COTS) goes through?
10. In the sliding window, the three parameters are used to identify the buffer. Which are they ? What are the four divisions made in the sliding window ?
11. Name the two options of multiplexing. Explain them.
12. Which are the two modes of end to end delivery? Compare and contrast connection establishment and connection termination.
13. What is TPDU? Explain its fields.
14. Which are the five transport classes in the OSI transport protocol? Explain them.
15. Compare COTS with CLTS. Which are the four different kinds of services mode available by COTS? Explain them.

FILL IN THE BLANKS

1. Transport layer is the _____ layer in the OSI model also known as _____ layer and _____ layer.
2. The transport layer performs the functions of similar type as the _____ _____ layer.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

3. In the case of end-to-end delivery, a message is moved from _____ to _____ of an entire package.
4. Reliable delivery is to be checked for four _____ at the transport layer.
5. _____ _____ _____ addresses are used by the transport layer.
6. Error checking in the case of data link layer is not done at the _____ whereas error control is needed at the transport layer because of potential errors due to _____.
7. If data segments arrives in the correct order, it is known as _____ _____.
8. If all the data packets are to reach the destination _____ control is needed.
9. If two exactly identical data packets reach the destination then _____ control has failed.
10. The window size in the beginning is 22. If 10 bytes are acknowledged and the window size moves upto 30, _____ bytes should the right wall move.
11. For a perfect network layer, transport classes used are _____ and _____.
12. For a residual network layer, transport classes used are _____ and _____.
13. For an unreliable network layer transport class _____ is used.
14. CONS means _____ _____ _____ _____.
15. CLTS means _____ _____ _____.
16. TPDU means _____ _____ _____ _____ .
17. _____ is a connectionless service in the transport layer.
18. In _____, packets of a single transmission travel from source to destination via different paths.
19. A virtual circuit is _____ _____ service.
20. Connections are established and terminated in _____ _____ service.

Answers

1. fourth ; host-to-host ; end-to-end
2. data link
3. source ; destination
4. controls
5. Application program port
6. routers ; routers
7. sequence control
8. loss
9. duplication
10. 18
11. TP0 ; TP2
12. TP1 ; TP3
13. TP4
14. connection oriented transport service
15. connectionless transport service
16. transport protocol data unit
17. CLTS
18. CLTS
19. connection oriented
20. connection oriented

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

22

UPPER OSI LAYER

The upper layers of OSI model have been mentioned many a times in this book. These are user layers :

- Session Layer (Layer 5)
- Presentation Layer (Layer 6)
- Application Layer (Layer 7)

TCP/IP, Novell protocols use the services of these layers and together all the three are implemented as application. This layer is often implemented with the operating system as system software.

22.1 SESSION LAYER (LAYER 5 OF THE OSI MODEL)

As already said earlier, the session layer is responsible for :

- Initiating (establishing)
- Maintaining and
- Terminating each logical session between end users (synchronisation)

Best example for this is telephone – When you lift the telephone, listen for a dial tone, dial a number, a physical connection is created through layer 1 as a person-to-network protocol. The other person at the other end of the telephone circuit is engaged with the first person in a person-to-person session; It is the dialogue between the two. This layer is responsible for managing and structuring all sessions. Session initiation involves :

- arranging all the desired and required service between session participants. (logging on to circuit equipment, transferring files, using various terminal types, performing security checks)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Session termination provides :

- an orderly way to end the session; a means to abort a session prematurely.
- some redundancy might have been built into recover from a broken transport connection in case of failure.
- also handles session accounting to the correct party to receive the bill.

No software is actually present at layer 5, since most of its functions in some of the networks, are actually done by layer 2 or layer 4. The session layer provides (1) a user interface to layer 4 (Transport layer) and is therefore the first layer with which a user interacts directly (to select the level of synchronisation or control needed for a transmission) (ii) handles upper layer problem like inadequacy disk space or lack of paper for the printer.

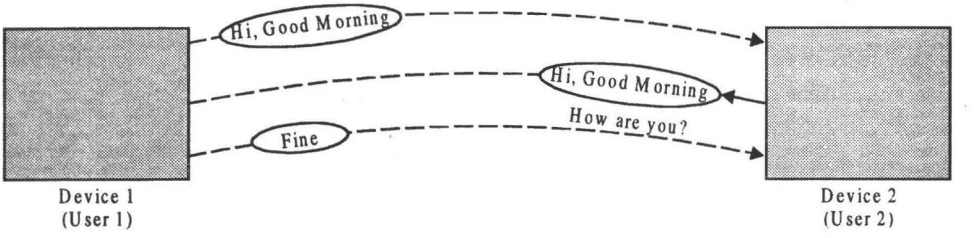


Fig. 22.1 Session layer dialogue

This layer uses the back and forth nature of the exchange e.g. to manage interactions between application programs. Within the system, user application programs must be able to communicate and exchange files or transactions with a host application programs. Normally, the questions would arise like :

- each application program is to transfer a file or transaction at any time?
- providing check points to allow the application programs to backup their work and recover from processing?
- process be full or half duplex? (Do we control the direction of flow in half duplex) etc.

Services of this layer are :

- Coordination of connection & disconnection of user dialogues between applications.
- Providing synchronisation points for data exchange.
- Coordination of who and when of dialogues.
- The data exchange should be complete before the session is over.

Session and transport interaction

Transport layer could make abrupt disconnection, whereas the session layer has an obligation to the user and would not disconnect until the session can be brought to a graceful conclusion.

The transport layer is allowed to do a portion of the job whereas a session layer must do all or none.

E.g. To take cash from ATM (at your bank)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Steps involved (in a session made up of many different half duplex information exchanges) are :

(i) Insert ATM card to the machine.

(ii) Enter code no; type of transaction, amount of cash in response to prompts.

(iii) Transaction processing time (you wait until the computer checks the validity of your card, pin number, balance etc.)

(iv) Computer verifies and updates your balance by the amount withdrawn ; sends a command to ATM to give cash.

If something wrong happens with the network, money does not reach the machine :

(i) Account debited by the amount of withdrawal, but cash not received (session layer is handling behind the scene).

(ii) it does not allow the transaction to close until all steps have been completed.

(iii) Updating of the account to be done; leaves the update pending until it receives a confirmation from ATM that money has been delivered.

(iv) Transport layer ceases functioning here after delivery of the message to the machine to give money is sent.

(v) Session layer cannot finish untill the receipt of confirmation of the full completion of the transaction.

(vi) The session layer can continue the session with another transport layer connection.

Relationship of the session layer with transport layer regarding communication is of three types :

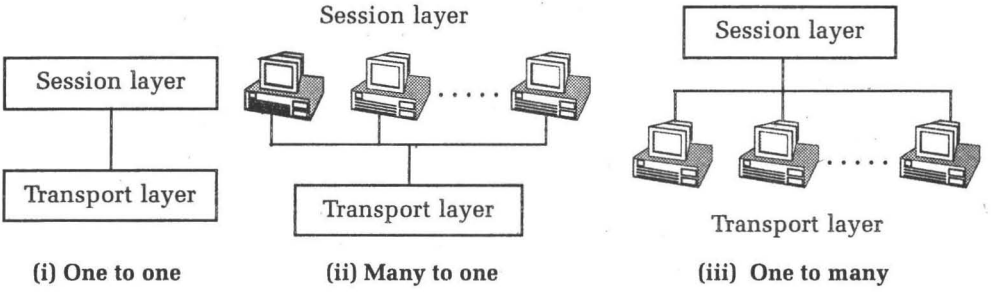


Fig. 22.2 Session-to-transport layer communication

Synchronisation points

- The transport layer is responsible for delivering a transmission with complete reliability. If an error (like a bug in the processing software) is found, the transmission is delivered to the destination process before use. In this case, a session layer provides a mechanism, called *synchronisation points* for recovering data that have been delivered but mishandled.
- The session layer allows *reference points* to be introduced into the data for controlling the flow of information and to allow recovery from software or operator errors.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- The above reference calls may ask for user acknowledgement and may provide a go back facility for data recovery (depending on the type of service)
- Synchronisation points used are of two types :
  - Major : It divides an exchange into a series of dialogs. Each point is to be acknowledged before the session can continue. Any error occurs, data is recovered only upto the last major point. A session layer activity can be of a single dialog or multiple dialogs separated by major synchronisation points.
  - Minor : These are inserted in between the dialog end points and may/may not need confirmation depending on the application and act as *security blankets*. If an error is found the control flow can go back one or more synchronisation points and resend the data.

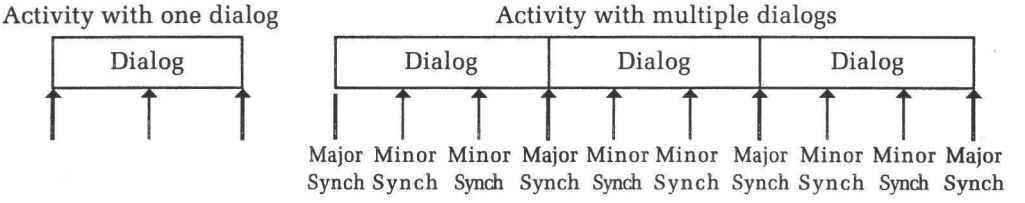


Fig. 22.3 Synchronisation points

In case of failure occurs at midway, the communication is interrupted and the system can go back to the last major synchronisation point and resend the data from there.

Session protocol data unit (SPDU)

36 different types of SPDUs are supported by the session layer.

SPDU identifier (SI) – Indicates type of the data unit.

Length indicator (LI) – Length of the SPDU parameter is given.

Parameter group information (PGI), Parameter Information (PI) } Includes control information and quality of service specifications.

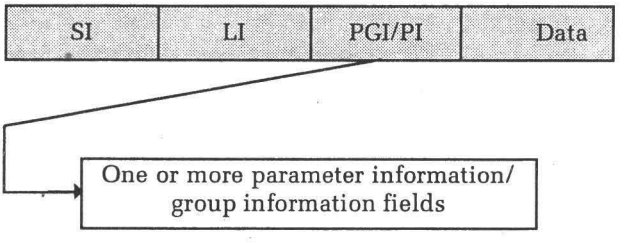


Fig. 22.4 SPDU

22.2 PRESENTATION LAYER (SIXTH LAYER IN TH OSI MODEL)

As already said, the presentation layer formats the data for presentation to the user. Its job is to accommodate the totally different interfaces on different terminals or computers so the application program is free of these. It is concerned with :

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Displaying
- Formatting
- Editing user inputs and outputs.

E.g. This layer might perform data compression, translation between different formats, encryption /decryption, authentication, screen formatting etc. Any function (other than found in layers 1 to 5) is requested sufficiently often to warrant finding a general solution is placed in the presentation layer, though some of these functions can be performed by separate hardware & software (e.g. encryption)

Data compression

It can increase throughput rate of data but it is not the only factor. By compressing the data, it can increase throughput of data over a communication link. One simple way to compress data is to examine it and send an instruction that provides a count of any characters that repeat themselves in sequence. This technique is called run length encoding and is normally used in combination with other techniques like code book compression, which uses specific codes to indicate a pattern of characters and phrases stored in each data compressor's memory.

Data compression uses methods to send data by reducing the number of bits. It is important of multimedia information like text, audio/video are sent. The data compression methods are grouped as :

- Loss less methods
- Lossy methods

In the former, the compressing and decompressing algorithms are usually the inverse in the sense after decompressing, the data remains same as it was before compressing. No loss is found. In loss less compression the techniques are :

(i) Run length compression
(ii) Statistical compression
(iii) Relative compression

(i) Run length compression

Assume data contain strings of repeated symbols (may be bits, characters etc.) the strings can be replaced by a marker by a repeated symbol followed by the number of occurrences. Symbol # is the marker.

E.g. 4 4 4 4 4 4 4 4 4 4 4 → written as #411 (4 number 11 times repeated)
(4 – 11 times)

8 8 8 8 8 8 8 8 8 8 8 8 8 8 → written as #814 (8 number 14 times repeated)
(8 – 14 times)

44444444444126888888888888800000001	→ written as	#411126#813#071
Original data		Compressed data

Fig. 22.5 Run Length Encoding

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

(ii) Statistical compression

Here short codes are used for frequent symbols and long codes for infrequent symbols. The length of the total data can be reduced drastically this way.

Three common encoding systems are :

- Morse code – Uses variable length combinations of mark (dash) and space (dot) to encode data; one symbol codes used to represent the most frequent characters and five symbol codes for the least frequent characters. A dot (.) to represent character E four dashes and a dot (--.--) to represent character Q. Character X may be 11 bits, since seldom used.
- Huffman coding – Uses variable length codes (a strong of 0s and 1s) to encode a set of symbols. It employs coding tables that use a number of bits to represent characters.
- Lempel–Zivcoding – Looks for repeated strings/words; stores them in variables; then replaces occurrence of that string with a pointer to that variable. Words e.g. the, then, and , and some strings like –in, –tion) repeated many times can be stored in separate variables; pointers can point to them. A pointer (address) requires only a few bits; A word may need tens of bits. This method is used in UNIX.

(iii) Relative compression or Differential encoding

The number of bits are reduced; useful if we are sending 30 frames of 0s and 1s every second (Video, commercial TVs). There is little difference between consecutive frames. Hence instead of sending the next similar frame after the 1st frame, send only the difference between frames. The small differences can be encoded into small streams of bits and sent after the 1st frame.

Lossy compression

If decompressed information is not required as an exact replica of the original information but close to it, we can adopt this method. Here some of the original data is lost. E.g. Video transmission. If an image does not have sharp discontinuation after transformation to a mathematical expression, most of the information is contained in the first few terms. These terms reproduces the frame with enough accuracy.

Translation

Character strings stored in computers may use different codes ASCII or EBCDIC. Information sent by one computer in ASCII format where as the receiving computer is EBCDIC, the result would be different. The presentation layer helps in solving this problem. Two methods are :

- The direct method of solving this is ASCII code is translated into EBCDIC code at the receiver (assuming simplex transmission half duplex/full duplex cases) This method is not acceptable in many cases. If computer communicates with other computers, it needs several conversion tables.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- The indirect method of solving this is ASCII code, translated to a standard format at the sender and translated into EBCDIC at the receiver. This is recommended by OSI. Model recommended here is *abstract syntax notation* (ASN-1). Translation problem together with formatting problems (diverse nature of data like text, program etc) and diversity in data storage (computer may store data in different formats) can be handled. ASN-1 provides a mechanism for defining data types (such as integer, real, bits, strings etc) in an implementation – independent format, using the concept of objects. (An object is an information entity having type and value that can be easily translated from one representation to another).

  E.g. In a country, where a word is not understood, its equivalent or meaning can be used by ASN-1. OSI equivalent to defining club soda (not understood in many countries while ordering in a hotel). As its component elements can be defined as carbonation and water.

Encryption/Decryption

The best way to prevent unauthorised access is encryption, a means of disguising information by the use of mathematical rules known as algorithms. Encryption is the process of disguising information , whereas decryption is the process of restoring it to a readable form. There is no sense to have one process without the other. When information is in readable form, it is called clear text or pretext, when in encrypted form, it is called cipher text.

An encryption system has two parts : Algorithm itself, and the key which personalises the algorithm by making the transformation of data unique. A system should assure privacy when sensitive information are carried out e.g. Military or financial data, Microwave, satellite and other wireless media cannot be protected from the unauthorised interception of transmissions. Cable systems also are not an exception. Cables pass through out-of-the-way areas (such as basements) that provide opportunities for malicious access to the cable and illegal reception of information. No system can completely prevent authorised access to transmission media. An important way to protect the information is to change it so that an authorized receiver can understand it. *Data tampering* is a common issue. It is not unique to the computer area. Now the method of making the information unreadable by unauthorised receivers is called as the *encryption* and *decryption* of information. Encryption is that the sender transforms the original information to another form and sends the resulting unintelligible message out over the network. Decryption is the reverse of this to transform the message back to its original form.

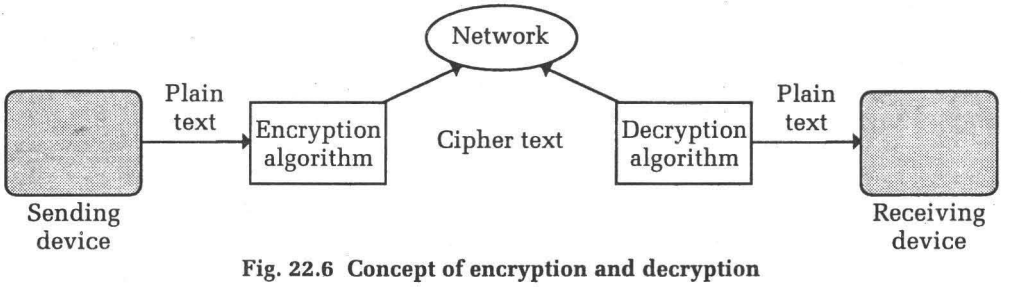


Fig. 22.6 Concept of encryption and decryption

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Encryption and decryption methods fall into two types :

- Conventional
- Public Key

Conventional encryption methods

The encryption key is only known to the sending device.

The Decryption key is known only to the receiving device.

These are not public. These methods started a long time ago. Encryption in the earlier days by monoalphabetic substitution. Julias Caeser in 100–44 BC also used this and hence known as Caeser.

The character substitution is polyalphabetic substitution one character is substituted for another. Plain text character is replaced by different cipher text characters. Substitution depends on the identity of the character and on the position of the character.

Transpositional encryption is still a better method. Here the positions are interchanged to create cipher text. This type of encryption is most efficiently accomplished by organising the text into a two dimensional table; It reorganises the columns according to a key. This indicates which column is transposed with other column.

Most of the above mentioned methods are obsolete. Conventional encryption methods used are on bits, not characters. In bit level techniques, data are divided into block of bits; then altered by substitution, transposition, swapping, exclusive - or circular shifting and so on.

DES (Data encryption standard)

IBM designed BES and this way adopted by the US government in the mid 1970s as the standard encryption method for non-military and non-classified use. DES is maintained by the National Institute of Standards and Technology. Algorithm takes a 64 bit plain text and 56 bit key. The text is put through 19 different and very complex procedures to create a 64 bit cipher text.

Figure 22.7 shows a schematic diagram of DES. First and last two steps are simple. Steps 2 to 17 are complex each requiring sub-steps (combinations of transposition, substitution, swapping, exclusive – or, and circular shift). Each uses a different key in these steps derived from the original key. The input would be output from the previous step, thus additional complexity is achieved.

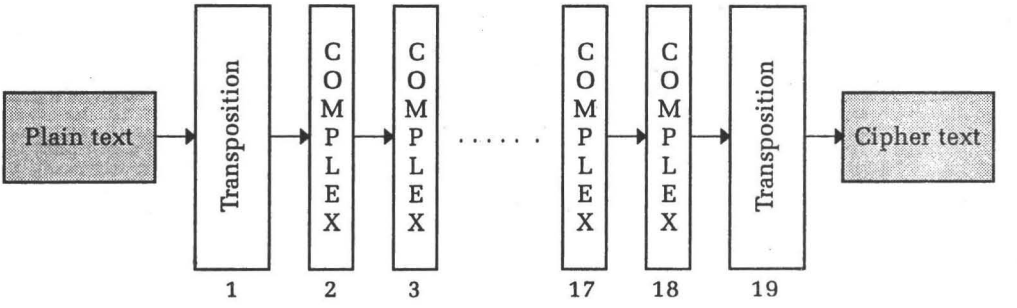


Fig. 22.7 DES

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

DES is a symmetric algorithm, which means that the key used to decrypt a particular bit stream is the same as the one used to encrypt it. Using any other key produces clear text that appears as random as the cipher text. Symmetric algorithm can cause some problems with key management. Keys must be dispersed and stored carefully. Because DES algorithm is known publicly, the disclosure of a secret key can mean total compromise of encrypted messages. In order for two nodes in a network to establish communication of cipher text, it is necessary to generate and communicate a common key over a secure channel or send it by personal courier. DES as classified as a block cipher, since it encrypts data in independent 64 bit blocks under the control of a 64 bit key. A 64 bit key produces about 100 quadrillion possible combinations, which may sound like a lot, but cryptographers who specialise in breaking these block ciphers have to test only half the combinations to obtain a 50/50 probability of arriving at the secret key.

Public key methods

This is a second popular technique, the most popular being RSA.. Public key encryption is inherently different from secret key systems like DES because it is asymmetric. There are two keys.

- *Public key* is used to encrypt the message; based on one way functions.
- *Private key* (very different) is used to decrypt the message.

The *decryption* algorithm is always the inverse of the encryption algorithm and uses the same key. Hence anyone familiar with encryption algorithm and key can work out the decryption algorithm and key. Security can be assured only, if the entire process is kept secret.

Public key system are based on one-way functions. Even if the contents of the message and the public encryption key is known, it is encrypted by the oneway function, the message cannot be decrypted without the private key. One way functions which are relatively easy to calculate in one direction, are impossible to uncalculate in the reversible direction. This is one of the more secure encryption techniques available, excluding special encryption techniques developed by national security agencies. Public key encryption greatly reduces the key management problem. Each user has its public key that is used to encrypt messages sent to it. These public keys are widely publicised (listed in a telephone book-style directory). That is the reason, these are called *public keys*. In addition, each user has a *private key* that decrypts only the messages that were encrypted key. If two parties wish to communicate with one another, there is no need to exchange keys before hand. Each knows the other's public key from the listing in a public directory and can communicate encrypted information immediately. The key management problem is reduced to the onsite protection of the private key.

Public key encryption permits authentication (or digital signatures). If one user sends a message to other, it is difficult to legally identify who sent the message. Legal proof is required in many communications (e.g. Bank transfers, buy/sell orders in currency/stock trading, which normally require legal signatures).

Public key encryption algorithm are invertable (text encrypted with either key can be decrypted by the other). We encrypt with the public key and decrypt

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

with the private key. Viceversa also is possible. As the private key is secret, we can use this to encrypt a message. Thus a digital signature or authentication sequence is used as a legal signature on many financial transactions. The signature is usually the name of the signing party plus other key contents such as unique information from the message (e.g. date, time or rupee amount). This signature is usually the name of the signing party plus other key contents are encrypted by the sender using the private key. The receiver uses the sender's public key to decrypt the signature block and compares the result to the name and other key contents in the rest of the message to ensure a match.

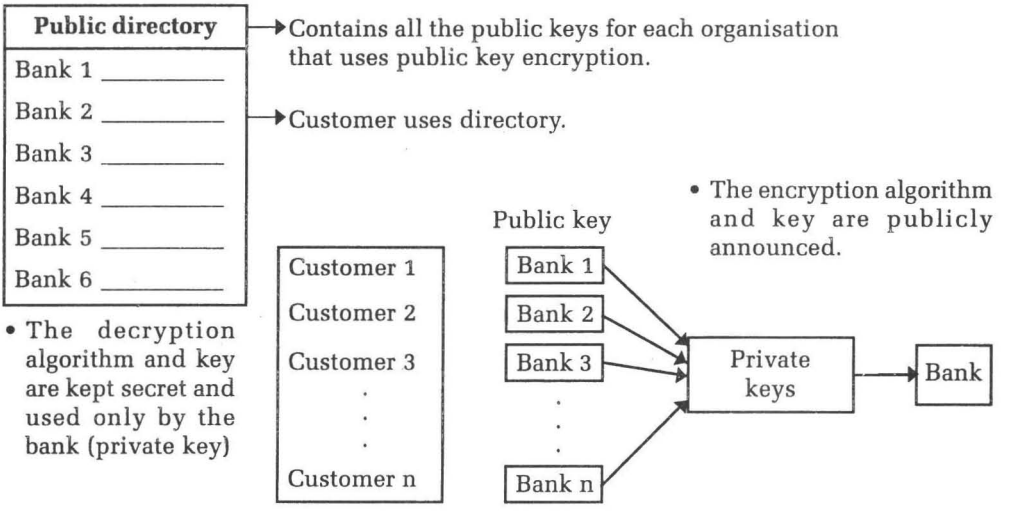


Fig. 22.8 Public key encryption (customers to Bank message)

Message from Bank 4 to Bank 1 (Refer public directory figure)

- Bank 4 wants to send a message to Bank 1 .
- It encrypts the message with Bank 1's public key using public directory a straight forward encryption of a message between Bank 4 and Bank 1.
- When message received at Bank 1, it decrypts the message using its secret private key.
- For complex encryption, Bank 4 can include its signature as authentication. Bank 1 can verify the signature (its ID) plus some of the key contents of the message using the Bank 4 private key.
- Bank 4 encrypts both the entire message contents and the already encrypted Bank 4 ID using the Bank 1 public key. Thus Bank 4 ID has been doubly encrypted (first using the Bank 4 private key then with Bank 1 public key).
- Message is then transmitted to Bank 1. Bank 1 now uses its private key to decrypt the entire message. Here Bank 1 is able to read the contents of the message (except for a block of data that is yet to be encrypted)
- Bank1 takes the Bank 4 public key and decrypts the trailing block of data that contains the Bank 4 ID plus some key contents of the message. Bank 1

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

knows Bank 4 actually sent the message because the key contents in this block of data had a date, time, and rupee amount that matched those in the already decrypted message.

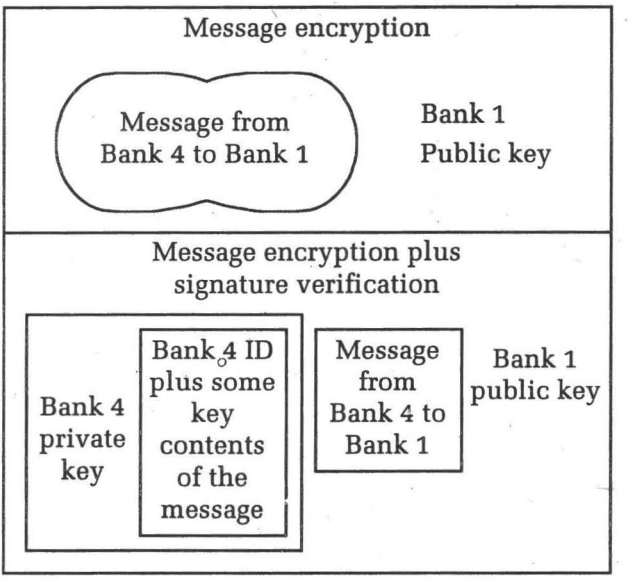


Fig. 22.9 Public Key Encryption (Bank to Bank message)

RSA encryption

It is the most popular technique invented at MIT in 1977 by Rivert, Shamir and Adleman. The inventors of the initial algorithm founded RSA data security in 1982, and many companies have licensed the RSA technique. This algorithm is based on number theory.

E.g. Letter F – Encrypted as 41

- Encode character F to 6 (A, B, C, D, E, – F is the 6th character)
- Choose two prime numbers (e.g. 7 and 17)
- Subtract 1 from each and then multiply i.e. 6 x 16 = 96.
- Choose a number that is relatively prime with 96 (e.g. 5) This number is the Ke (Ke = 5)
- Multiply two prime number originally chosen 7 x 17 = 119
- Calculate 6 Ke% 119 (modulo division) = 41
- The encrypted text 41 is sent along the network. Even if intruder knows this encryption procedure and Ke as 5, he cannot decipher the original character F easily, since the procedure is not reversible.

  At the receiver end, 41 is decrypted as F in a different way, using a different key.
- Subtract 1 from each prime and multiply 6 x 16 = 96
- Multiply two original numbers 7 x 17 = 119

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Find a number Kd, such that $\frac{Kd \times Ke}{96} = \left(\frac{77 \times 5}{96}\right)$ the remainder is 1. Thus we got 77 (kd = 77)
- Calculate the 41 kd% 199 (modulo division), which is 6.
- Decode 6 as F

It appears that if somebody knows Ke = 5 and number 119 could find the secret ke (77) by trial & error. If private key is a large number chosen, instead of 119, it is highly difficult and time consuming to do so.

Authentication (digital signatures)

Public key encryption permits this. When one user sends a message to another, it is difficult legally to prove who actually sent the message. *Authentication* means verifying the identity of a sender. An authentication technique verifies that the message is coming from an authentic sender and not from an imposter. Many methods have been developed, one of which is a digital signature method based on public key encryption/decryption.

Concept of this is similar to that of putting signature on transaction documents when business is carried out in a bank. Banks need your signature while withdrawing heavy amount and the signed form kept for records (for legal purpose, in case of disputes).

It adds another level of encryption/decryption to the process. A private (secret) encryption key is developed and kept by the customer while the corresponding private decryption key is kept and used by the bank. The customer uses one public and private key for encryption and the bank uses one private and one public key (kd) for decryption.

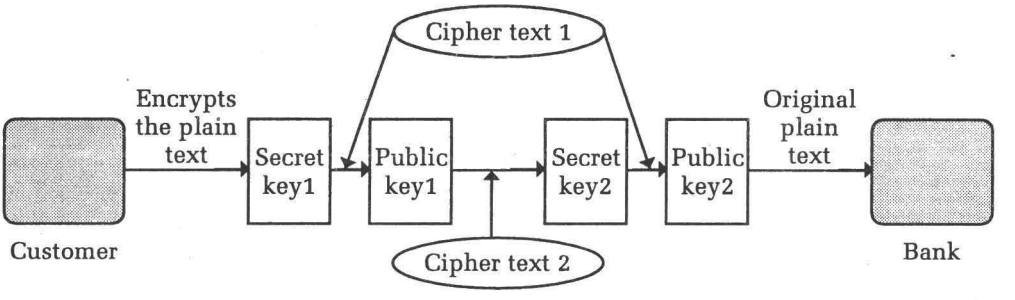


Fig. 22.10 Signature authentication

- Customer encrypts the plain text with secret key (Chosen and kept by the customer); creates the first level of cipher text.
- Cipher text 1 is encrypted again using public key to create cipher text 2 which is sent through the network and received by the bank.
- Bank uses the secret key 2 to decipher into cipher text 1; stores it in a separate file. Public key 2 is used to the decipher cipher text 1 to the original plain text.
- In case of disputes, Banks can show the customer cipher text 1 and apply public key 2 to it to show that it creates original plain text. This would not

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

have been possible unless the customer had applied secret key to the plain text to create cipher text 1.

22.3 APPLICATION LAYER (LAYER 7 OF THE OSI MODEL)

- It primary purpose is to provide a set of utilities for application in programs.
- End user's access to the network.
- It contain whatever functions the user needs like :
  - Electronic mail
  - Airline reservations
  - No standardisation in general is possible.
- Each user program determines the set of message and any action it might take upon receipt of a message.
- Other considerations include :
  - Network management statistics
  - Remote system initiation and termination.
- Network monitoring
- Application diagnostics
- Making the network transparent to users,
- Simple processor sharing between host computers.
- Use of distributed databases and industry specific protocols.

ITU–T specifies several common applications wherein standardisation is possible. Five of them are :

(i) Message handling system (MHS)
(ii) File transfer access and management (FTAM)
(iii) Virtual terminal (VT)
(iv) Directory system (DS) and
(v) Common management information protocol (CMIP)

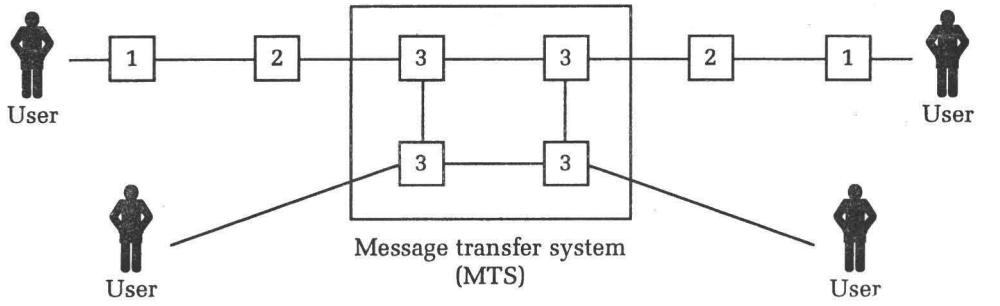
(i) Message handling system (MHS)

- It is the OSI protocol that underlies : electronic mail and store and forward handling.
- Derived from the ITU–T X.400 series.
- Used to send any message (copies of data, files etc) that can be delivered in a store and forward manner (Instead of opening an active channel between sender and receiver the protocol provides a delivery service that forwards the message when a link becomes available. If not possible to transmit the message immediately it stores the message until the conditions change. When the message is delivered, it is stored in the recipients mail box until called for). In most information sharing protocols, both the sender and the receiver must be able to participate in the exchange concurrently. (e.g. A regular postal system is similar to OSI models message handling system).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

MHS structure



Note : 1 is user agent
2 is Message storage (mail box)
3 is Message transfer agent

Fig. 22.11 MHS

The MHS structure of the OSI message handling system is shown as above in figure 22.11

Users communicate with a program or process called a *user agent*. It is unique for each user (Each user receives a copy of the program or process).

(E.g. Electronic mail program associated with a specific operating system that allows a user to type and edit message)

Message storage : Consists of disk space in a mail storage system, known as Mail box. It can be used for storing, sending or receiving messages. It communicates with a series of processes called message transfer agents (MTAs). It is like different departments of a post office. All these put together is message transfer system (MTS).

Message format

- Standard defines the format of a message.
- Body of the message (is something like a letter in the envelope of a conventional mailing)
- Messages include the address of the sender (name), the address of the recipient (name), subject of the message. List of any others to receive the copy.

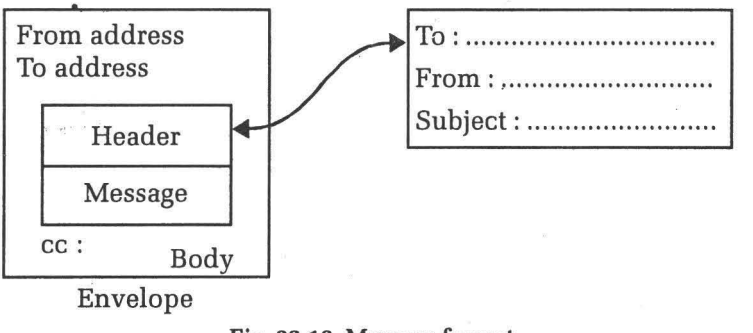


Fig. 22.12 Message format

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

(ii) File transfer, access and management (FTAM)

This protocol is used to :

(a) Transfer/copy

(b) Access (Read, Write or Modify) and

(c) Manage (Control) files.

Files are stored in different system in different fashions (eg. UNIX – a file is sequence of characters (bytes); IBM VMS – a file is a collection of records). The organisation of a file depends on the operating system of the host.

Virtual files and file stores

- FTAM uses the concept of virtual files and virtual file stores, to allow the interaction of different file systems (virtual file store is a nonimplementation specific model for files/databases that can be used as an intermediary for file transfer, access and management). Concept of file store for files is similar to that behind ASN-1 for data.
- FTAM is based on asymmetrical access of a virtual file. (asymmetrical is that each transaction requires an initiator and a responder). The initiator requests the transfer of, access to or management of a file from the responder. Responder creates a virtual model of its actual file and allows the initiator to use the virtual model instead of the real file.

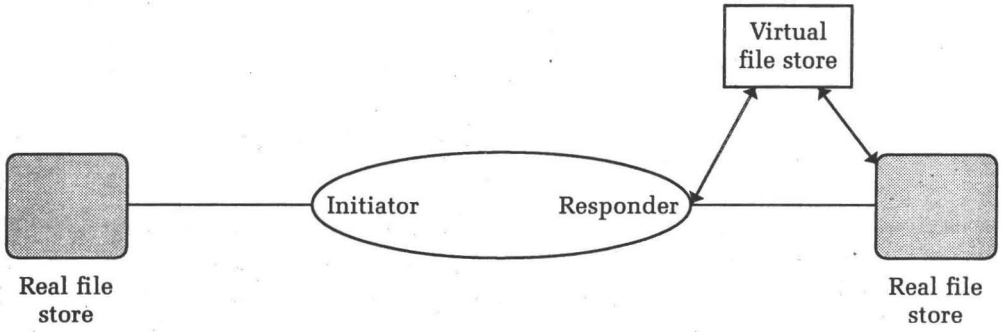


Fig. 22.13 Virtual file storage

Since the model is software, it can be designed to be independent of hardware and operating system constraints. The model creates a secure separation between the file that the initiator is allowed access to and others in the same real storage.

- The creation of a virtual file store is based on two aspects of the file:
  - attributes; a set of properties or security measures used to control either the contents or access.
  - content
- FTAM distinguishes between two different types of attributes :
  - per content; related to the contents of the file.
  - per access; security measures that control access to the file.

(iii) Virtual terminal (VT)

- One of the most important applications in the OSI model.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

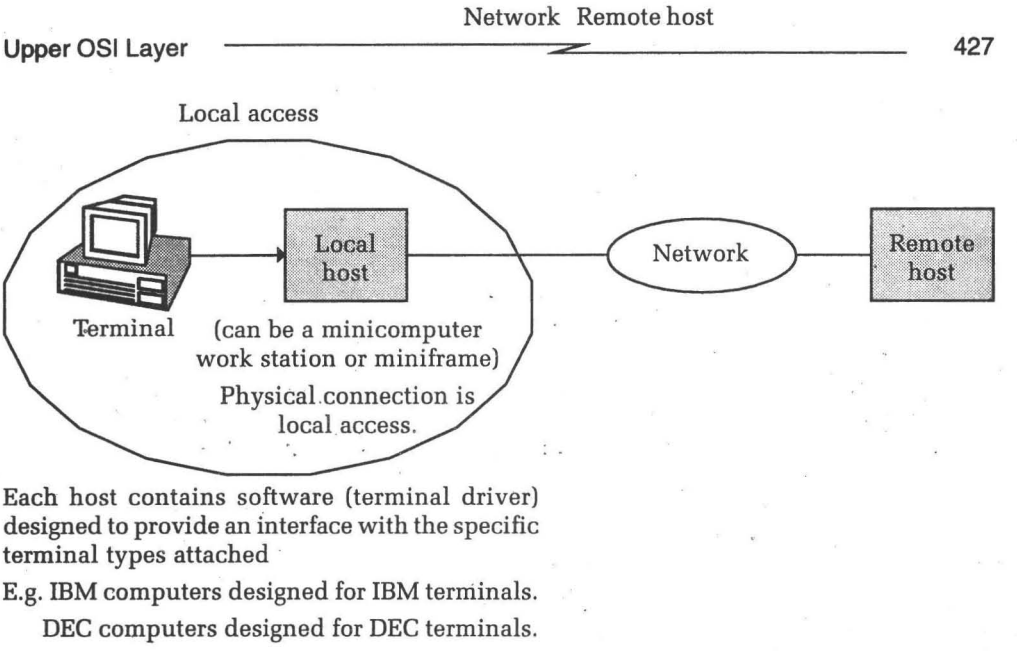


Fig. 22.14 Remote access

If the terminal and the remote host are of the same type eg. IBM, then the network acts as an extra-long local link. Remote host is of another type, problem arises, needing hundreds of terminal drivers. Hence challenge for the designers of OSI model was to create a mechanism to allow any terminal to have access to any computer despite hardware incompatibility.

The above problem was overcome by a construct called a *virtual terminal* which is an imaginary terminal (a software model) with a set of standard characteristics that every host understands – a software version of physical terminal.

In the above figure 22.14 a terminal wishing to communicate with a remote host:

- Communicates first to its local host.
- Local host contains VT software; translates the requester data received from the actual terminal into the intermediary format used by the VT.
- Reformatted data travels over the network to the remote host.
- Remote host passes the transmission to its own VT software; transforms it from its VT format into the format used by the remote hosts own terminals.
- Remote host receives the input as if from a local host (VT).
- After processing the request, the remote host can return a response in the reverse way same procedure.

(iv) Directory Service

- OSI directory service is designed as per ITU–T X.500 standard. A *directory* is a global source of information about different objects.
- It's service is an application program used to represent and locate objects (people, organisations, logical groups, programs, files etc) found in an OSI directory.
- Type of information a directory holds varies according to the type of the object.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- A directory service for the user is that all the information appears to have been stored in a single database in a single host (which is impractical).
- A *directory* is a distributed database, with each host holding only a part. User known only one entry port from which all information may be retrieved as the access mechanism is structured (user may be a person or an application in a directory service).
- DIB is the directory information base, containing the information; stored as set of entries, each describ .g one object. An entry consisting of several parts, each one describes a different attribute of the object. E.g. an entry about the ISO might include (i) a short description of the purpose of the organisation (ii) a mailing address (iii) phone number ... etc.
- The structure of DIB can be organised as a tree with different levels.

DUAs and DSAs

(i) DUA is *directory user agent* which provides the users to gain access to the DS. It communicates with one or more entities called *directory system agents* (DSAs).

(ii) DUA passes a request for information to a DSA.

(iii) If a DSA known the information availability, it fills the request or passes it on to another DSA with the necessary access etc. The requested information is retrieved and passed back to the DUA through successive DSAs.

(iv) If a DSA doesn't know how to fill a request, it can do so by three ways.
- It can forward the request to a DSA with access to different level of the tree.
- It can broadcast the request and wait for a response.
- It can return report of failure to the DUA.

(v) Common management information protocol (CMIP)

- A series of services for the management of an OSI system have been developed combinedly by ISO & ITU–T. The most important is CMIS – *Common management information services;* Protocol for implementation of this is *CMIP*.
- Managed objects occur by monitoring and manipulating communication between OSI entities in all CMIP management.
- These are network resources – a work station, a switch, routing hardware, software, queuing programs etc.
- CMIP allows two OSI management service users to perform actions on managed objects (including changing status for efficiency and testing purposes) and to collect data about the status of those objects.
- A user can evaluate the performance of a system and identify the problems as and when it occurs (i) by keeping logs of collected data (the number of bytes of data processed by a router over specified periods of time) and (ii) by changing the settings of managed object and (iii) monitoring the response.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

CMIS

Five objectives to be fulfilled are :

- Fault management – Services like detect, isolate and correct any normal operation of the OSI environment, specific tasks are diagnostic testing, fault tracing, fault correction.
- Accounting management – Services are to track user costs and charges, and if necessary to place limits on the use of managed objects.
- Configuration and name management – Services are included for initialising and closing down managed objects, for reconfiguring an open system, for associating names with objects/set of objects. CMIS allows a user about the continuous operation of communication services in an environment changing frequently.
- Performance management – Here services are for the users to evaluate the behaviour of managed objects and the effectiveness of networking functions.
- Security management – To evaluate the effectiveness and operability of network security measures.

CMISE (Common management information service elements)

CMIS provides specific services CMISE, which falls into three types :

(i) Management association services : This establishes application associations to allow CMIS users to communicate. The three association service elements are :

M-INITIALISE – used to establish an association with a peer CMISE service.

M-TERMINATE – used to obtain normal termination of an association

M-ABORT – used to obtain an abrupt release from an association

(ii) Management notification services : This is used to convey notifications of managed object events.

M-EVENT-REPORT – used to report managed object events to a service user. A report can be any event the CMISE user chooses to collect and include a time stamp of the occurrence.

(iii) Management operation services

Six services to a CMISE user :

M-GET – Requests the retrieval of management information

M-CANCEL-GET – Requests cancellation of a previous M-GET request.

M-SET – Requests the modification of specific attribute values of a managed object.

M-ACTION – Requests another user to perform an action on a managed object.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

M -CREATE – Requests another user to create a representation of an instance of a managed object and the associated management information values.

M-DELETE – Requests a peer user to delete an instance of a managed object (opposite to M-CREATE).

POINTS TO REMEMBER

- The session layer is responsible for initiating (establishing), maintaining and terminating each logical session between end users (synchronisation)
- A session layer provides a mechanism called synchronisation points for recovering data that have been delivered but mishandled. It allows reference points to be introduced into the data for controlling the flow of information and to allow recovery from software or operator errors.
- The presentation layer formats the data for presentation to the user. Its job is to accommodate the totally different interfaces on different terminals or computers so the application program is free of these. It is concerned with displaying, formatting, editing user inputs and outputs. It handles translation, encryption, authentication and compression.
- Data compression can increase throughput rate of data, but it is not the only factor. By compressing the data, it can increase throughput of data over a communication link. Data compression methods are two : loss less methods, Lossy methods. In loss less compressions, the techniques used are run length compression, statistical compression and relative compression.
- Encryption is the process of disguising information whereas decryption is a process of restoring it to a readable form.
- Encryption renders a message – plain text unintelligible to unauthorised personnel. Decryption transforms an unintelligible message (cipher text) into meaningful information.
- Encryption and decryption methods fall into two types conventional and public key.
- In conventional encryption, the encrypting algorithm is known by everyone but the key is secret except to the sender and the receiver.
- DES is a symmetric algorithm, which means that the key used to decrypt a particular bit stream is the same as the one used to encrypt it.
- Public key method is second popular technique after RSA algorithm. In this encryption, both the encrypting algorithm and the encryption key are known to everyone but the decryption key is known only to the receiver. Digital signature is one of the authentication method used today.
- Five standard application protocols are the following :
  - Message handling system (MHS) – the protocol for electronic mail and store and forward handling
- File transfer, access and management (FTAM) – used to transfer/ copy, access (read, write or modify) and iii) manage (control) files.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Virtual terminal (VT) – allows dissimilar terminals or machines to communicate with one another.
- Directory service (DS) – It is a directory created by an application program to find OSI objects.
- Common management information protocol (CMIP) – A series of services for the management of an OSI system have been developed combinedly by ISO and ITU-T. The most important is CMIS – Common management information services.

QUESTIONS

1. What are the responsibilities of the three upper layers? Explain each of them.
2. What are the services of the session layer ?
3. Explain session and transport layer interaction.
4. Define synchronisation point. Explain.
5. What is SPDU? Explain.
6. What do you mean by data compression? Which are the types of compression methods? Explain each one of them in brief.
7. What are the different types of compression techniques found in loss less compression? Explain in brief.
8. Explain encryption/decryption? Why are they needed? Give examples.
9. Which are the two types of encryption and decryption methods ? Explain them.
10. What do you mean by transpositional encryption?
11. What is DES? Explain.
12. Explain public key methods ? What are the two keys used in it? Explain them.
13. Explain public key encryption with an example.
14. Explain RSA encryption. Why is it popular ?
15. What is digital signature? Why is it needed?
16. Which are the five different standard application protocols? Explain them in brief.
17. What do you mean by virtual terminal? What is the concept of VT needed? Why is it considered as one of the most important applications in the OSI model?
18. Explain the functions of common management information protocol and its services.

FILL IN THE BLANKS

1. Dialog establishment, maintenance, synchronisation and termination are connected with _____ layer.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

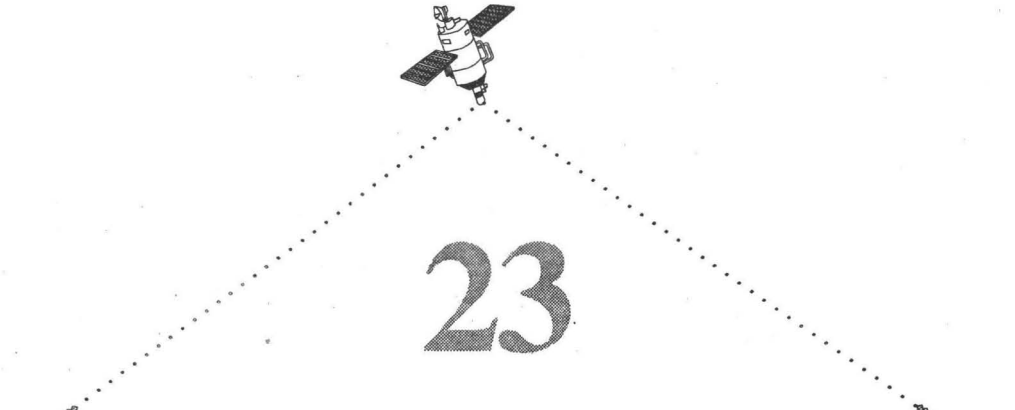
2. The _____ layer disconnect a session abruptly and _____ layer provides for graceful closure.
3. The protocol to define services that manage a system based on the OSI model is called _____ .
4. CMISE is _____ _____ _____ _____ _____ .
5. DUA passes a request to the information to the _____ .
6. In MHS, UA is a _____.
7. SPDU IS _____ _____ _____ _____.
8. A protocol that is connected with file transfer, management and access is _____.
9. A protocol using a store and forward method for delivery is _____ .
10. An application program _____ represents and locate objects in a directory.
11. _____ points provide a method to recover data that has been delivered but not yet used.
12. In conventional encryption, the main problem found is the maintenance of the secrecy of the _____.
13. In the public key method of encryption and decryption, the publicly known key is _____ .
14. In the public key method of encryption and decryption the receiver has possession of the _____ key.
15. Encryption and decryption are functions of the _____ layer.
16. RSA encryption is named after _____ _____ _____ inventors.

Answers

1. session
2. transport ; session
3. CMIP
4. Common management information service elements
5. DSA
6. program
7. session protocol data unit
8. FTAM
9. MHS
10. DS
11. Synchronisation
12. key
13. encryption
14. decryption
15. presentation
16. Rivert, Shamir, Adleman

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.



23

TRANSMISSION CONTROL PROTOCOL (TCP)/ INTERNET PROTOCOL (IP)

23.1 OVERVIEW OF TCP/IP

TCP/IP is the oldest net working standard, developed for the US department of defense's advanced research project agency network (ARPANET) in the 1970s. It is also the most popular network protocol used by almost 50 percent of installed backbone, metropolitan and WAN. It is the network protocol used on the Internet. It allows reasonably efficient and error - free transmission between different systems. It is a file transfer protocol and hence can send large file of information across sometimes unreliable networks ensuring that the data will arrive uncorrupted. It is compatible with a variety of data link protocols, hence popular. In a survey conducted 5 years back by mainframe network managers, many have opined that TCP/IP was critical to their future plans (about 79%) and another 18% said it is important. TCP/IP is a set of protocols or a protocol suite to know how all transmissions are exchanged across the Internet. ARPA established a packet switching network of computers linked by point-to-point leased lines called ARPANET which provided a basis for early research in networking.

TCP/IP and the Internet

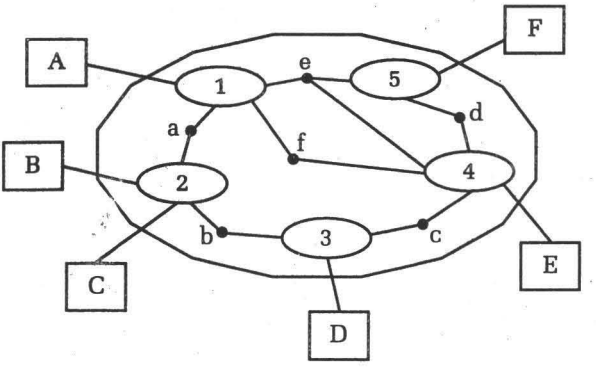
TCP/IP and the concept of internet working were all developed simultaneously. The growth of each is from the other. Let us understood how TCP/IP relates to the physical entity of the internet it serves.

TCP/IP has two parts. TCP performs the functions of the transport layer in the OSI model (sequence of operations are : breaking the data into smaller packets, numbering them, ensuring each packet is reliably delivered, putting them back in the proper order). IP performs the role of the network layer in the OSI model (e.g. routing and addressing). TCP/IP can operate as either connection - oriented or

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

connectionless. TCP is inherently connection oriented while IP is inherently connectionless. An internet under TCP/IP operates like a single network connecting many computers of any size/type. An internet is an interconnection of independent physical networks (such as LANs) linked together by internetworking devices. Figure 23.1 shows the topology of a possible internet.



A, B, C, D, E, F – hosts (computers)

1, 2, 3, 4, 5 – Physical networks

a, b, c, d, e, f – routers/gateways

For TCP/IP, the same internet appears differently. TCP/IP considers all interconnected physical networks as one huge network (1 + 2 + 3 + 4 + 5)

Fig. 23.1 An Internet

It considers all the hosts are connected to this one big network rather than to their individual physical networks.

TCP/IP and OSI

TCP was developed before OSI was developed. Hence the layers in both two do not match. TCP/IP protocol is of 5 layers :

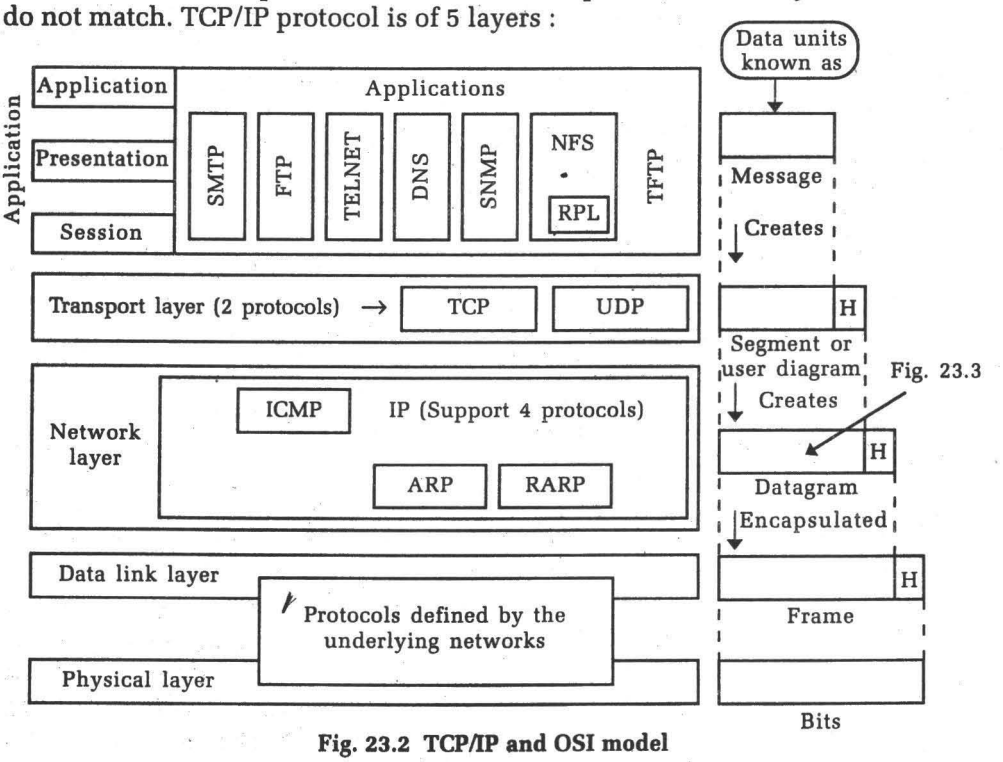


Fig. 23.2 TCP/IP and OSI model

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Above figure shows the encapsulation of data units at different layers of the TCP/IP protocol suite.

The movement of the datagram (IP Layer) across the Internet is the responsibility of the TCP/IP protocol. In order to move physically from one network to another, the datagram is to encapsulated in a frame in the data link layer of the underlying network and finally transmitted as signals along the transmission media.

23.2 NETWORK LAYER

At the network layer, TCP/IP supports the internetwork protocol IP, which in turn supports 4 protocols These are :

- ICMP (Internet control message protocol) handles error and control message.
- IGMP
- ARP (Address resolution protocol) – obtaining the physical address of a node when the internet address is known .
- RARP (Reverse address resolution protocol) – allows a host to discover its internet address when it knows only its physical address.

Internetwork protocol (IP)

- It is the transmission mechanism used by TCP/IP protocols.
- Unreliable and connectionless datagram protocol (best effort delivery service) (Best effort means IP provides no error checking or tracking).
- Assumes the unreliability of the underlying layers and gives best to get a transmission through to its destination (with no guarantee).
- Transmission along physical networks gets destroyed for various reasons.
  - Noise can cable bit errors during transmission across a medium.
  - Congested router may discard a datagram if enable to relay it before a time limit.
  - Routing quirks can end in looping (ultimate destruction of a datagram)
  - Disabled links leave no usable path to the destination.
- For good reliability, IP must be paired with a reliable protocol like TCP e.g. best effort delivery service in a post office; self addressed stamped post card. If the reply card not received, the sender will think it is lost. Sender many a times joins with the post office to find out the lost letter (if registered letter is lost). In the case of unregistered letter, the sender takes the responsibility rather than the post office.
- IP transports data in packets known as datagrams. These are transported separately and travel along different routes and may arrive out of sequence or even duplicated. IP will not keep track of the routes and has no facility also for reordering datagrams once they arrive. Since it is a connectionless service, IP does not create virtual circuits for delivery; No call setup to alert the receiver to an incoming transmission.
- IP functionality in a limited way is not a weakness.
- IP provides bare-bones transmission functions; frees the user to add only those facilities necessary for a given application; allows for maximum efficiency.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

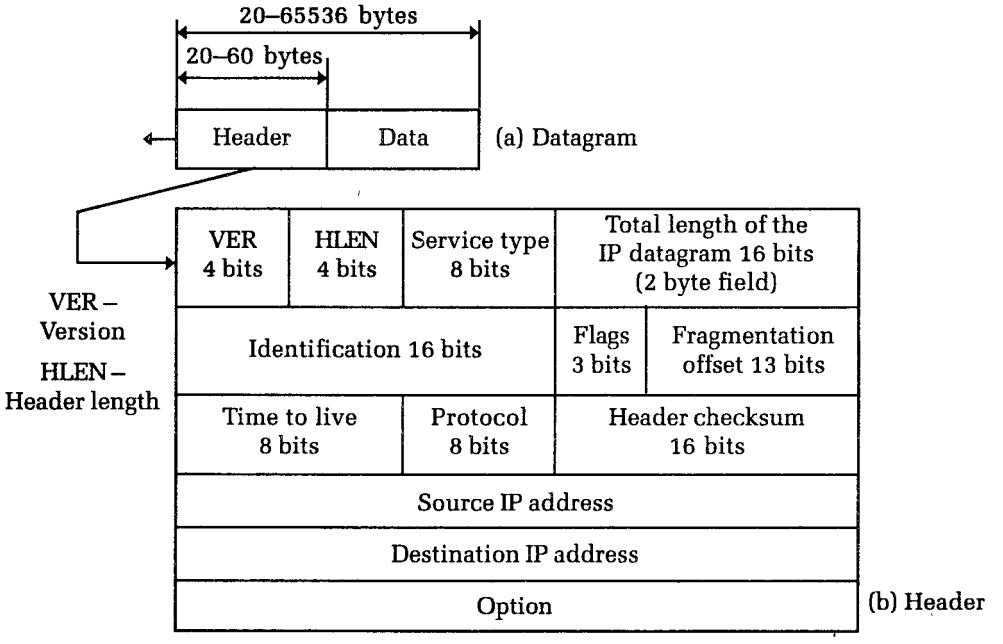


Fig. 23.3 IP datagram

- Datagram is a variable length packet (upto 65,536 bytes); consists of two parts Header and data [Figure (23.3(a)]
- Header can be 20 to 60 bytes and contains information essential to routing and delivery.
- Header is in 4 byte sections in a TCP/IP.
  - *Version* is first field; defines version number of the IP: current version is 4 (IPV4) with a binary value of 0100.
  - *Header length (HLEN)* : defines the length of the header (multiple of 4 bytes). The four bits can represent a number between 0 & 15; Multiplied by 4 gives a maximum of 60 bytes.

Service type : Defines how the datagram should be handled; includes bits that define the priority of the datagram; also contains bits that specify type of service the sender desires such as the level of throughput, reliability and delay.

Total length : Can define up to 65,536 bytes; two byte field.

Identification : Used in fragmentation. Datagram when passing through different networks, may be divided into fragments to match the network frame size. If this occurs, each fragment is identified with a sequence number in this field.

Flags : Bits in the flags deal with fragmentation (Datagram can/cannot be fragmented; can be the first, middle or last fragment etc.)

Fragmentation offset : A pointer shows the offset of the data in the original datagram (if it is fragmented).

Time to live : This field defines the number of hops a datagram can travel before it is discarded; source host, when it creates the datagram sets this field to an initial value; when the datagram travels through the internet router by router,

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

each router decrements this values by 1. If this value becomes 0 before the datagram reaches its final destination, the datagram is discarded. This prevents a datagram from going back and forth between routers.

Protocol : Field defines which upper–layer protocol data are excapsulated e.g. TCP, UDP, ICMP etc.

Source address, destination address : Each field is a four byte (32 bit) Internet address. It identifies the original source and final destination of the datagram respectively.

Options : The field gives more functionality to the IP datagram. It carries field that control routing, timing, management, and alignment.

Addressing : Physical addresses are on NICs. It identifies individual devices. The internet requires an additional addressing consention :

- an address that identifies the connection of a host to its network.
- each internet consists of four bytes (32 bits) defining three fields :

(i) Class type
(ii) Netid
(iii) Hostid

} Varying lengths and depends on the class of the address.

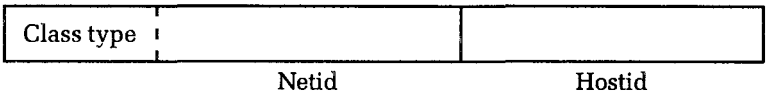


Fig. 23.4 Internet address

Classes :

- It accommodate the vast number of addresses (required for global interconnectivity)
- Class type fields vary in length.
- Five different field length patterns are in use (each defining a class of address)
- Different classes are designed to cover the needs of the different types of organisations, e.g. class A addresses are the lowest.

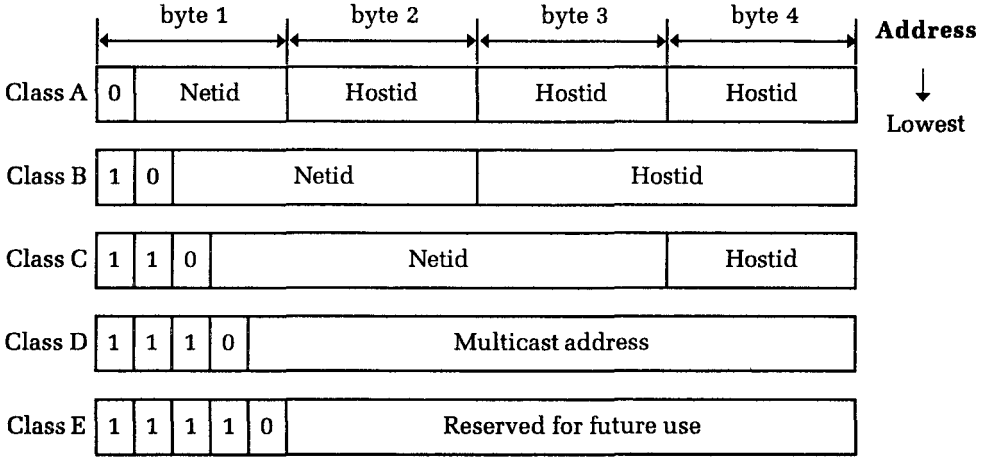


Fig. 23.5 Internet classes

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Multicast addresses allows copies of a datagram to be passed to a select group of hosts rather than to an individual host; similar to broadcasting (Broadcasting requires that a packet be passed to all possible destinations). Allows transmission to a selected subset.

	From		To	
	Netid	Hostid	Netid	Hostid
Class A	0	. 0 . 0 . 0	127	. 255 . 255 . 255
	Netid	Hostid	Netid	Hostid
Class B	128 . 0 .	0 . 0	191 . 255	. 255 . 255
	Netid	Hostid	Netid	Hostid
Class C	192 . 0 . 0 .	0	223 . 255 . 255	. 255
	Hostid		Hostid	
Class D	224 . 0 . 0 . 0		239 . 255 . 255 . 255	
	Undefined		Undefined	
Class E	240 . 0 . 0 . 0		247 . 255 . 255 . 255	

Fig. 23.6 Class range of internet addresses

Nodes with more than one address

- Internet address defines the nodes connection to its network.
- Any device connected to more than one network (any router) must have more than one internet address. A device has a different address for each network connected to it.

A sample internet

- An address specifies both the network to which a host belongs (netid) and the host itself (hostid).
- An example given below is an internet made up of LANs (two ethernets and one token ring). Addresses are all class B.

  An internet addresses specify both the network and hosts addresses (Host belongs either netid or hostid). Figure 23.7 gives an example of an internet made up of 3 LANs (two Ethernets and a token ring). Addresses are taken from class B. Routers and gateways are shown as Rs and Gs and these have separate addresses for each of its connected networks. The hostid parts are set to 0s. A host with more than one IP address is a multi-formed host. Network addresses are 139.6.00, 182.2.0.0 and 178.5.0.0.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

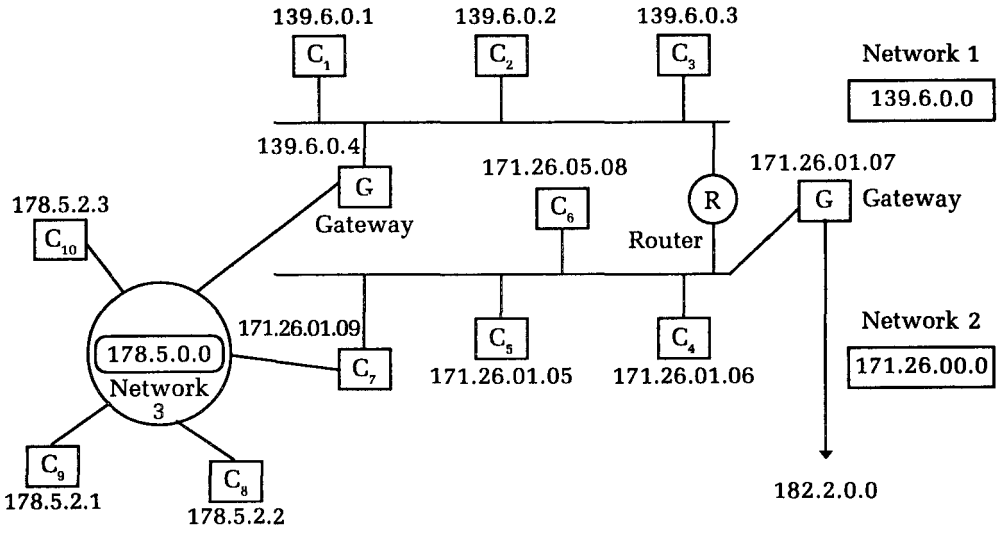


Fig. 23.7 Network and hosts addresses in an internet

Other protocols in the network layer

See figure 23.2. TCP/IP supports the following protocols in the network layer:

(i) Address resolution protocol (ARP) :

- This is used to connect an IP address with the physical address.
- In a LAN (a Physical network), each device on a link is identified by a physical or station address (imprinted on the network interface card NIC)
- Physical addresses can be meddled (changed); They have only a local jurisdication. E.g. Physical address changes of NIC on a machine fails.
- IP addresses, on the contrast have universal jurisdiction and cannot be changed.
- ARP is used to find the physical address of the node when its internet address is known.
- A router, a host in order to find the physical address of another host on its network, it formats as ARP query packet. It includes the IP address and then broadcasts over the network.

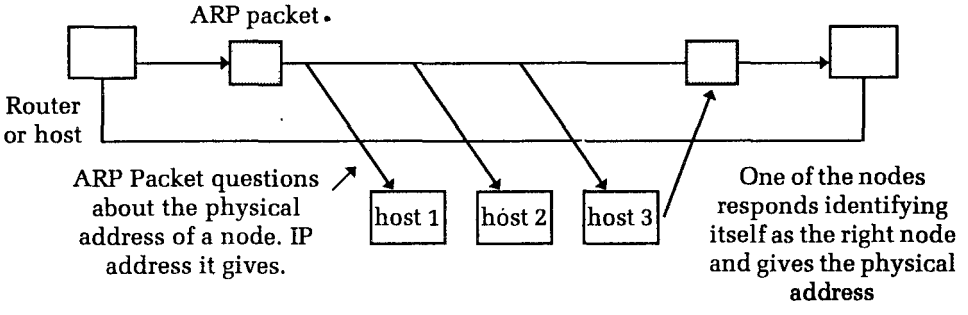


Fig. 23.8 ARP request/response

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Every host on the network receives the message and processes the ARP packet.
- Intended recipient recognises its internet address and sends the physical address.

(ii) Reverse address resolution protocol (RARP)

- It allows a host to discover its internet address, only when it knows its physical address. Though host is supposed to have its internet address on its disk, But in the case of host being a diskless computer, or being converted to the network for the first time (when it is being booted) or a new computer with old NIC, the above is required.
- RARP works similar to ARP. Host wishing to retrieve its internet address broadcasts an RARP query packet that contains its physical address to every host on its physical network. Server on the network recognises the RARP packet and returns the hosts' internet address.

(iii) Internet control message protocol (ICMP)

- It is a mechanism used by hosts and gateways to send notification of datagram problems to the sender.
- An unreliable and connectionless protocol; Allows IP to inform a sender if a datagram is undeliverable.
- Datagrams travels from gateway to gateway till it reaches one that can deliver it to its final destination.
- If this is not possible due to some unusual conditions like disabled links, or the device is on fire, or because of network congestion, ICMP allows it to inform the original source.
- It uses echotest/reply to test whether a destination is readable and responding; also handles both control and error messages; its sole function is to report problems and not to correct them. Responsibility for correction lies with the sender.
- A datagram carries only the addresses of the original sender and the final destination. The addresses of the previous routers that passed it along is not known to it. Hence ICMP can send messages only to the source, not to an intermediate router.

23.3 TRANSPORT LAYER (LAYER 4 OF THE OSI MODEL)

It is often called the host to host layer or end-to-end layer. It establishes, maintains, terminates logical connections. It is represented in TCP/IP by two protocols : TCP and UDP. UDP out of the two is the simplest.

User datagram protocol (UDP)

UDP is user datagram protocol. It is an end-to-end transport level protocol. It adds only port addresses, checksum error control and length information to the data from the upper layer.

Packet produced by the UDP is called a user datagram. The fields in UDP are:

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

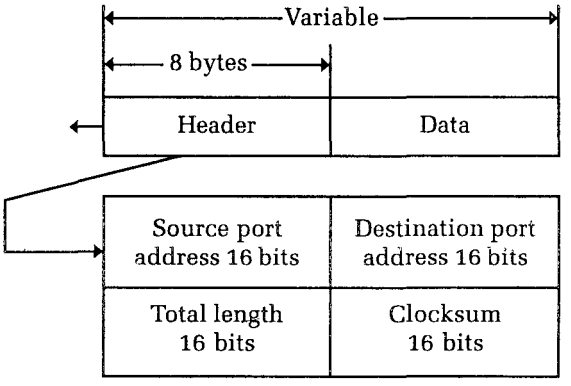


Fig. 23.9 UDP Datagram format

(i) *Source port address* : Address of the application program that has created the message.

(ii) *Destination port address* : Address of the application program that will receive the message.

(iii) *Total length* : Total length of the user datagram in bytes.

(iv) *Checksum* : 16 bit field used in error detection.

- UDP provides only the basic functions needed for end–to–end delivery of a transmission. However, it will not provide any sequencing/reordering functions.
- It cannot specify the damaged packet while an error is reported (Here it must be paired with ICMP).
- UDP can find out if an error has occurred after which ICMP can inform the sender about the damage and discard of the user datagram.
- Both cannot specify which packet has been lost; UDP contains only a checksum and do not contain ID or sequencing number for a particular data segment.
- UDP provides nonsequenced transport functionality when reliability and security are not much important than size and speed. UDP is unreliable and connectionless.

Transmission control protocol (TCP)

TCP is used in most applications since these need reliable end to end delivery. TCP provides full transport layer services to applications. TCP is a reliable *stream transport port to port protocol.* Stream means connection oriented. A connection is to be established between both ends of a transmission before either may transmit data. TCP in between a sender and receiver generates a virtual circuit, which is active for the duration of a transmission (connections are handled by session functions in individual applications).

TCP begins each transmission after alerting the receiver. This makes the receiver to know that more datagrams are on their way and each transmission ends with a connection termination. The receiver knows that instead of a single packet, the entire transmission is expected.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

IP and UDP finds that multiple diagrams belonging to a single transmission as independent units are different from each other and not related. Each datagram when it arrives at the destination as a separate unit is unexpected by the receiver. TCP on the contrary is responsible for the reliable delivery of the entire stream of bits. This is what contained in the data unit originally generated by the sending application. By providing error detection and retransmission of damaged frames, reliability could be ensured. The virtual circuit is discarded after all the segments are received and acknowledged before the transmission is complete.

TCP divides long transmissions into a number of smaller data units and packages each into a frame known as segment at the senders end of each transmission. The segment thus formed includes :

(i) a sequencing number for reordering after receipt.

(ii) an acknowledgement ID number

(iii) window-size field for sliding window ARQ

Segments are carried across network links inside IP datagrams. TCP collects each datagram as it receives at the receiving end and reorders the transmission based on sequence numbers.

Most applications in the transport layer require reliable end-to-end delivery and hence make use of TCP. IP delivers a datagram from source host to destination host.

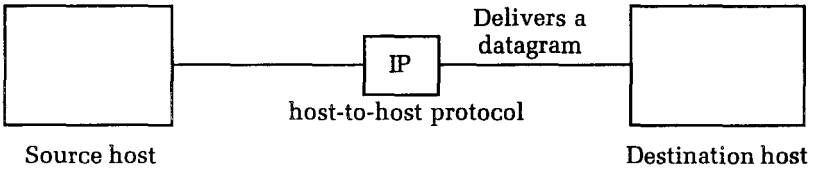


Fig. 23.9 UDP

Operating systems of the present day, support multi user, multiprocessing environments. An executing program is called a process. A datagram received by a host may run several different concurrent processes. Any one of which is a possible destination. Though it is said that hosts sending messages to other hosts over a network, it is the source process actually sends a message to the destination process.

The transport protocols of TCP/IP suite define a set of conceptual connections to individual processes called *Protocol Parts* (or ports).

A *protocol port* is a destination point (a buffer) for storing data to be used by a particular process. Hosts operating system provides the interface between processes and their corresponding ports.

IP is a host-to-host protocol. It can deliver a packet from one physical device to another. TCP/IP's transport level protocols are nothing but port-to-port protocol which operates on top of the IP protocols and delivers the packet from the originating port to the IP services at the commencement of transmissions and also from the IP services to the destination port at the end.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

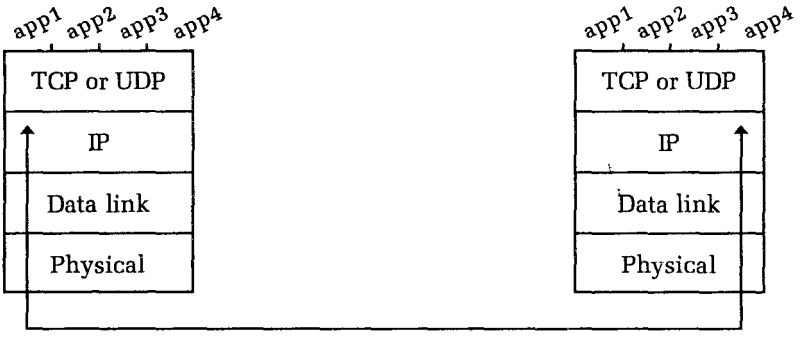


Fig. 23.10 Port-to-port addresses

Each port is defined by a positive integer address carried in the header of a transport layer packet.

IP datagram uses :

- Hosts 32 bit internetaddress
- A frame at the transport level uses the process port address of 16 bits.

This would allow the support of up to 65,536 (00000 to 65535) ports.

TCP Segment

TCP services require that the segment header to be extensive. Figure 23.11 below shows a TCP segment format compare the same with that of UDP datagram format to know the differences between the two protocols.

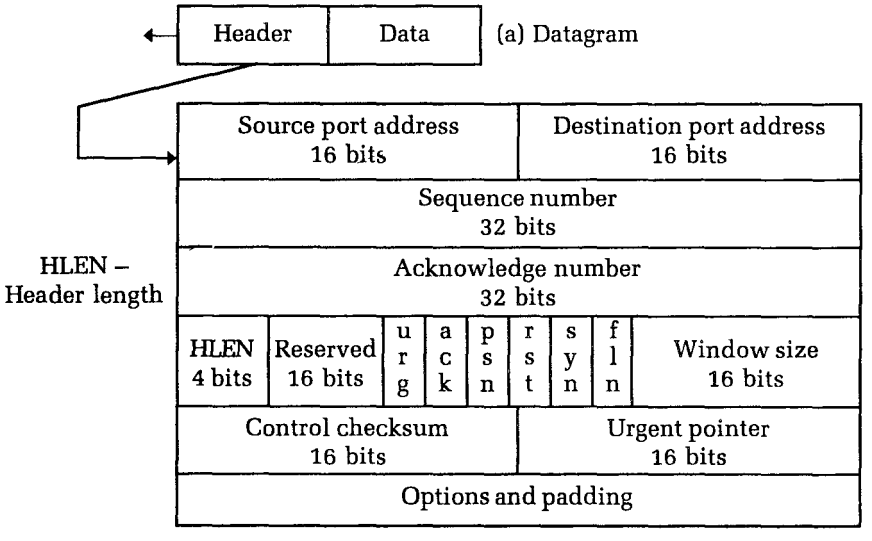


Fig. 23.11 TCP segment

Source port address : Defines the application program in the source computer.

Destination port address : Defines the application program in the destination computer.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Sequence number : Stream of data from the application program divided into two/more TCP segments. Sequence number field shows the position of data in the original data stream.

Acknowledgement number : Used to acknowledge the receipt of data from the other communicating device. The number is valid only if the ACK bit in the control field is set. Here, it defines the byte sequence number that is next expected.

Header length (HLEN) : The field indicates the number of 32 bit (four-byte) words in the TCP header. Four bits can define a number up to 15. This when multipled by 4 gives the total number of bytes in the header. Size of the header can be 60 bytes maximum (4 x15). Minimum size of the header is 20 bytes, 40 bytes are available additional (for options).

Reserved : A field of 6 bits for future use.

Control : Each bit of the six bit control field functions individually/ independently. A bit can either define the use of a segment or serve as a validity check for other fields (i) urgent bit, when set validates the urgent pointer field. Both the bit and the pointer indicate that the data in the segment are urgent (ii) ACK bit validates the acknowledgement number field. Both are used together and have different functions depending on the segment type (iii) The PSH bit – used inform the sender that a higher throughput needed. If possible, data is pushed through paths with higher throughput. (iv) RST bit – Reset bit is used to reset the connection whenever a confusion sets in the sequence numbers (v) SYN bit – used for sequence number synchronisation in three types of segments : connection request, connection confirmation (with the ACK bit set) (vi) FIN bit – used in connection termination in three types of segments : termination request, termination confirmation with the ACK bit set and acknowledgement of termination confirmation (with ACK bit set).

Window size : Defines the size of the sliding window.

Checksum : Used in error detection.

Urgent Pointer : Last required field in the header value is valid only if the URG bit in the control field is set. Here, the sender is informing the receiver that there are urgent data in the data portion of the segment. This pointer defines the end of urgent data and the start of normal data.

Options and Padding : Remainder of the TCP header defines the optional fields; used to convey additional information to the receiver or for alignment purposes.

23.4 APPLICATION LAYER

- The application layer in TCP/IP is equivalent to that of the combined
  - Session
  - Presentation
  - Application layers of the OSI model.

  Out of the many protocols only few are popular.
- The concept of client/server model is explained for the above level. An application program issues a request for services to a second application

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

program, in the roles of client/server respectively. The requested service is provided, using the *client/server paradigm*.

Fig. 23.12

- Actual users of the Internet are people; people prefer names to numbers. *Domain name system (DNS)* identifies each host on the Internet with a unique name that identifies it as unambiguously as its IP address. With the help of the domain name, a program can obtain the IP address associated with it by engaging the service of a name server in a client server session.
- In order to create unique names and make it easy to change and at the same time decentralised, TCP/IP designers have selected a system which is hierarchical in nature and made up of a number of labels separated by dots. Maximum length of the label is 63 characters. A host can have any number of identifying labels with unique names.
- DNS is implemented with a tree wherein each node represents one possible label. The tree is divided into three domains :
  - Generic (organisation domain) – divides registered hosts based on their generic behaviour.
  - Country – uses two character country abbreviations (e.g. US for USA) in place of three characters organisational abbreviation in Generic.
  - Reverse.

Generic domain

Names if read from left to right, starts with the most specific information (about the host) and moves more and more general with each label until they reach the rightmost label (here it describes the broadest affiliation of the host) First level of the generic domain convention have seven possible three - character labels describing organisation type.

com. Commercial organisation	mil. Military group
edu. Educational institution	net. Network support center
gov. Government institution	org. Organisations other than the above
int. International organisation	

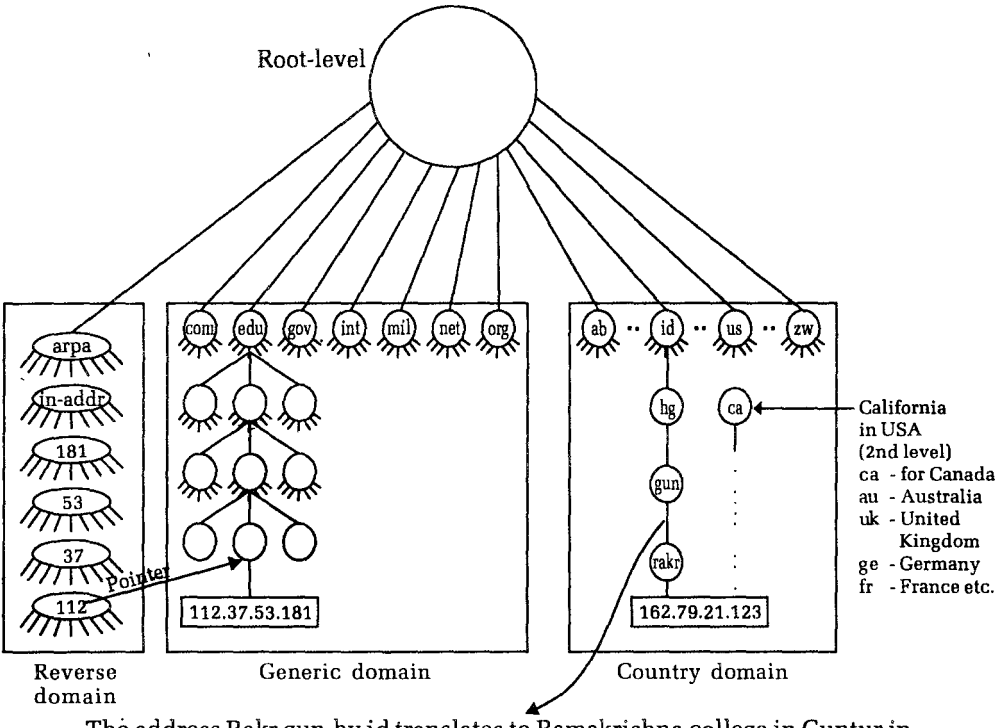
Each domain name has a particular IP address. To find this address, the resolution application searches with the first level label (organisation) If match is found or fits with label a pointer leads to the next level and finally to the associated IP address.

Country domain

Here second level labels can be organisational or specific national destinations. United States uses abbreviations for the states as a sub division of US (e.g. ca.us) California.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.



The address Rakr.gun.hy.id translates to Ramakrishna college in Guntur in Hyderabad in India.

Fig. 23.12

To use the reverse domain, if we have the IP address but need the domain name, use the reverse domain functions of the DNS. If we give the server, the IP address eg. 112.37.53.181 it adds in addr.arpa to the end. So it becomes 112.37.53.181 in addr.arpa. The system then starts from the top of the tree (arpa) and searches until it finds the number. If the number is found, a pointer leads it to the associated domain name.

Many international networks structure their addresses in much the same way as the US does e.g. UK uses AC to indicate academic institutions, co to indicate commercial organisations (an address henry@xyz.ac.uk would indicate a person at a British University)

TELNET

- Second important application could be mentioned as TELNET where TCP/IP's client-server process for remote login. Remote login allows a user at one site to have access to computer at another site. But issues of security would be there. TELENT protects the server against unlawful access by requiring would be users to supply login and password identifiers.
- To use TELNET, a user invokes a TELNET first at his own site.
- He establishes a connection with a TELNET server at the remote site.
- TELENT relays, the keystrokes from the user's keyboard to the remote computer back to the user's screen.
- Here users hardware would be communicating with software in the remote server.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Internet enables users on one computer to login to another computer on the internet. The command to do this is known as *TELNET*. Once the connection is obtained from the TELNET you can login to the computer as you would if you had dialed in with a modem. But you should know the account name and password of an authorised user. It can be faster or slower than a modem depending upon the amount of traffic on the Internet.

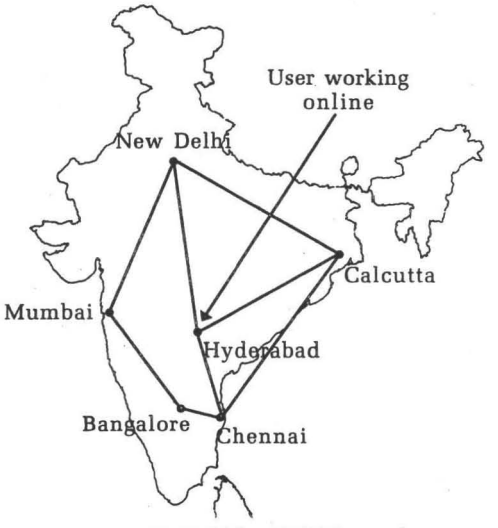


Fig. 23.13 Using TELNET to login

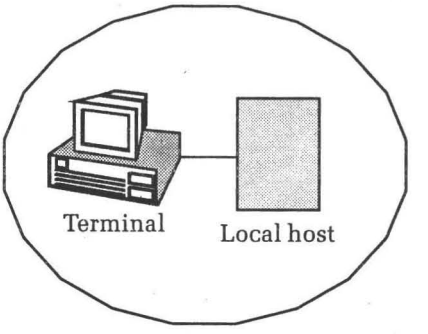


Fig. 23.14 Using TELNET to login

Telnet is light useful, it poses a great security threat; Anyone on Internet can attempt to login to your personal account and use it as and when they use; security precaution is to prohibit remote logins via telnet unless a user specifically asks for his/her account to be authorised for it.

Virtual terminals (VT)

TELNET provides translation services between two machines to provide homogeneity between the user and remote server. TELNET working involves following steps.

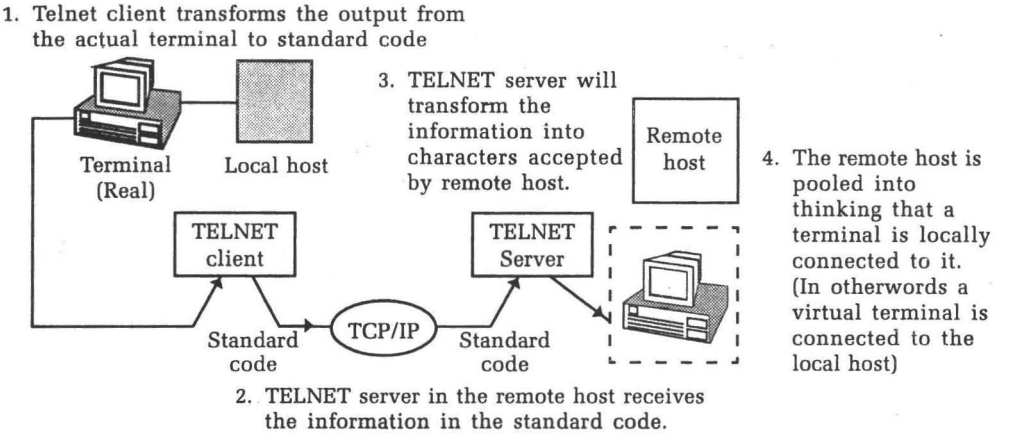


Fig. 23.15 Steps involved in TELNET (Remote login is shown).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

The concept of VT makes a complex process (though not simple, atleast straight forward); It relieves one of the great potential impediments to true universal connectivity; that of connecting multiple incompatible terminals to a single remote server.

File transfer protocol (FTP)

FTP enables anyone to send and receive files over the Internet. Anyone can establish an FTP site, permits anyone on Internet to login and send and receive files.

(i) Closed site – requires users to have permission before they can connect and gain access to the files; Access is granted by providing an account name with a secret password.

(ii) Anonymous site – permits any internet user to login using the account name of anonymous; password is anything you want to type; but most anonymous. FTP sites request that you type your Internet account name (eg. heavy@allstate.org) as the password; This allows them to track who is accessing their files. The process for getting and sending files via FTP is shown in the *technical focus box*.

Many files available via FTP are programs that do various things like data compression, file utilities. Each program is written for a particular type of computer and would not work on any other eg. DOS, Machintosh, UNIX. Many files are compressed to reduce the amount of disc space they need.

Two application programs used to transfer files from a server to a client host are :

(i) *Trivial file transfer protocol (TFTP)* – Simpler one out of the two; intended for applications that do not require complex interaction between client and server; allows a local host to obtain files from a remote host but do not provide security/reliability; With these limitations, TFTP is simpler to use and smaller to store than FTP type; It does not require the reliability of a connection – oriented base protocol such as TCP; instead uses the fundamental packet delivery services offered by UDP.

It includes some basic connection, error detection/transmission features, to ensure that the file requested does indeed arrive.

TFTP is simple, small size and hence specific applications can be encoded into read–only memory, making it useful for hosts that lack the disk capacity to store more elaborate FTPs.

(ii) *File transfer protocol (FTP)* – A standard mechanism for copying a file from one host to other; FTP messages are encapsulated in TCP; These are reliable/ secure; FTP uses TELNET protocol and requires the user to supply login and password identifiers before transferring files.

FTP differs from other client server applications; FTP establishes two connections (virtual circuits) between the hosts; one connection for data transfer, and other for control information.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

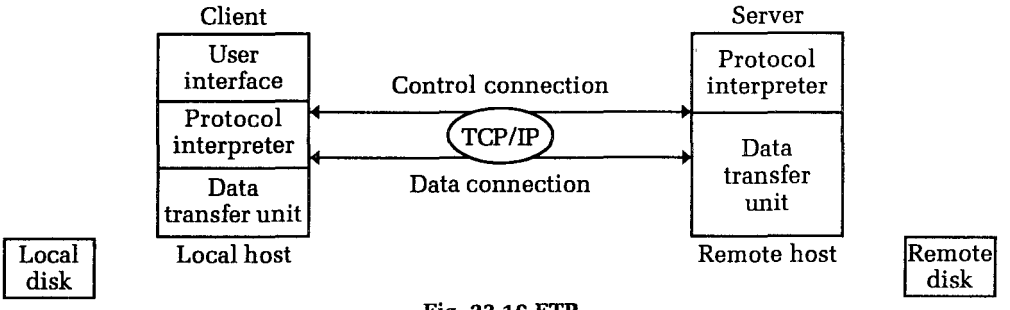


Fig. 23.16 FTP

Control Connection : Used for commands, replies and process updates; uses minimise delay type of service (TOS); remains on for the entire period of the exchange; when data transfer is occuring across the data connection, control connection issues reassurances to the user interface as file transfer beginning, expected duration in minutes, data transfer complete, x bytes transferred successfully.

File access using NFS and RPC

(i) *Network file system (NFS)*

This is a file access protocol. When FTP and TFTP are involved in transfer of entire files from a server to the host (client) a file access service makes file systems on a remote machine visible as though they were on your own machine but without actually transferring the files. NFS allows to edit a file on another machine exactly in a similar way as you would if it were on your own machine. It even allows for the transfer of files from the server to a third host not directly connected to either of you.

(ii) *Remote procedure call (RPC)*

NFS works by invoking the services of a second protocol RPC. The concept of a local procedure call is given below in figure 23.17.

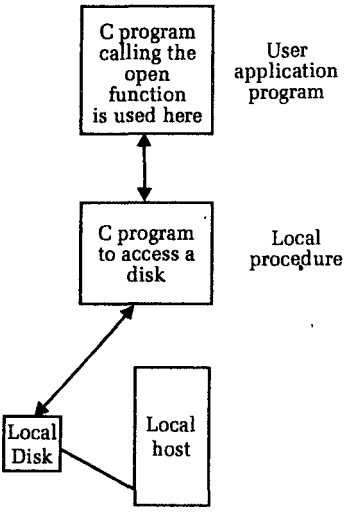


Fig. 23.17 Local procedure call

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

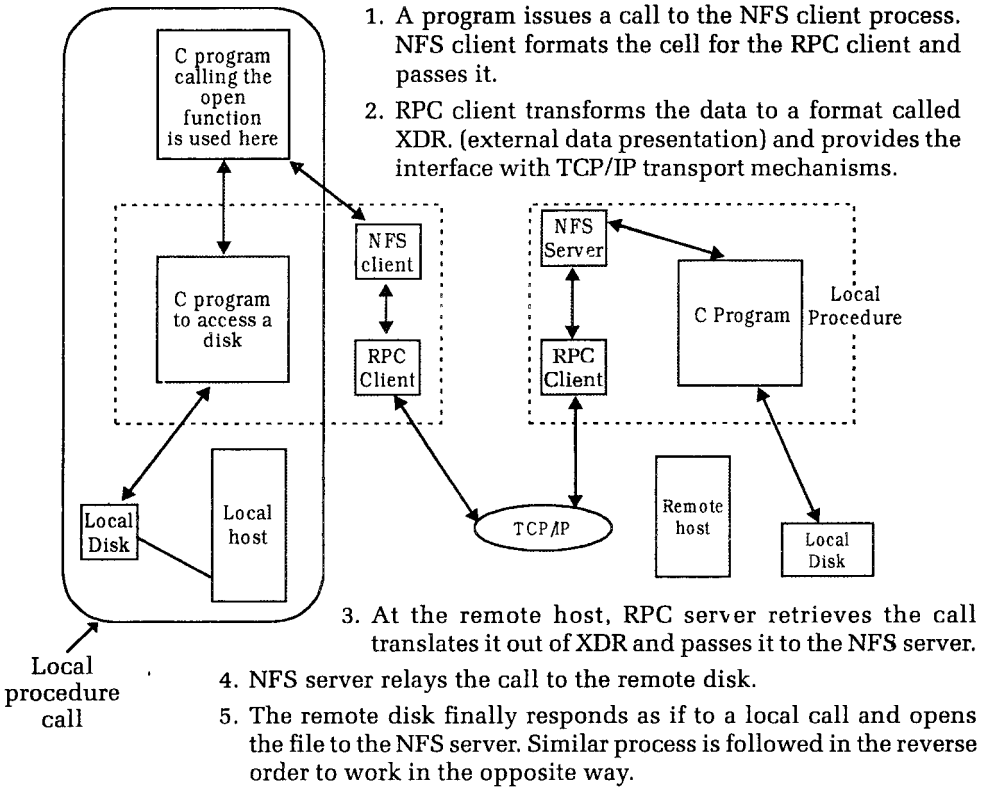


Fig. 23.18 Remote procedure call

RPC transfer the protocol to another machine. Using RPC, Local procedure calls are mapped onto appropriate RPC function calls.

Electronic mail : SMTP (Simple mail transfer protocol)

Most familiar network services is E-mail. It was one of the earliest groupware tools and is also the most heavily used tool. With e-mail,

- Users create and send messages to one user, several users or all users on a distribution list. Messages could be text, voice, video or graphics.
- Packages permit users to attach graphics to their messages; allows to do the same things you do with a regular paper mail.
- Users can file messages in electronic file cabinets, forward copies of messages to other users, send carbon copies of messages, request automatic confirmation of the delivery of the message etc.
- Permits to filter or organise message by priority (e.g. boss's message is given priority)
- Fast (takes seconds or minutes, depending upon the distance to the receiver). Cost is less, because it costs nothing to transmit the message over the network.
- Paper mail is called as snail mail by E-mail users; cheaper in the time invested in preparing the message.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- It can substitute for the telephone (telephone is avoided. The person to be called may not be available); enough communication with less time than a phone call.
- Sending messages calling for a response from a computer program rather than a user.
- Effective for multinational organisations sending messages to users on network outside the Internet.

The TCP/IP protocol that supports electronic mail on the Internet is call *SMTP*.

E-mail

- It is a widely used network service.
- It is a system for sending messages or files to other computer users based on mailback addresses instead of a direct host-to-host exchange.
- It supports mail exchange between users to send anything from short notes to extensive files, without worrying about the current availability of the receiving host.
- It's design echoes the postal system. Addresses will be used to identify both the recipient and sender of a message (return address). Messages not delivered within the specified time are returned to the sender.
- Every user on the network uses a private mail box. Received mail is stored therein until the recipient removes or discards it.
- A mechanism called *spooling* is used which allows a user to send mail even if network is temporarily disconnected or the receiving machine is not in good condition. When a message is sent, a copy is placed in the spool (storage facility). Spool appears like a queue with some fundamental differences. Messages are processed on first come, first-served basis. Messages on a spool is similarly processed on the basis of first come, first searched basis. If the message is in the spool, it is searched every 30 seconds by a client process which runs on the background.

  The background client searches for new messages and not yet sent old messages, and attempts delivery. In the event of client process unable to deliver a message, it puts the message with the time of attempted delivery and leaves it on the spool. It repeats again at a later time. If every time the attempts at delivery fails, the message is considered as undeliverable and after few days it is returned to the mail box of the sender.
- A message is considered delivered only when the client and the server agree that the recipient has seen and disposed of it.
- Till then, copies are kept in both the sending spool and the receiving mail box.

Electronic mail addresses

E mail addresses can be classified into 2 parts :

(i) Local part – Mail box identifying name followed by an@symbol.

(ii) Domain name – destination

E.g. ROPVATS@

Local part	@	Domain name
(Address of the mail box at the local site)		(destination)

The formats may differ at sites using protocols other than TCP/IP.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Aliases

If messages are to be forwarded to more than one recipient at a time by including a number of mailing addresses, it is possible. Frequent messages are sent to the same group of people, this becomes tedious and time wasting. Electronic mailing lists or mailbox groups are provided in certain systems. Here, an e-mail facility (known as mail alias expansion) allows one name (called an alias) to refer to an entirely different name or even to multiple recipients. eg. In a company, the accounting department sends frequent reports to the various managers of all departments as well as to others like Board of directors. In such cases, they can set up an e-mail list under an alias which includes the e-mail addresses of everyone who are supposed to receive reports. When a report is distributed, the sender mentions alias as the recipient and all the above would receive the transmission. One more advantage of the aliases is that the same person can have several mail names (say first and last names, maiden names, married names, nick names etc.) Aliases are stored in a database accessed by an alias expansion program. If a match is found from the mail interface program when it is sent to the alias expander, the existing recipient address is mapped to its official address.

On the contrary, if no match exists, it means no alias exists, or alias is not stored locally.

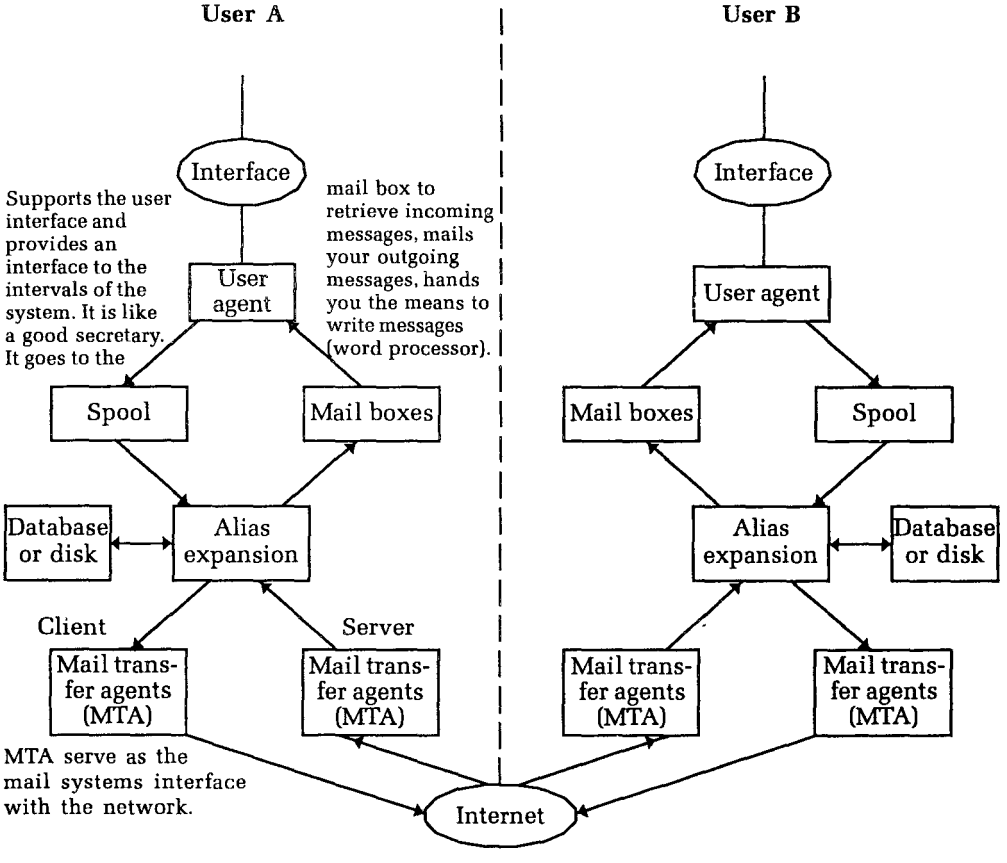


Fig. 23.19 Electronic mail in two directions (sending and receiving)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Simple network management protocol (SNMP)

It provides a set of fundamental operations for :

- Monitoring
- Maintaining an internet.

SNMP was derived from an earlier management protocol known as simple gate way monitoring program, which was again derived from one more protocol called the *high level entry management system (HEMS).* SNMP was developed initially to control and monitor the status of network devices on TCP/IP networks, but it is now available for other network protocols.

Each SNMP device (router, gateway, server) collects information about itself and the messages it processes, and stores the information in a database called the management information base (MIB). The network managers management station that runs the network management application software has access to the MIBs. Using this software, the network manager can send control messages to individual or groups of devices asking them to report the information stored in their MIB.

Management information bases (MIBs) and agents

SNMP uses the concept of manager and managed devices. Every host or a router can be a managed device. Few hosts are managers. Every managed device consists of a combination of hardware and software known as *agent* which acts as a book keeper for the host and accessed by a manager.

Each agent has a database called MIB, inside which has a list of the variables that the protocol supports and tracks. A *variable* is a performance record of an agent (which indicates information like the number of bytes that have been received and gone out of the host over a given time period). Managers can also give variable a value to change or monitor its behaviour. It is also noted that management on TCP/IP internets is accomplished by setting and checking the variables.

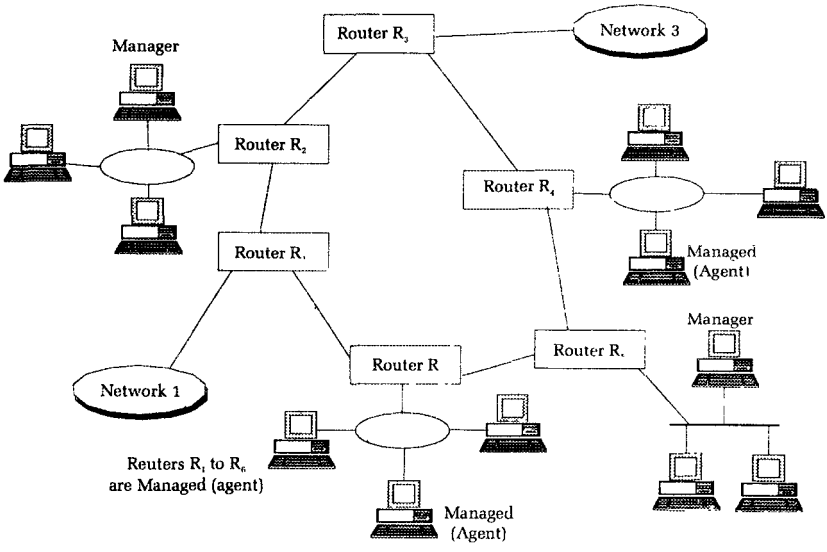


Fig. 23.20 SNMP

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

SNMP is a simple request/response protocol based on UDP. Hence no security is found. Little reliability exists. Most monitoring and maintenance is done using single datagrams. It is felt that level of reliability available through UDP is sufficient. But the lack of security gives more problems. Another version SNMP v2 was introduced. Though it provided with security, it is considered more difficult to implement, though powerful compared to SNMP.

The major methods of accessing computers and locating the files you need are Gophers, Archie, Veronica, WAIS.

Gopher

This was developed at the University of Minnesota (home of the Golden Gophers). It is a client-server and menu driven application program using multiple servers, can navigate through the internet and find a document. It hides computer boundaries completely, and makes information on a large set of computers.

Gophers are a character oriented approach tool for locating data on the Internet that enables the users to locate essentially all textual information stored on Internet servers through a series of easy to use hierarchical menus. It has thousands of Gophers server sites on the Internet throughout the world, with its own system of menus listing subject matter topics, local files and other relevant gophers sites. Each gopher site may contain several thousand listings within its various levels of menus. When the user intitiates the gopher software in search of a specific topic and select a related item from a menu, the server will automatically transfer you to the appropriate file on that server or to the selected server whenever in the world it is located.

Archie

It is a tool for locating data on the Internet that performs keyword searches of an actual databak of document, software and datafiles available for downloading from servers around the world. While no individual archie database can list more than a limited small percentage of the files in the world, checking on a relevant listing from one archie server will take you to another computer system where relevant files are stored. Subjects like Tele-conferencing, optic fiber, inflation etc, resulting in a list of sites contain files on that topic. Several college library universities information can be searched through archie, around the world. Through a file transfer program, files can be downloaded.

It is an automated title-search application program that locates all files having a given name. Most hosts have these databases all over the world. In USA, it is archie, internic.net. This can be accessed through TELNET. Archie (come from Archives) has a data base associating all file names in the Internet with the names of the hosts.

Veronica

It is an automated title- search application program like Archie using a world wide index to computerised archives. It uses gopher services. It searches gopher menus to find a file. Conditional expressions can be used to narrow down the search.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

WAIS – Wide area information service

It is a service for content search to find the name of a file if some information is given about the contents. It is difficult to search the contents of all the files available in the world. Hence the database has been divided into different sources. The user should limit the search to the source required.

It is another way to locate the files around the world. A specific file can be located but it requires the name of database to be searched. With specific database names and key identify words, WAIS searches for the keywords in all the files in those databases.

Internet is so vast it is like an electronic cloud encircling the earth. The numbers one can find vary widely and changes day to day but there are many tens of millions of users located all over the world. The numbers are outdated. It is like looking a rear view mirror. It will be appropriate to say that Internet is larger today compared to yesterday and it will be still large tomorrow than today.

Hyper text transfer protocol (HTTP)

- It is an advanced file retrieving application program which can be used for accessing distributed and linked documents on the worldwide web. This can access:
  - Linked textual documents (hyper text)
  - Linked documents containing images, graphics and sounds (hyper media)

  Some useful web addresses examples are :

  http://www.cern.ch – CERN's home page

  http://www yahoo.com – Yahoo, a list of "interesting" pages

  http://www.cs.colarado.edu/home/mcbryan/wwww.html – A web crawler

  http://www.biotech.washington.edu/webcrawler/webquery.html – A web crawler

All web addresses begin with seven characters : http://. These file files/ pages (where web server stores information in a series of text files) use a structured language called HTML (Hypertext markup language) Messages in HTTP have two broad categories : (i) request (ii) response

request command	— sent from client to the server.
response command	— sent from server to the client.
get-request command	— to retrieve information from the server.
head-request command	— used by the client to receive only header information but not data.
post-request command	— sent by the client to the server for passing information to the receiver (for sending mails, news, bulletin boards and so on)

23.5 WORLD WIDE WEB

www is a repository of information spread all over the world and linked together.

www uses the concept of hypertext. In this environment, information is stored in a set of documents. Concept of pointers are used to link the documents

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

together. An item could be associated with another document using the pointers. Reader who browses through a document can move to other documents by clicking the items that are linked to other documents. A hypertext on the web is known as a *page* and the main page for an organisation/an individual is called as a *home page*. Information on any subject can be :

- Undistributed – whole information may consists of one or more web pages on the same server.
- Distributed – Information made up of many pages distributed on different servers.

World wide web (or web or www. or w3)

It is another information retrieval tool. The web is attractively easy to use, and lends itself to publishing or providing information, to anyone interested. Its popularity has increased dramatically, because of easy to use, colourful and rich in content. *Web* is a series of interconnected documents stored on computer sites. If you use your computer and a software program (browser) to visit a site on the web, the screen displays a document called a *home page*. Home page gives the name of the organisation or individual sponsoring the web site and displays a list of highlighted words, buttons or pictures. It is the text and graphical screen display that welcomes the user and explains the organisation that has established the page. This will lead to other pages, with all the pages of company being known as a *web site*. For a corporation to establish a presence on the web, therefore, it must set up a web site of its one or more pages. The *web* is a network of billions of interlinked documents. These links called *hyper-links* or links which are the highlighted words, buttons, icons or picture. Each link contains the address of another document on the same computer or another computer any where in the world; from this one can jump to the linked pages by clicking one of these links. Clicking them plays videos, music, 3D animations or takes you through a virtual reality experience.

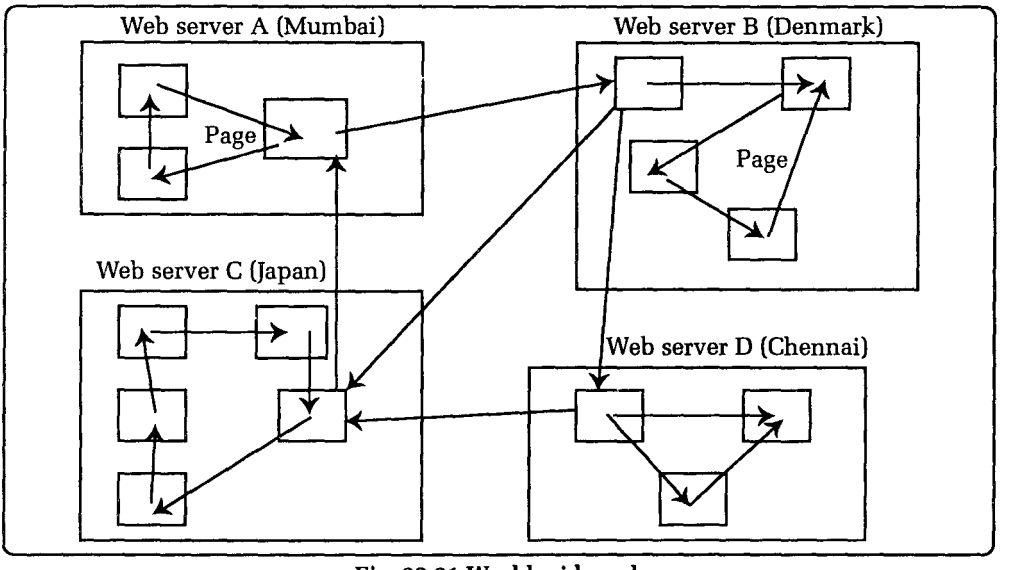


Fig. 23.21 World wide web

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

It is a set of standards for:

- Storing
- Retrieving
- Formatting
- Displaying

information using a client/server architecture, graphical users interfaces (GUI) and a hyper text language that enable dynamic links to other documents. It is one of the most executing Internet services. Worldwide Web (WWW) has tens of thousands of web servers that provide service almost on the idea of a hypertext. *A page* in hypertext may contain links that point to other documents or to other spots in the same document. When users click on a link with the mouse, they jump to other documents/other spots in the same document. Users can navigate the web easily, pushing their interests.

One of the main functions of Internet is easy to use offerings of information and products. This function is provided by the World Wide Web at the heart of the recent explosion in the business use of the Net. This is based on an hyper-text language called *Hypertext mark up language (HTML)* that formats documents and incorporate dynamic links to other documents and pictures stored in the same or remote computers.

World wide web and Internet are not the same though people think they are the same. The Internet is the network itself and many activities other than the world wide web will be done on it. The services like E-mail, Gopher, Usenet news groups are available separately, and access to them has been integrated into the world wide web. While the other methods of locating information on the net are namely text based, the web pages have made an impact by combining text, hypermedia, graphics and sound. Through use of web, commercial enterprises are providing information on demand (say customer support, marketing and sales). The specific hypermedia technology used in the web in known as *hyper links*. Navigating (or surfing) the web requires a graphics computer to the Internet and a web brower. The user must also have a special software tool to navigate the web known as a *web browser*. A popular web browser is *Mosaic*, developed by the National centre for super computing applications. There is another web browser known as *Travel web*, a web site that gives complete details of electronic information on 16 resort hotels in the USA and the Caribbean and similar information on 87 non-resort hotels in North America. Prospective travellers can use Travel web any time to find out information on hotel details, sight seeing attractions related to USA and Caribbean. The world wide web needs:

- A functional architecture
- A structural Architecture
- A navigational architecture

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

A functional architecture is as shown below:

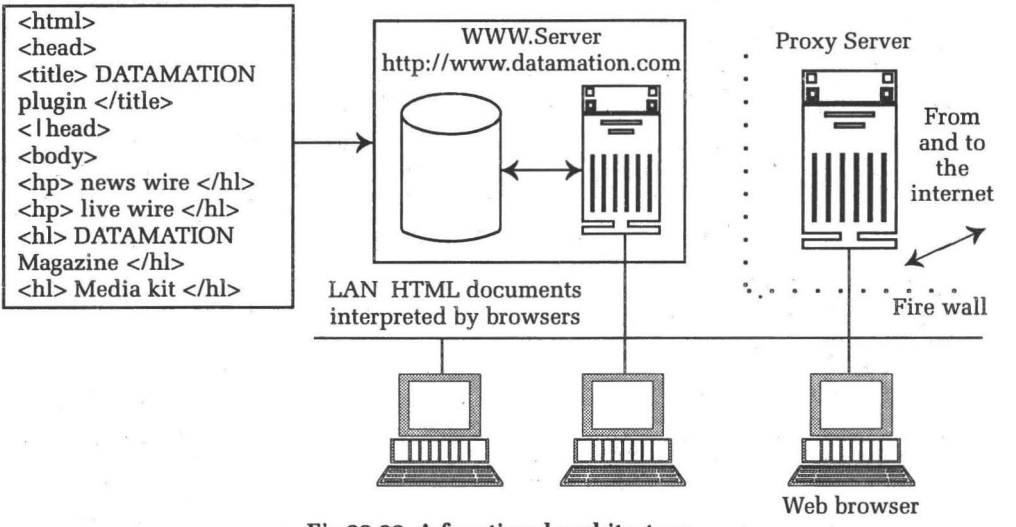


Fig 23.22 A functional architecture

A structural architecture is as under:

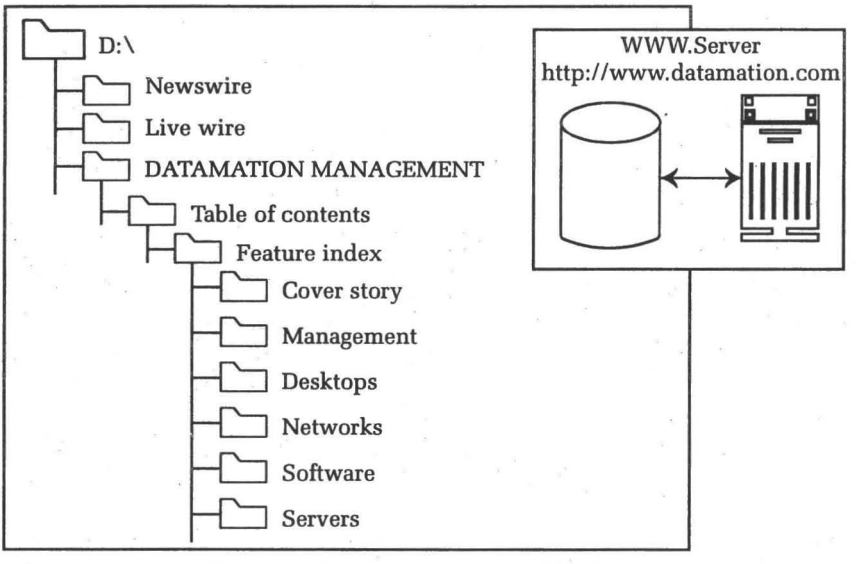


Fig. 23.23 A structural architecture

Uniform resource locator (URL) method ://Host/path

- A client needs an address if he wants to access a web page. WWW uses the concept of locators, to facilitate the access of documents distributed all over the world.
- URL is a standard to specify any kind of information on the Internet. It defines:
  - Method (a protocol used to retrieve the document. The different types of protocols that can retrieve a document are gopher, FTP, HTTP, news and TELNET).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

– Host (a computer where the information is located. Webpages are usually stored in this given alias names that usually begin with w.w.w)

– Path (a path name of a file where the information is located. The path can contain slashes that separate directories from sub directories and files in the UNIX operating system) E.g. URL is http:/ www.datamation.com

Browser architecture

- Many commercial browsers exist.
- These interpret and display a web document. Each of these use the same architecture.
- Browser has three parts (i) Controller (ii) Client programs (iii) Interpreters
  - Controller gets input from the keyboard or mouse; uses the client program to access the document.
  - After the document is accessed, controller uses one of the interpreters to display the document on the screen.
  - Client program is one of the methods (protocols) such as HTTP, FTP, gopher or TELNET.
  - Interpreters are HTML, CGI or Java.

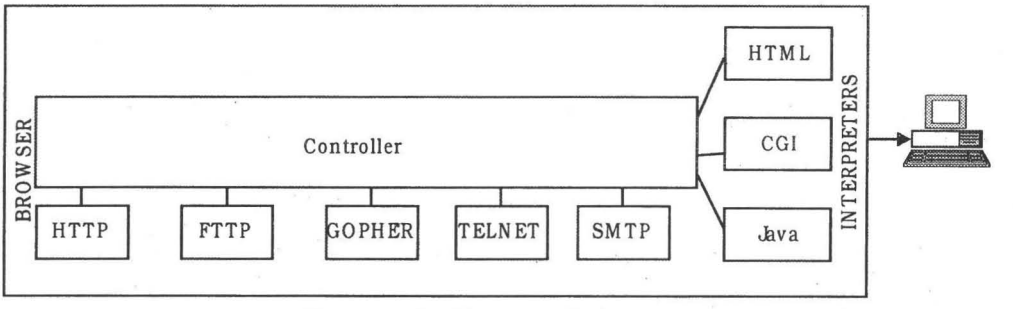


Fig. 23.24 Architecture of a browser

Web documents are grouped into :

(i) Static (HTML) (ii) Dynamic (CGI) (iii) Active (Java)

Static documents :

- As the name itself is static – fixed content documents are created and stored in a server.
- Client accesses the document, a copy of the document is received.
- User can use a browsing program to display the document.
- User cannot change the contents; but the contents can be changed in the server.

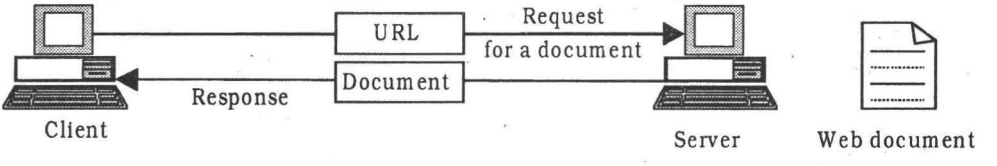


Fig. 23.24 Static Documents

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Dynamic documents

- These do not exist in a predefined format.
- Documents are created by a web server when a browser requests the document.
- When the request arrives, the web server runs an application program to create the dynamic document.
- Server then returns the output in response to the browsers request for document.
- Contents of document varies as these are created for each request (getting the time & date from the server). Time and date are types of information which are dynamic. These change moment to moment.
- Client can request that the server run a program in UNIX and send the result back.

Steps :

1. Client requests for running a program.
2. Run the program create document.
3. Respond.

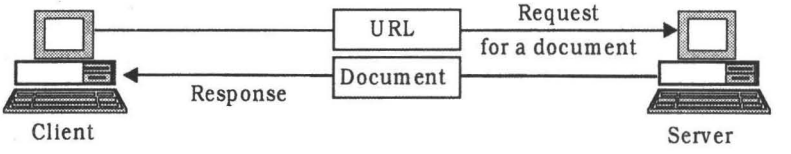


Fig. 23.25 Dynamic documents.

Active documents

- Dynamic documents are produced when requested; produced at the server site; not at the client site; but occasions are there to get a copy by running the program at client site. eg. animated graphics (here the program is to be run by creating, compiling and storing at the server site. If the client needs, a copy is requested.
- A copy of the program (in binary form) is sent to the client. The interpreter at the client site is responsible for running the program.

Steps :

1. Client requests for a copy of the program
2. Copy of the program is sent by server.
3. Running the program and creating the document at the clients' end.

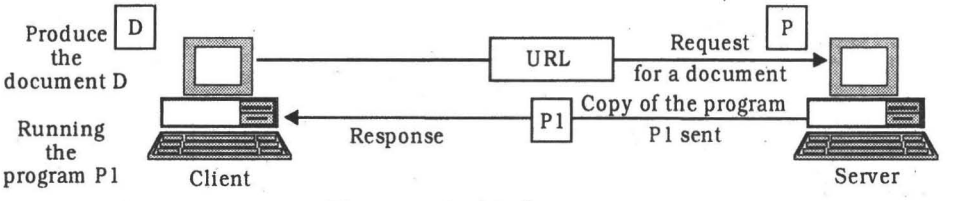
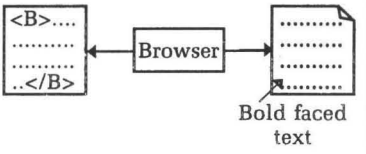


Fig. 23.26 Active document.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Hyper text markup language HTML (Static document)	Common Gateway Interface CGI (Dynamic document)	JAVA (Active document)
• A markup language for writing web pages (Mark up language means it lets the browsers format the web pages). Idea from book publishing industry. E.g. To make a part of the text to be displayed bold face, boldface markup tag must be included in the beginning and at the end. B tag is shown below.  **Fig. 23.27 Effect of <B> tags** • HTML allows us to embed formatting instructions in the file itself; instructions stored with the text; Browser can read and format the text. • Different word processors use different techniques/procedures for formatting the text. Hence formatting capabilities of word processor not utilised to create the text. E.g. IBM computer with Machintosh computer have different formatting procedures not able to receive the web page without HTML. • HTML lets us use only ASCII characters for both the main text and the formatting instructions. Computers can receive ASCII document; Main text used as data. Formatting instructions can be used by the browser to format the data.	• Standard for building dynamic web documents. • It is a model, defines the type of language to be used in preparing the document. • Most of the CGI programs today have been created using shell scripts in UNIX. • Browser in the client machine does not have to know anything about running the script. The script is run at the server site.	• JAVA was incorporated by Sun Microsystems. • They used a language called Java. • Three components of Java are programming language, runtime environment and a class library. • Programming language is used to create programs at the server site. It is an object oriented language with many similarities to C++. • Runtime environment is used at the client site to run the program in binary form. • Class library is a collection of predefined objects to make object oriented programming easier. • Java uses the term *applet to* define an *active document program*. It distinguishes active programs from regular programs.

POINTS TO REMEMBER

- TCP/IP is the oldest networking standard developed for the ARPANET in 1970s. It is a set of protocols or a protocol suite to known how all transactions are exchanged across the Internet. It was developed originally for the US department of defenses' advanced research agency project network.
- TCP/IP is a five layer protocol suite. It matches almost all the OSI model layers closely. Bottom four layers match with the OSI model bottom four layers. Top three OSI layers combined together as an application layer matches with that of TCP/IP's fifth layer (highest layer).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Internet work protocol (IP) is defined at the network layer. It is the transmission mechanism. It is unreliable and connectionless datagram protocol.
- IP transports data in packets called as datagrams, consists of a variable header and a variable data field.
- An internet address specifies both the network and host addresses (host belongs either netid or hostid). It is also known as IP address uniquely defines the connection of a host to its network. A multihomed host means a host more than one IP address.
- The various class types are A, B, C, D or E. Netid – Network identification number and hostid – host address. If host.id is zero, the entire physical network is referred.
- Address resolution protocol (ARP) is used to connect an IP address with the physical address. Reverse address resolution protocol (RARP) allows a host to discover its internet addresses only when it knows its physical address. The internet control message protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems to the sender. It handles control and error messages in the IP layer.
- Two protocols at the transport layer are : User datagram protocol (UDP) and transmission control protocol (TCP). UDP is user datagram protocol. It is unreliable and connectionless; connection is port to port; UDP packet is a user datagram.
- A protocol port is a source or destination point of executing program in the application layer. It is a destination point for storing data to be used by a particular process.
- TCP on the other hand is connection oriented. It is a reliable stream transport port to port protocol. Here the packet is called a *segment*.
- In a client server system, an application program (the client) requests services from the servers side application program.
- DNS is the domain name system devised to provide user friendly names for hosts. IP address can be found out with the domain name.
- TELNET is a remote login application. It allows a user at one site to have access to computer to another site. TELNET provides translation services between two machines to provide homogeneity between the user and remote server.
- File transfer protocol (FTP) enables anyone to send and receive files over the Internet. Two applications programs used to transfer files from a server to a client host are (i) Trivial file transfer protocol (TFTP) and (ii) File transfer protocol (FTP).
- TFTP is simpler than FTP. It is intended for applications that do not require complex interaction between client and server.
- File access is done using NFS and RPC. Network file system (NFS) is an application available on TCP/IP. NFS works by invoking the services of a second protocol RPC (Remote procedure call).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Simple mail transfer protocol (SMTP) is the electronic mail application available on TCP/IP. It provides alias capabilities and a spool based on the firstname, first searched concept.
- Simple network management protocol (SNMP) is an application on TCP/IP used to monitor and manage hosts on a network. An SNMP manager checks variable values on a managed host. It uses the concept of manager and managed devices. It is a simple request/response protocol based on UDP.
- The major methods of accessing computers and locating the files you need are Gophers, Archie, Veronica, WAIS. Gopher is a client server and menu driven application. Archie is an automated title search application programe. Veronica is also similar to Archie using a worldwide index to computerised archives. It searches gopher menus to find a file.
- WAIS – wide area information service is an application program that searches file contents for keywords. It returns the file names of successful finds.
- Hypertext transfer protocol (HTTP) is an advanced file retrieving application program which can be used for accessing distributed an linked documents on the world wide web.
- World wide web (www) is a repository of information, spread all over the world, linked together. Hyper text and hypermedia are the documents linked to each other through the concept of pointers.
- Uniform resource locator (URL) is a standard to specify any kind of information on the Internet. It defines host, method, path.
- Browsers interpret and display a web document. Web documents are grouped into static, dynamic and active documents. A dynamic document is created by a server at a browser request.
- Hypertext markup language (HTML) is used to create static web pages. CGI is a common gateway interface is a standard building dynamic web document.
- An active document is a copy of program retrieved by the client and run at the client site.
- Java is an active language that enables the running of an active document.

QUESTIONS

1. What is TCP/IP ? What are its functions?
2. Which are the layers of OSI model with which TCP/IP layers match ? Compare and contrast.
3. What is encapsulation?
4. What is IP? Explain an IP datagram with a sketch.
5. What are the different class types? Explain each of them.
6. What do you mean by ARP and RARP? Compare and contrast.
7. What is ICMP? Explain.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

8. Define the terms reliable and connection oriented as applicable to data communications and relate the same to TCP?
9. Explain Generic domain, Reverse domain and Country domain. How these three domains are put in the tree? Illustrate this with a sketch.
10. What are the advantages of using a UDP in place of TCP?
11. Explain and give reasons for the two connections between client and server that are needed in FTP.
12. Explain why domain name is reversed while searching for the IP address.
13. What are virtual terminals? Explain.
14. What is remote login? Explain with a sketch how TELNET is used to login?
15. Explain the two application programs found to transfer files from server to a client host?
16. Explain how the files are accessed using NFS and RPC?
17. What is electronic mail. Explain its advantages.
18. What is Alias? Explain the terms SNMP and SMTP.
19. What is MIB? Explain.
20. Which are the methods of accessing computers and locating files? Explain each of them briefly.
21. What is Hypertext transfer protocol? Explain.
22. Explain worldwide web, uniform resource locator and browser architecture.
23. What are the different web documents? Explain each one of them in brief.
24. Compare and contrast HTML, CGI and Java.

FILL IN THE BLANKS

1. TCP/IP's application layer corresponds to _____ layers of OSI.
2. IP address has ____ bits long.
3. _____ contains destination and source point address.
4. The data unit in the TCP/IP, IP layer is called a _____ _____.
5. _____ file transfer protocol uses UDP.
6. _____ application allows a user to access and change remote files without actual transfer.
7. TFTP is _____ _____ _____ _____.
8. RARP is _____ _____ _____ _____.
9. MIB is _____ _____ _____.
10. SNMP is _____ _____ _____ _____.
11. NFS is _____ _____ _____.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

12. WAIS is _____ _____ _____ _____.
13. HTML is _____ _____ _____ _____ .
14. CGI is _____ _____ _____.
15. _____ _____ _____ is ARP.
16. _____ _____ _____ is UDP.
17. Java use the term _____ to define an active document.
18. An applet is _____ document application program.
19. _____ is used to build dynamic web documents.
20. Browser's components are controller, _____ _____ , interpreter.
21. _____ searches the contents of a file for requested information.
22. Conditional expressions in the search field are used in _____ file retrieval method.
23. Shell scripts are used in _____ documents.
24. _____ web document is fixed content and is created and stored at the server site.
25. Hypertext document are linked through _____.
26. _____ TCP/IP protocol monitors and maintain an internet.
27. Transport layer protocols need _____ and _____ port address fields.
28. _____ transport layer protocol is connectionless and _____ transport layer protocol needs acknowledgement.
29. _____ application allows a user to login to a remote computer.
30. In DNS, first level classification in the _____ domain is base on the organisation type of the host's network.
31. _____ uses TCP and establishes two virtual circuits between the local and remote server.
32. The data unit which used UDP and from the transport layer is called a ____ _____.
33. Class A of Internet address ranges from ___.0.0.0 to ___.255.255.255.
34. Class B of Internet address ranges from ___.0.0.0 to ___.255.255.255.
35. Class C of Internet address ranges from ___.0.0.0 to ___.255.255.255.
36. Class D of Internet address ranges from ___.0.0.0 to ___.255.255.255.
37. Class E of Internet address ranges from ___.0.0.0 to ___.255.255.255.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

38. Class E Internet addresses are known as _____ where as class D are _____; class A, B, C are Netid and Hostid.
39. RPC and TCP/IP are involved in _____.
40. Purpose of ARP on a network is to find the _____ address given in the _____ address.

Answers

1. all
2. 32
3. UDP
4. datagram
5. Trivial
6. NFS
7. Trival file transfer protocol
8. reverse address resolution protocol
9. management information bases
10. simple network management protocol
11. network file system
12. wide area information server
13. hyper text markup language
14. common gateway interface
15. Address resolution protocol
16. User datagram protocol.
17. applet
18. active
19. CGI
20. client program
21. WAIS
22. veronica
23. dynamic
24. Static
25. pointers
26. SNMP
27. source ; destination
28. UDP ; TCP
29. TELNET
30. generic
31. FTP
32. user datagram
33. 0 ; 127
34. 128 ; 191
35. 192 ; 223
36. 224 ; 239
37. 240 ; 247
38. undefined ; hostid
39. NFS
40. station ; Internet

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

24

EMERGING TECHNOLOGIES COMPUTER TELEPHONY AND IP TELEPHONY

24.1 IP TELEPHONY FINDS ITS VOICE

IP has become the protocol of choice for data. Now it is being used for voice communications, making it easier than ever to reach out and touch someone. Quite a bit of attention is being paid to IP telephony these days. After all, not since the 1984 breakups of AT&T, has the telecommunications industry been so shaken up. In the early 1980s we had to get used to the Baby Bells providing phone service. Now, in the late 1990s, we're about to start receiving our services from ISPs.

Unbelievable as it may sound, voice traffic and the Internet have been introduced to each other, and they seem to be getting along quite well. "IP telephony", an umbrella term that refers to voice over IP, also includes other technologies such as fax and multimedia over IP. The technology is taking off largely because of its potential to save companies thousands of dollars on long distance phone calls.

However, end-user organizations are not the only ones that stand to benefit. Telcos and ISPs are hoping to offer the technology as a value-added service, while vendors of IP telephony products are positioning themselves to take advantage of the imminent market surge.

Far from a novelty or flash in the pan, IP telephony is expected to become a US$1.81 billion market by 2001, according to "World Internet Telephony Product Markets", a report published by the market research firm Frost & Sullivan in late 1997.

Pulver.com, an IP telephony consultancy based in Great Neck, Newyork, predicts that sales to home PC users will drop, while sales to the enterprise and telco markets will mushroom (See Table 24.1).

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

For a market that's only recently hit its stride, particularly among corporate users, this growth is quite remarkable.

	Hobbyists	Enterprise	Telcos
1995	94 per cent	2 per cent	4 per cent
1996	90 per cent	3 per cent	7 per cent
1997	75 per cent	5 per cent	2 per cent
1998	55 per cent	1 per cent	35 per cent
1999	45 per cent	15 per cent	40 per cent

Table 24.1 The IP telephony market

(Source : Pulver.com)

Person-to-person call

IP telephony made a smashing debut in early 1995, when VocalTec, which has offices in Herzliya, Israel, and Northvale, U.S, introduced its Internet phone client. Although the company didn't invent the concept of voice over IP, it was the first to commercialise and market it successfully.

Before VocalTec, those who wanted to put voice traffic over IP had to cobble together their own solutions. VocalTec's first product allowed two PCs on a LAN to talk to each other. It was found that there was a demand for the same product but over the wide area network, and so Vocal Tec developed a product for the Internet.

With client software such as Internet Phone, a user with a multimedia PC can place phone calls over the Internet to another user with a multimedia PC. To make a call, a user establishes a connection with his ISP, launches the Internet Phone client software, then looks through a list of other users who are also online and using the software, and then makes the call.

While Internet Phone was something of an IP telephony breakthrough, it had its fair share of drawbacks. For example, because most users, especially those using the software at home, do not have permanent Ip addresses, they are dynamically assigned an address each time they log in. This factor can make locating people on the other end of a call difficult.

Also, for PC-to-PC communications to take place, both computers must be on and running IP telephony software, which likely means a call has to be arranged in advance. Additionally, early versions of the software supported half-duplex transmissions, making calls sound like CB-type conversations. Even when later versions of the software supported full-duplex voice, quality remained well below that which could be enjoyed through the phone company.

In addition, IP telephony software wasn't interoperable, which meant that you and your friends and family had to have the same product to communicate with one another.

Given these caveats, IP telephony was more a novelty that allowed you to call relatives overseas than a technology that could save a business serious money. To circumvent the need for every IP phone call participant to have a multimedia PC and to bring the technology to the business mainstream, vendors realised

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

they needed to leverage the existing Public Switched Telephone Network (PSTN) and cooperate with the telcos.

Bridging the gap

Top overcome the limitations of PC-to-PC telephony, companies in IP telephony began developing products called gateways, which allow users, regardless of whether they have a PC or just a plain old telephone, to place voice calls over the Internet. The first gateway products began shipping in late 1996.

"Gateways make sure you can talk to anybody regardless of their [equipment's] level of sophistication," says Ravi Gururaj, Internet project program manager at Dialogic, Singapore. "You need to be able to make a call from any enterprise phone to any other phone device, either a PC or a phone. And, regardless of the sophistication of the destination device, you need to be able to reach it. It's no good if I have a phone hooked up to my laptop but no one can reach me", he adds.

Gateways are being positioned as the great equaliser in the world of IP telephony. Now, you don't need a beefed-up multimedia PC with sound card, speakers, and a microphone to place or answer a call coming over the Internet. Rather, a gateway bridges the distance between the packet-based Internet and the traditional circuit switched telephone infrastructure. (See figure 24.1)

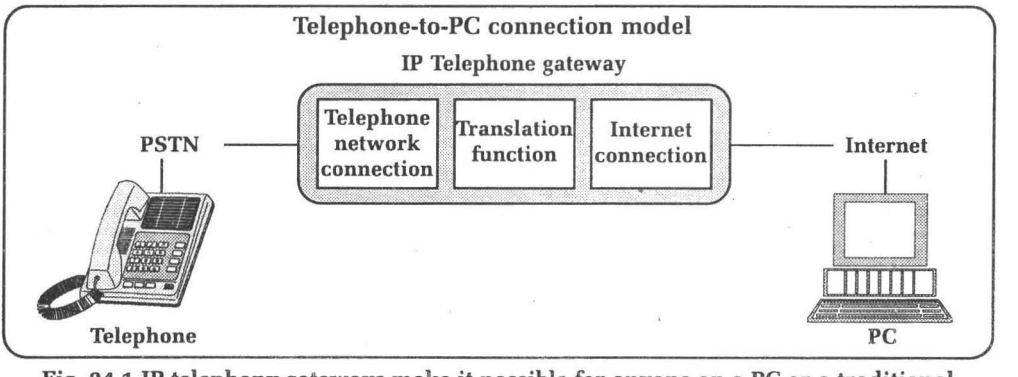


Fig. 24.1 IP telephony gateways make it possible for anyone on a PC or a traditional phone to use the Internet to place voice calls. The gateways digitise voice signals, compress them and packetise them for transmission over IP.

(Source : Dialogic)

Gateways connect to the PSTN on one side of a call and to the Internet on the other side. In a phone-to-PC call scenario, a phone signal travels over the PSTN, which also involves the PBX, to the gateway. If the phone signal is analogue, the gateway digitises it, compresses it, and packetises it for transport over IP. The gateway then sends the call directly to the intended PC.

In a phone-to-phone scenario, once a voice signal is packetised, it first goes through the PSTN to an IP telephony gateway near the call sender. Then, the signal goes out over the Internet to a second gateway close to the call receiver; this gateway receives the call and sends it over the PSTN to the intended phone recipient. Traditional voice calls require 64 Kbps of bandwidth, but with compression, IP telephony calls can be transmitted at 8 Kbps to 12 Kbps.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Gateways can run on a variety of platforms, but Windows NT appears to be the top choice for many vendors. Leading vendors such as VocalTec and Clarent both use Microsoft's operating system. As for hardware, VocalTec uses voice processing boards from Dialogic, while Clarent uses boards from Natural Microsystems.

Other IP telephony gateway vendors include Micom, (now part of Nortel Networks) whose V/IP Phone/Fax Ip Gateway can operate on servers or desktop PCs running DOS, Windows 95, or NetWare. Other gateway products, such a s Nuera Communications' Access Plus F200ip, handle voice over both IP and frame relay in a single device.

You can deploy gateways in a variety of locations, including branch offices and call centres, and you can directly connect gateways to PCs or indirectly connect them to phones through the PSTN. (See figure 24.2).

Telephone-to-PC connection model

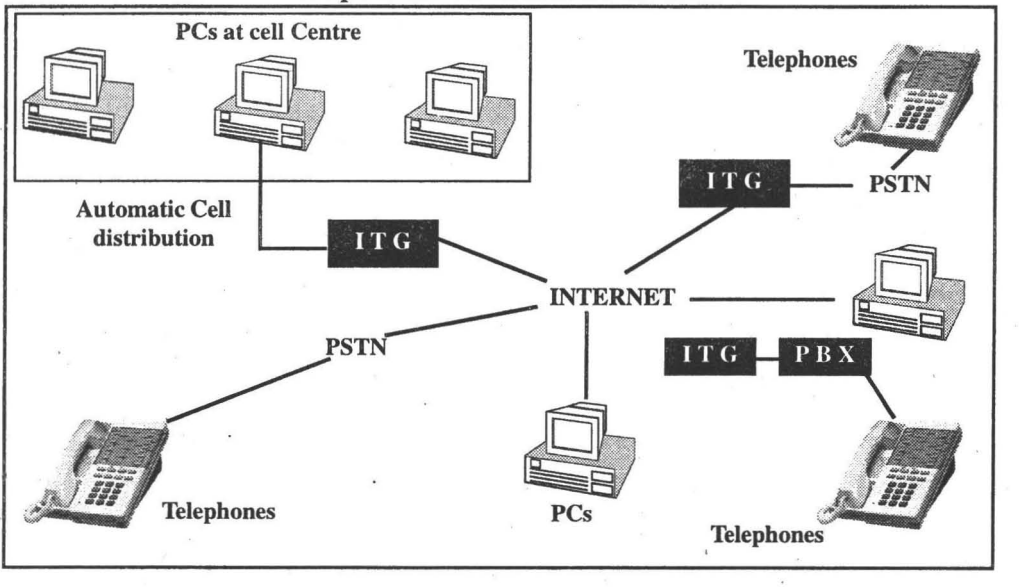


Fig. 24.2 Companies can choose to invest in their own gateways at strategic locations to allow voice to run over IP throughout their organisation, or Internet telephony service providers can run gateways and sell access privileges to customers.

(Source : LAN Magazine, December 1999)

The challenge for vendors now is to ensure interoperability among different products. VocalTec's focus on interoperability is the key to making the market grow faster and to making the technology a viable business application, beleive analysts.

A group of companies founded the Voice over Ip (VolP) forum in early 1996, with the goal of defining a single implementation of VolP to which all products could conform. This effort includes adoption of the ITU's H.323 standard, which defines the transmission of multimedia data over IP. For more on this standard and how it will be used for IP telephony, see the box item.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

In Real time

As you probably know, the Internet, unlike the PSTN, isn't the best medium for real-time communications. Voice packets encounter problems such as heavy traffic and delay when going over IP. To address these potential drawbacks, vendors are ensuring that their products support features that make IP telephony as reliable as the traditional phone system. In addition, customers are taking steps on their end to ensure that voice calls routed over the Internet arrive safely and intact.

When data packets are sent over IP, it doesn't matter whether they get out of order during transport or whether some packets arrive before others. With real time voice traffic, however, packets must be sent in a particular order, and they must remain in that order for the duration of their journey and with as little delay as possible. If voice packets travel through many different routers on the way to their destination, the potential for delay increases.

The greater the delay with voice packets, the less useful the call becomes, Studies have shown that the human ear can tolerate delays of 300ms to 600 ms before the degradation gets too annoying to put up with. "Our view is that 150ms delay is very good quality, and anything less is very good end to end," says Dialogic's Gururaj. "Between 150ms and 300ms, delay is very difficult to detect and may still be tolerable, but at around 300ms the interchange begins to sound like a bad cellular phone call."

The delay can be attributed to the several steps required to prepare and send voice traffic over the Internet. These steps include coding (compression) of the voice signal, transmission over the network, and decoding on the other end. If the voice traffic is travelling over an Internet, you have full control over network delay because you can control the routers and other devices on the network and configure them to your liking.

While reducing delays can improve the quality of voice traffic, providing sufficient bandwidth can ensure that voice packets arrive at their destination. Because IP telephony traffic shares the same space as data traffic, network managers, who by default will most likely be charged with ensuring that the technology works for their companies, will have to be diligent about bandwidth utilisation and traffic prioritisation.

One approach to controlling bandwidth utilisation is to implement protocols such as RSVP, which reserves specific amounts of bandwidth for certain applications. As such, RSVP can be used with IP telephony to ensure that voice traffic gets the bandwidth it needs.

A more costly approach is to upgrade to a high-speed network. With the sky as the limit on bandwidth, companies can send redundant voice packets to compensate for dropped ones. However, while this approach sound like a great idea for safeguarding voice traffic during transit, it defeats the purpose of IP telephony, which can reduce a voice call from 64 Kbps to around 10 Kbps. If you start sending multiple copies of packets over the network, the savings in the amount of bandwidth an IP call consumes become irrelevant.

A more cost-effective approach to the issue of bandwidth utilisation is to prioritise voice traffic. One way to do this is to send voice traffic over UDP instead

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

of TCP. TCP numbers packets in the order they go out and expects the receiving node to acknowledge the arrival of each packet. While this processing overhead is useful for data transmissions, which require integrity, it can degrade the transport of voice transmissions.

UDP, which does not send an acknowledgement for each packet, is more suitable for real-time data such as voice, which requires low latency.

As such, many companies are turning to UDP as the Transport layer protocol of choice, assigning voice packets to UDP ports on routers. Traditionally, UDP traffic has been considered high priority, and because most routers today support this protocol, very little router configuration must be performed. Like TCP, UDP transmits packets in sequence, so it's easy to find out whether any packets were lost during transmission.

You can take other steps to manage voice traffic effectively. For instance, to manage your own gateways, you need to make sure products have a scalable port density. This way, you can go with a T-1 line (24 voice calls) at the main office and perhaps an 8-port solution at branch offices.

You also have to look for high availability, something we take for granted in the phone world. To route voice traffic over an existing network, you need to make sure the network is as reliable as the PBX is today. To get to this point, some companies might have to upgrade their corporate backbone.

Carrier-class service

As you can imagine, the benefits of using the Internet for voice traffic are significant for companies that wish to reduce the exorbitant costs of international long distance calls. However, IP telephony isn't being targeted just at multinational enterprise customers with high phone bills; the technology also stands to benefit carriers, telcos, and even ISPs.

For the most part, only large multinational companies have the time and money required to install IP telephony gateways,, at each office to allow PC-to-phone connectivity. As such, companies that can't invest in gateways or that don't want to deal with the hassles of configuring them, might seem to have few or no options for using the internet for their voice traffic. Fortunately, service providers can pick up this slack. ISPs can install gateways at their POPs, and carriers can install them at central offices to enable their customers to take advantage of the Internet.

A new breed of service providers, the so called Internet Telephony Service Provider (ITSP), is materializing. In August, 1997, VocalTec announced the NextGen Telephonic program, a joint marketing agreement with several ITSPs around the world which include DeltaThree, Biztrancs Technology, PacificNet, NetTel, Halidon, and Access Power.

VocalTec's program allows PC users running the company's Internet Phone 5 (the latest version of VocalTec's IP telephony client software) to dial up one of these ITSPs and use its gateway to contact a regular phone. This service is available in many locations throughout the world, including HongKong, London, Paris, Moscow, TelAviv, Tokyo, Beijing and major cities in the US.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Although this program specifically addresses PC-to-phone connections using VocalTec's software and gateways, individual ITSPs can also provide phone-to-phone service, and they can even use other vendors' gateways, although interoperability is still an issue.

In July 1997, Global Exchange Carrier, a company that provides long distance calling over the Internet, and 11 ISPs announced the creation of the global network for carrying voice over IP. This network includes many countries, such as the US, the UK, Switzerland, Germany, Australia, New Zealand, Japan, Korea and Israel.

ITSPs come from a variety of existing markets, including the ISP, telco, and even cable company arenas. Some companies will spring up to handle only IP telephony services, but many IP telephony vendors are specifically targeting existing service providers.

For instance, Clarent is selling the product to enterprise markets, but a big chunk of its business has been to telcos, inform company officials. The company has been selling to carriers, telcos, and ITSPs; it is even making inroads in countries where only one telco is permitted to operate.

In countries within the Asia/Pacific region, like Koera, Japan, Singapore, HongKong, and Malaysia, governments are starting to deregulate telecommunications, but the cost of international long distance calls is still high. This situation makes these markets prime candidates for IP telephony, especially where companies have lot of international voice traffic among fixed locations. However, for IP telephony to work worldwide, there must be wide acceptance and implementation of gateways in as many areas as possible, which will likely take time.

Big brother and Big business

Telephone companies around the world are either government owned and operated, or they are highly regulated by the government. Because IP telephony encroaches upon traditional telephone territory, it's a potential point of government regulation.

However, vendors seem confident that Big Brother won't make a pest of himself when looking into IP telephony around the world. Industry pundits believe that governments will begin to regulate if a service provider starts to give phone-to-phone service. However, because the medium doesn't matter, phone-to-phone connections using IP should be treated the same as any other phone-to-phone connection.

It would not be possible for the government to regulate PC-to-phone or PC-to-PC calls, however because there is no way to tell who originated the call.

Dialogic's Gururaj thinks IP telephony will be treated the same as Internet service is today. "This technology will grow so fast that companies will want to invest in areas of the world where this might be regulated, but those countries will come under immense pressure not to [regulate]," he says.

Governments around the world might still be up in the air about what to do about IP telephony, but it looks as though big business is not. By purchasing IP telephony gateways or outsourcing the task to ITSPs, companies can expect to receive a return of investment of thousands of dollars a month.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Today, cost is probably the most important factor driving companies to evaluate IP telephony, but in the future, the ability to run multimedia and other services to customers might outweight bottomline savings.

On the telco side, instead of spending millions of dollars in central office infrastructure and maintenance, carriers can spend hundreds of thousands of dollars to deploy and maintain a network of gateways running over IP.

In the future we may see telcos supporting both the traditional PSTN and IP, and consumes may have a choice of different types of services.

Today, IP telephony may just be getting off the ground, but it's real. And with a high calibre of vendors, service providers, and multinational companies backing it, the technology could forever change the way we reach out and touch someone.

24.2 VOICE AND DATA COME IN PACKETS

During the time when wristwatches with numerical displays hit the market in a big way, a lot of people wondered, even argued about whether time had run out for the traditional clock face. At that moment, the numerical display marketed as "digital" appears to be running a distant second to the old clock face, which came to be called "analogue". Both are likely to persist for quite some time – yet something has changed, hasn't it ? Behind the displays, both watches are driven by cheap, robust digital electronics instead of mechanical works.

These days, the buzz about trends in networking swarms with either/or propositions, despite abundant evidence that real choices are seldom that simple. A prime example is the discussion about whether a single packet technology will emerge as the solution for a multitude of needs. The line is usually drawn between the "connectionless" type of packet networking prevalent in LANs and the Internet on one hand and the connection-oriented type standardized as ATM on the other.

The assumption underlying the connectionless versus connection-oriented discussion - that packet technology will supplant circuit switching and transport in most private and public networks - is probably sound, considered on a long enough time scale. Digital technology has progressed steadily from trunks to branches to the leaves of networks, from central systems to all sorts of smart elements and terminals, and from specialized systems and applications to more general ones. The move toward infrastructures based on packet technology for broadband, mixed media networking is less a revolution than another step in this progression.

Just over a decade ago, packet switching and transport technology was at best a dark-horse candidate to carry the kind of traffic entrusted to ultra reliable circuit-switched networks; communications in "real-time" media such as interactive voice and video, carrying high value along with high expectations for quality and availability. Nevertheless, the potential of packet technology – particularly for using bandwidth more efficiently, handling a mix of applications with different bandwidth, and performance requirements, and allowing network infrastructure and applications to evolve independently – was recognized and has been developed aggressively.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Meanwhile, pumped mainly by Internet and intranet growth, the sheer volume of data and mixed-media traffic has surged on both packet and circuit-switched networks. This trend will be amplified by the expansion of high-bit-rate access options and by improved coding and applications for Internet telephony, audio, and video.

But wondering whether packet technology will win out is a bit like focusing on the superficial difference between "digital" and "analogue" watches without regard to the underlying transformation that they have in common. It also underestimates the complexity of providing real-time services in a packet world, and the impact of legacy technology on network evolution. No two network operators or customers are starting in exactly the same place. The coexistence of 1880s and 1980s timepiece styles in 1997 reminds us that even the most inevitable looking trend is shaped by what people have, know, and trust – together with what it's worth to them.

Worlds collide

The sets of standards that originated in data communications and the telecom standards for ATM offer different, almost complementary strengths. Neither will do everything for everybody any time soon, despite recent developments including third-generation ATM products, gigabit-per-second Ethernet and router technology, switching speed, and IPv6, the latest version of the Internet Protocol.

The either/or perspective may be a legacy of the era before the covergence of everything. For many years, the telecom and data worlds were effectively insulated from each other. It hardly mattered that they were so different, with telecom operating like an alliance of stable, conservative republics – in which technological transformations were legislated and implemented in standard ways – while datacom plunged ahead in a rough-and-tumble free-for-all.

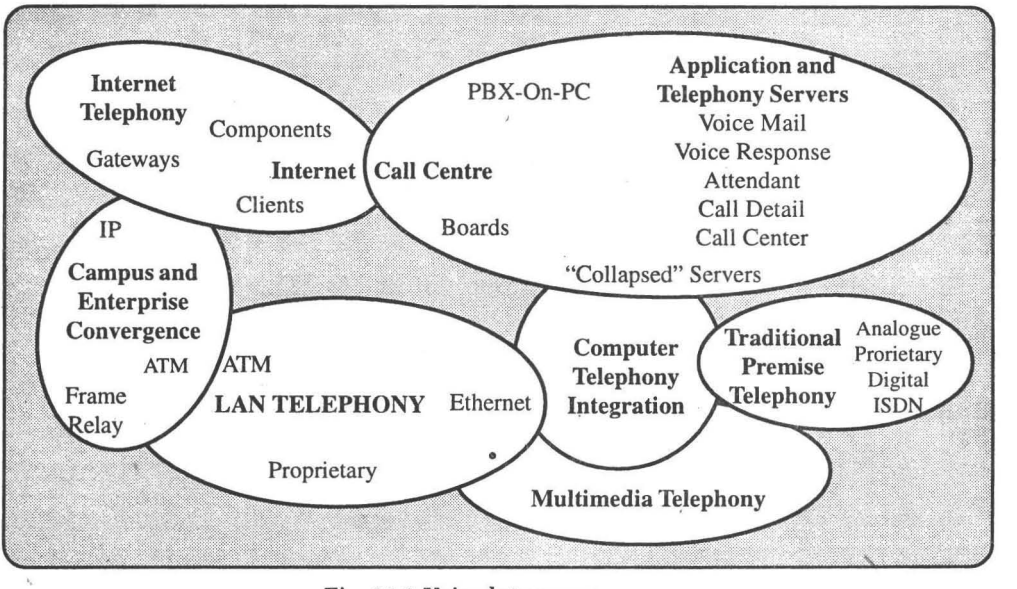


Fig. 24.3 Voicedata convergence

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Now that the stuff of communications has gone completely to bits, the worlds have collided. Phone calls, e-mail, faxes, file transfers, video streams, web pages, medical images, and mixed-media teleconferences are all essentially digital and don't much care whether they traverse, originated in datacom or telecom. The collision has produced a dynamic environment for innovation aimed at giving customers the best of both worlds. It's a good time to keep an open mind.

Remember Elisha Gray. On the verge of inventing the telephone, he set that "scientific toy" aside. Gray's technical expertise, business savvy, and reputation were so wrapped up in the world of telegraphy that he was blind to the possibilities that inspired A.G.Bell, an outsider and relative amateur. Similarly, experts in arc lighting dismissed Thomas Edison and his light bulb, and Edison's resistance to alternating current played out the pattern again.

It's only natural that all parties to the big doings in network evolution – technologists, suppliers, network operators, and end users alike – have more expertise, experience, and investment in technology from one world or the other. But heads up ! The way networking technology is going experts of every stripe should stay alert for insights and innovations from telecom, datacom, and unexpected quarters.

From Voice/Data to tele-immersion

In applications, delivering the best of both worlds means following through on changes taking place now and perhaps establishing applications that have been hailed as "futuristic" for an awfully long time. It may also mean paving the way for unforeseen "killer" applications – like the spreadsheet for the PC and HTML for the Internet – that will spawn industries.

The convergence of voice and data applications on packet networks is under way. It is driven mainly by cost considerations and the promise of flexible, mixed-media communications under customer control; limited mainly by the association of packet telephony with low quality of service and lack of features compared to voice services through private branch exchanges and public telecommunications networks.

On one hand is the compelling prospect of savings to be realized anywhere infrastructures and operations can be consolidated. On the other, is a set of unsolved technical problems in packet telephony – most of which stem either from the relative immaturity of packet voice in terms of service features and management or from the ill effects of excessive queuing and delay variation (jitter) on real-time communications. Delay is an issue as central to packet telephony as was quantisation noise – the error between a continuous waveform like speech and the stream of discrete samples used to represent it digitally – to the development of digital switching and transmission.

The limitations have been significant, but the premise seems inescapable, and the problems appear to be yielding. The trend is toward increasing growth of traffic on packet networks, in both traditional services and mixed media calling.

Voice/data convergence has progressed further in campus and enterprise environments, where intra-company voice traffic is moving from private-line trunks to Frame Relay and ATM WANs. Components and systems based on the

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

H.323 protocol–allowing flexible interactions between voice - and data - oriented networks and terminals - have started to extend packet-voice applications to the business desktop. Call servers can enable interworking between business voice and data networks to give LAN terminals access to typical PBX features.

Distinctions are blurring in more than one way. Consider a catalogue shopping or personal banking application that allows the user to call a representative with a click of the mouse, either carrying on both a voice call and browsing session from that point or toggling between them.

Data or voice ? Suppose the user clicks to talk to a person and is connected to a voice mail system : If she decides to leave a message, does it need to be treated as real-time traffic? On connecting with voicemail, the application could drop the long-distance phone connection, record her voice message, and then forward it to the mail system over the Internet. More and more applications are coming that mix data with voice, audio, and video.

In time, it appears likely that mixed media communications, broader bandwidth, and mobility options will finally move some of the so-called tele-immersive applications out of the labs and into wide use.

"Telepresence" applications may finally catch on for business meetings, design collaborations, and education. Some of the best teachers in the world could be virtually accessible. In "telemedicine", heralded since the 1920s, applications might range from monitoring patients at home to managing disaster response – integrating information from many sources in real time for emergency crews on the scene, hospital teams, and others. Robots could be dispatched to perform tasks in hazardous or inaccessible sites, run by experts whose immersion in sensory information and intuitive controls, lets them work as if they were really there.

Similar applications might take off as games or training vehicles.

The proliferation of information appliances will also influence the direction of applications and the packet networks that support them. The most pervasive information applicances may turn out to be virtually invisible, like the twenty-odd motors in a modern car that are doing something other than driving the wheels. Networked devices may multiply like mice and vanish into the woodwork of our lives.

One thread running through all trends in packet applications is "want more, pay more, get more". In sharp contrast to the typical Internet user's experience, packet telephony and mixed-media services will be expected to deliver basic levels of quality and availability that approach traditional phone service and higher levels for a price.

Glimpses of cloud nine

What would it mean to have the best of both worlds, datacom and telecom? The following sketch should look pretty close :

- The quality, reliability and performance associated with voice networks, including sophisticated capabilities for lowcost, reliable operations;
- The relative ease of media integration and low cost associated with data networks;

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Scalability to the gigabit-per-second level and beyond, combined with flexible, efficient bandwidth utilization;
- Reduction in complexity, making it simpler and less expensive to run and use networks – if not by putting data, voice, and mixed media on a single infrastructure, then by creating the effect of s single infrastructure through integration of legacy and emerging technologies;
- The ability to make a high degree of security and privacy standard, and to offer even higher levels at a premium.

Layered architecture supporting convergence

Technology for Enterprise Functions		Technology for Carrier Functions
• NM systems • Call centres • Mixed-media applications	Application/Network Mangement	• Web servers • Transaction server
• Virtual private networks • Virtual LANs • QoS administration	Virtual Networking Abstracting the network to ensure rapid service delivery and management	• Service management systems for virtual private networks
	Control Points Distributed control architecture	• Voice internetworking points • Connection managers • Internet control points
• PBXs, multimedia call servers and gateways • Internet telephony servers and gateways • Domain name servers • LAN emulation servers • Multiprotocol over ATM, other protocol servers	Communication servers Centralising functions	Servers for : • Domain name service • Internet directory service • Intelligent Network services • Firewall/security • LAN emulation • Multiprotocol over ATM
• Gigabit routers • Layer 3 switches • Enterprise multiprotocol routers • Branch routers	Layer 3 Routing and Switching, Packets of information	• Gigabit routers • Layer 3 switches • Enterprise multiprotocol routers • Branch routers
• ISDN, Frame Relay • ATM switching • LAN switching	Layer 2 Switching • Circuit, packet and cell switching • Deterministic vs. statistical multiplesxing	• ISDN, Frame Relay • ATM switching • LAN switching
• SONET/SDH • Wireless air interfaces • POTS, ISDN, digital subscriber line (xDSL) • 10,100 and 1000 Mbps, Ethernet • Token ring FDDI	Transmission and Access • Transporting bits • Enabling connectivity	• SONET/SDH • Wireless air interfaces • POTS, ISDN, digital subscriber line (xDSL) • 10,100 and 1000 Mbps, Ethernet • Token ring FDDI

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

The touchstone for any solution goes by the name of QoS, for quality of service. The term is used broadly for guaranteed delivery of the expected service. Specifically, QoS means the ability to treat different types of traffic and classes of service differently, giving some priority over others, and automatically applying the appropriate treatement to each. QoS capability touches on the attributes outlined above, and it's essential for the first and the last of them.

Is there a way to get there from here? More ways than one – by combining the strengths of connectionless and connection-oriented networking technologies.

Here and Now : Not a bad place to start

When LAN environments are asked to perform like telephone networks, results can be disappointing. Segmentation, abstraction, and over-provisioning of LANs can help to achieve better performance, network management, and voice quality than connectionless packet networks have had in the past.

Switched Ethernet and virtual LAN technologies enable segmentation of LANs for higher performance and separation of work group configuration from the actual layout of facilities. The raw bandwidth offered by new Ethernet technology – 100 Mbps now, with a gigabit per second on the horizon – can help to protect voice traffic from the vagaries of the connectionless approach, atleast until the new bandwidth is saturated. Looking further ahead, several approaches to providing QoS on switched and shared LANs are in circulation.

The TCP/IP protocol suite has proven successful as a unifying technology for data and mixedmedia communications. The number of computers running Internet-oriented protocol stacks is said to be approaching 100 million and climbing. Even the well known shortcomings of IP networking have more to do with unanticipated applications than with flaws in the original design. For instance, the best-effort approach to packet delivery is fine for the data traffic the Internet was designed to handle, and it's part of the reason the Internet has survived its explosive growth.

In the draft specification for IPv6, some of the most serious limitations are addressed, if not solved. The Internet Engineering Task Force has simplified the protocol, added header information that allows a flow of packets to be identified with an individual call or session, and reduced the amount of work that must be done to route packets. And it has enlarged the name space in such a way that just about every object in your life could have an Internet address.

IP switching offers one route to QoS for wide area networking, combining tags or flow identification with weighted fair queuing algorithms – mathematical techniques for enforcing QoS policies on networks that carry mixed media traffic from diverse sources. Reservation protocols such as RSVP and "aware applications" equipped to use them also represent a partial step. Given the popularity of linking Ip domains by Frame Relay, some consider frame switching to be an avenue worth exploring in the quest for QoS. Many consider IP over ATM to be the most effective approach that's available today.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

QOS : Thinking it through, End-to-end

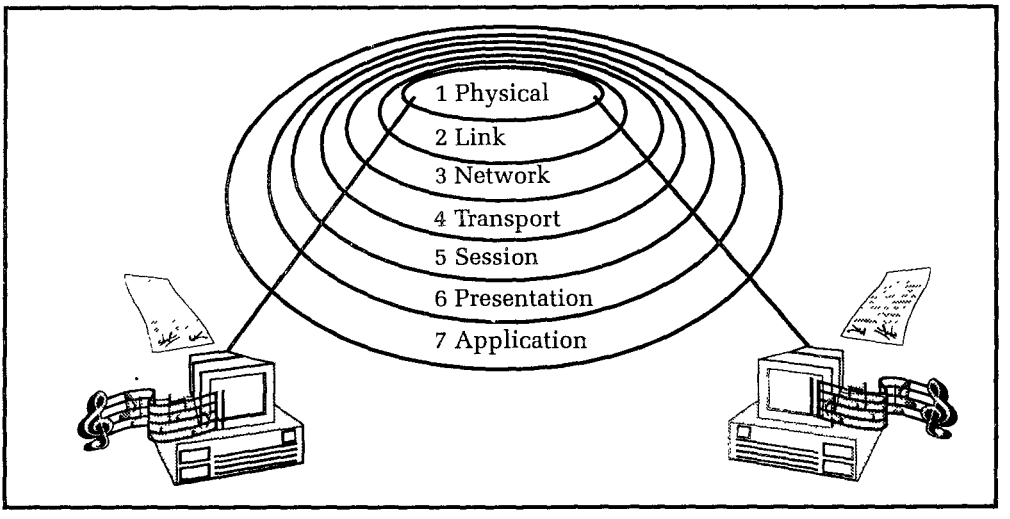


Figure 3. Operations at every layer of the Open Systems Interconnection reference model can affect Quality of Service. So can scheduling of resources in the communications terminals during packet-voice and mixed-media calls. End-to-end thinking must reach all the way out (or in) to the terminal's operating system.

ATM is the maturest switching technology for mixed-media networking at very high bit rates. Its provision of virtual circuits and its use of short, fixed length cells simplify mapping a mix of traffic types onto broadband transport systems based on Synchronous Optical Network and Synchronous Digital Hierarchy (SONET/SDH) standards. From its conception, ATM was designed to ease mixed media service integration while preserving attributes of voice networks and offering QoS guarantees.

With ATM, as critics point out, QoS and other benefits rooted in the telecom world come at price, paid in the complexity of switch software and in the "cell tax", and additional burden of processing required to convert IP and other protocols to and from the ATM format. On the other hand, it has also been noted that connectionless approaches levy a "lack-of-network-management tax", particularly where traffic is highly aggregated and congestion control would have a large impact on the efficiency of bandwidth utilization. In addition, current approaches to providing network management and QoS on a connectionless network call for more code, more processing and more complexity in end-user applications, network elements, or both.

What matters most is knowing where you stand and understanding the trade-offs going forward.

Out to the horizon

Private and public network operators, including ISPs, need to integrate the technologies they have and know best, with new technologies in a way that smooths network evolution and facilitates internetworking. Near-term trends point toward the predominance of different packet technologies in different parts of the network landscape. Available solutions differ by network domain, as do traffic characteristics.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

In the core of a carrier network, surging tributaries of packets and cells come together and get shunted toward other destinations. The characteristics of aggregated traffic here make bandwidth requirements relatively stable and highly predictable. The trend for the core is toward SONET/SDH with ATM switching – capitalizing on ATM's high throughput – or re-configurable high-speed cross-connects.

"Edge" networking the domain where wide area networking and high-capacity private lines come into play, may be handled by an enterprise or ISP, by a telecom carrier, or by both in concert. From the edge out (or in) to the end-user, traffic volume tends to be lower and also much more variable than in the network core. At the edge, the trend is toward wide area networking with Frame Relay and ATM, relying heavily on ATM's dexterity in bandwidth management.

Within an enterprise, switched and routed IP intranets, which may or may not use ATM, seem likely to predominate. At the desktop, it's likely to be IP networking over conventional and switched Ethernet LANs. The day when the typical end-user outside an enterprise will plug into a packet-based access network instead of firing up a modem may be far enough over the horizon that we can set that prospect aside, for now.

As the broad convergence of voice and data networking plays out over the next few years, a few central themes will become increasingly insistent. QoS is one. Another is "abstracting the network", as in virtual LANs, to provide virtual private network across wide areas.

Security can only grow in importance with the continuing rise of electronic commerce at all levels. Security technology will extend from software firewalls to firewall like packet filtering on silicon. Encrypted virtual LAN technology will extend the kind of security that exists within a firewall across non-secure networks, enabling secure communication between members of a workgroup located at different campuses.

One last theme is billing. No, its not entirely a technology issue, but technology will certainly play a roll if companies want to run packet-based communications businesses more like the traditional phone business. In a QoS-capable network, monthly charges could be based on classes of service. Usage could be metered by counting cells though probably not by counting packets. A flat charge per slice of bandwidth might be an option. Beyond such rudimentary suggestions, however, technology should probably defer to the inventiveness of business.

Adapted from "Bell Labs Technology Trends and Developments" from Luccent Technologies.

24.3 WHAT IS COMPUTER TELEPHONY?

Two technologies are revolutionising the way the world communicates: telephone and computers. Telephones are everywhere. For decades, they have been prevalent in offices, public establishments and homes. And computers are catching up. However, these two technologies historically have remained separate. Often, the only thing in common has been the desk on which they both sit.

The power driving the Computer Telephony industry is telephone network access to computer information through almost any convenient, easy-to-use, and available terminal device, including :

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Telephones (pulse dial, touch-tone, and wireless)
- Analog Display Services Interface (ADSI) phones
- Pagers
- Facsimile (fax) machines
- Personal Digital Assistants (PDAs)
- Personal Computers (PCs)

Through these devices the computer and the telephone can work together to offer a range of services.

In simplest terms, computer telephony is the technique of coordinating the actions of telephone and computer systems. This technology has existed in commercial form since the mid-1980s, but it has been exploited only in a few niche markets particularly in large call centers, where call volumes easily justified the cost of complex custom-built systems.

Computer Telephony systems can range from simple voice mail to multimedia gateways. The equipment used in these systems includes voice response units (VRUs), fax servers, speech recognition and voice recognition hardware, and Intelligent Peripherals that are deployed by telephone companies.

Today's businesses need to leverage the power of these diverse, multi-user Computer Telephony systems to improve productivity, give users more access to information, and provide communications options and services to both customers and employees. For example.

- Bank customers can use the telephone to access their personal account information stored in the bank's main computer. (To some extent, Citibank allows you to do this in India)
- Business customers can use the telephone to automatically receive information about a product through a fax machine.
- Employees can access computer-managed voice, fax, and even data (text messages and other information) though telephones, computers, or both, to effectively connect offsite workers to the office and to expand relationships with the external community.

Computer telephony applications

The varied applications of computer telephony include :

Advanced Intelligent Network/Intelligent Peripherals, Audio Conferencing, Audiotex, Business Conferencing, Call completion, Emergency Notification/ Dispatch, Enhanced Fax Services, Fax Broadcast, Fax-on-Demand, Follow-Me/ One-Number Service, Interactive Voice Response, LAN Fax Gateway, Telemarketing/Call Centre, Unified Messaging and Voice Mail.

24.4 WHAT IS UNIFIED MESSAGING

Imagine you are a network administrator who often must troubleshoot remote office sites. How do you keep in contact with headquarters while you're offsite? Most likely with a pager and telephone. It's not an ideal solution, but at least you are immediately notified of any emergencies.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Now imagine that you are a salesperson who spends half of your time on the road. How do you keep in touch with the home base? What if a client sends you a request for proposal via fax while you're driving on the road?

With unified messaging, a growing number of sales people would know about that incoming fax – without needing an assistant to monitor the fax machine and place a call when it comes in. And that beleaguered network administrator could prioritise all of his or her messages – no matter what the medium – with one glance at one unified mailbox.

But what exactly is unified messaging? Well, that depends on who you ask. There are almost as many definitions as vendors, and what one vendor calls "unified messaging", another vendor will call a "universal in box", and yet another will term "integrated messaging".

Defining our terms

The Unified Messaging Consortium (UMC, www.unified-msg.com), a market research organization and think tank that has the support of many of the industry's heavy hitters – including Oracle, Nortel Networks, Lucent Technologies, and Callware – makes a distinction between unified mail and unified messaging.

UMC defines unified mail solutions as having the capability to store the messages of several media types in one mailbox, with user accessibility from a PC and/or telephone. Unified mail, which is becoming more commonplace, is basically a passive (albeit very helpful) solution. The user can access a single message store, but before the user responds, he or she must still verify that the message being sent can be received by the originator.

For example, a caller leaves a voice message that is stored in a unified mailbox. The recipient retrieves and reads the message via PC, and types a response to the caller. But how will the response be delivered? The recipient who is now responding cannot be sure that the original sender has e-mail unless it is explicitly stated in the message. So, although the recipient can retrieve a message in the medium of his or her choice, the success of the reply cannot be known.

Unified messaging is defined by the UMC as the ability to create and respond to multimedia messages with fidelity to the originator from either a telephone or PC. Basically, this means that like unified mail, the user can access a single message store containing multiple message types, and then (unlike unified mail) respond automatically in a format acceptable to the original sender.

As an analogy, think of e-mail. Even though you use Microsoft Exchange, you can still receive a message originated in Lotus Notes and use your reply function to respond to it, without worrying about whether the original sender will be able to read your response. Although unified messaging vendors are aiming for this sort of interoperability, it is not yet a reality.

For the purposes of this article, and to better reflect the de facto definition in the marketplace, I will use the term "unified messaging" to merely signify a solution with a single inbox for voice, e-mail and fax messages that is accessible by both telephone and PC; how responses are made is not a defining factor.

There are two basic architectural approaches to unified messaging. One approach integrates all three message types at the client, and the other does the

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

job at the server. Unifying messages at the client can be complex, because it means integrating separate fax, voice, and e-mail servers with software that may be running on still another server. Although the client approach requires a high degree of coordination between the IT and telephony departments, it is also generally considered safer, because if e-mail goes down, you still have the use of your telephone and fax systems.

The other selling point of the client-side approach is that companies may be unwilling to spend the money to uproot all three servers and replace them with one system when there is no clear cost justification.

The alternate approach is to unify all media type on one server. Although this idea may cause a lot of uneasiness (especially among the telephony folks), it does not offer an architecture that is much simpler to manage. With this approach, administration is much more straightforward because there are no server synchronization issues to contend with.

The Market

As with the ambiguous definition of the technology itself, there is much disagreement over the size and scope of the market. Frost and sullivan (www.frost.com) estimate the size and scope of the market.

Frost and Sullivan (www.frost.com) estimate the size of the unified messaging market to nearly US$5 billion by 2005. The Pelorus Group (www.pelorus-group.com) forecasts that unified messaging revenues for customer premises equipment are expected to hit nearly US$1 billion by 2002. But there are many contrarians who doubt the rosy forecasts and see the unified messaging market levelling off, or even trending down.

The sceptics see the unified messaging market as being very narrow and appealing mainly to organizations with either large sales forces or mobile workers. Many observers think that because of its complexity and expense, unified messaging will never be widely implemented.

The unified messaging market can be roughly divided into two segments : vendors that provide unified messaging software for service providers and the enterprise, and the service providers that offer outsourced unified messaging to both business and home consumers. In this article, we will look at vendors providing software or services for the enterprise customer.

Software vendors

Most unified messaging software vendors tend to come from the telephony world, and their unified messaging solutions often reflect this bias. The first generation of unified messaging products (and still the most prevalent) were usually from voice mail vendors who integrated e-mail, with varying results, into the existing voice messaging system.

Nortel Networks is, of course, a big player in the telecom equipment world, and it moved aggressively into the unified messaging market with the introduction of CallPilot, a Windows NT-based system that integrates with a company's existing e-mail applications at the desktop to create a unified messaging solution that uses the native e-mail interface. CallPilot integrates with groupware applications, including Lotus Notes and Microsoft Exchange and Outlook, and uses Internet

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Message Access Protocol 4 (IMAP4) to integrate with browser-based clients such as Netscape Messenger, Outlook Express, and Qualcomm's Eudora Pro.

One of CallPilot's most unique features is its speech-recognition capabilities. Using voice commands such as "play" or "print", a user can remotely manage voice and fax communications over the telephone. Additionally, voice messages can be stored on a PC for archival purposes or forwarded as a .wav file as an attachment to an e-mail. Remote users can dial in and have voice messages streamed to their PC.

CallPilot offers several interesting fax management features, including password protected access to faxes and outbound faxing from any Windows Application. The downside of CallPilot is that it presently integrates only with the Nortel Meridian 1 PBX; the company says it plans to support other manufacturer's systems early 2000.

US unified messaging revenue forecasts 1999-2005 (In US$M)

Market Segment	1999	2000	2001	2002	2003	2004	2005
*Software	$402	$728	$1026	$1317	$1633	$2018	$2415
Services	$148	$295	$603	$1085	$1641	$2115	$2518
Total	$550	$1021	$1629	$2402	$3274	$4133	$4933

Source : Frost and Sullivan

* Market includes software for enterprise customers and service providers

Applied Voice Technology (AVT, www.applied voice.com), whose roots also lie in the telephony world, offers unified messaging capabilities for OS/2 and Windows environments with its CallXpress computer telephony product line. With CallXpress, you can add a module called Desktop Message Manager that provides a unified messaging interface for the PC so that voice, fax, and e-mail can be managed using a GUI and a common set of management commands. Support for Microsoft Exchange and Outlook or Lotus Notes is available.

One of CallXpress' most interesting features is its text-to-speech capability, which enables a user to hear e-mail to a fax machine using the telephone, or reply to an e-mail with a voice message. If your organization does a lot of faxing, you may want to consider CallXpress because of its tight integration with AVT's Right Fax fax server, which lets you do things like access faxes from the telephone and send faxes with voice annotations.

AVT's offering integrates with a slew of PBXs, but it does require dedicated hardware to run, so you can't put it on the same server as our e-mail application. CallXpress has some nice management capabilities that let you administer multiple systems centrally over a WAN, and the Windows NT version lets you manage it from any Windows client on the LAN.

Callegra is a Callware Technologies' (www.callware.com) computer telephony flagship, and it provides unified messaging capabilities through its CallegraFax and CallegraDesk modules. Callware's unified messaging solution resides on either a Windows NT or NetWare server that sits between your network server and your phone systems, and it supports and most major PBXs. Like the other unified messaging products already covered, Callegra is a voice a fax solution

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

that integrates with e-mail; in Callegra's case, it supports GroupWise, Lotus Notes and Exchange/Outlook.

One interesting feature of Callegra is that it can notify users of waiting messages through pagers, cell phones, and message-waiting indicators. Callegra Desk also enables users to identify urgent messages by viewing the caller's identity, message time and date, length, and the subject of the call.

Another old standby from the telephony world is Lucent Technologies. With its buyout of Octel communications in September 1997, Lucent acquired Octel's considerable experience in integrated messaging. Shortly after the acquisition, the newly formed Lucent technologies octel messaging Division released Unified Messenger, the first product to add voice mail to Microsoft Exchange.

Unified Messenger is still betting on Exchange, as it is the only e-mail application with which Unified Messenger integrates. If you already have or are planning to buy an e-mail application other than Exchange, Lucent's Intuity Audix Multimedia Messaging System offers a software option that links the system to HP OpenMail, Lotus. Notes, and other e-mail applications in addition to Exchange.

Both Octel's Unified Messenger and the Intuity Audix Multimedia Messaging System offer the basic functionalisties of unified messaging, including access to all three message types via PC or Touch-Tone phone. A selling point of unified Messenger is that it simplifies system administration by combining the administrative interface for both voice and e-mail. Because the same Microsoft Exchange interface is used, changes to the Exchange Server directory will automatically be replicated to all system directories, so the change is made only one.

The voice messaging capabilities of unified Messenger let users create, route, comment on, and save voice messages just like they do e-mail messages. And, like other products covered, voice messages can be retrieved from any Touch-Tone telephone, and the text-to-speech capabilities allow for e-mail retrieval over the telephone.

Service providers

International Data Corp. (IDC,www.idc.com) estimates that the market for unified messaging services will reach US$3 billion by 2002, and many industry observers predict that the service provider segment of the market will grow much more quickly than the software segment.

If your company wants the flexibility and benefits of unified messaging without the administration worries and capital outlay, then why not outsource? The concept seems to be catching on; although there are currently only a handful of unified messaging service providers, several telcos and ISPs have plans to offer unified messaging services in the year 2000. Among the companies developing services are AT &T WorldNet, GTE Internetworking, and Infonet Services.

Back to the Future

In 1994, a draft proposal for voice mail over MIME was presented to the Universal Messaging Interoperability Group (UMIG). After the UMIG disbanded later that year, the Electronic Messaging Association (EMA) formed the voice

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

Profile for Internet Mail (VPIM) Work Group, which had the goal of creating a unified-messaging standard to integrate e-mail, voice messaging, and a fax over TCP/IP. VPIM2, which is based on MIME, has been approved by the IETF as a proposed standard, and was published as RFC 2421 in September 1998.

Eventually, we will all have low-cost Personal Digital Assistants (PDAs) that give us the unified messaging capabilities described in this article, plus sophisticated filtering agents that alert us to the messages we really care about. The question is, how long must we wait? And, in the meantime, will unified messaging as it exists today ever grain a foothold in the enterprise, or will it remain a handy, but ultimately limited application for high-powered executives and travelling sales people?

The answer likely will depend on how successful the VPIM Work Group is in carrying out its stated mission of empowering businesses and individuals to increase productivity by eliminating the barriers of proprietary massaging systems. The vendors behind VPIM are hoping that as more and more VPIM-compatible products are released, end users will be able to send and receive voice mail and fax with the same level of interoperability that e-mail enjoys. The other cbvious benefit of IP messaging is that voice messages and faxes distributed over the Internet do not incur long distance tolls.

Since the "buy" decision regarding unified messaging will be made by folks looking at return on investment, and not the less tangible factor of convenience, vendors will have to make a much more compelling bottom line case for the productivity benefits of unified messaging than they have thus far.

24.5 ALL ABOUT CALL CENTRE TECHNOLOGY

There are two important technologies used for call centres today. They are the conventional EPABX based model and the new PC Based technology.

EPABX based call centre

Historically call centres evolved from a place where telephone lines landed on agent desks. Then PBX was added with an automatic call distributor (ACD) to distribute calls coming on a common lines. Over time, Predictive Dialers, IVR systems and CTI were added to create a full fledged call centre. The systems were thus created on a gradual build up model.

PC based call centre

A PC based call centre integrates all the components of a call centre into one server as software components. The basic platform is a PC based server running a PC Operating System and circuity for the telephony interfaces, eliminating the need for an EPABX. All these are industry standard systems, providing reliability and lower cost of ownership by allowing the call centre solution to ride the technology evolution curve.

The traditional EPABX architecture has not kept pace with the rapid changes in the computer industry. Telecom was a relatively protected industry and products and technology were evolving much slower than the computer industry. Thus, while computer systems power and reliability were growing and costs coming down in accordance with Moore's law, the telecom equipment market saw near stagnation. Thus a PC based call centre now costs far less than the

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

traditional architecture. There are two main reasons for the dramatically lower cost of a PC based system :

- Standard hardware and software components rather than proprietary systems.
- Call centre components are software modules on a common platform thus eliminating expensive and difficult integrations due to the need for integrating proprietary systems from different vendors.

Technology comparision

Feature comparision		
Feature	**Legacy systems**	**PC based call centre**
ACD Capabilities	Simple Hunt Groups groups	Skill based routing with Virtual Agent
Call Control	Complex Keypad	Simple Desktop GUI
Conferencing	Only Conferencing	Conferencing and Coaching
MIS & Statistics	Limited Reports	All statistics available in open database
Architecture	Proprietary and closed	Standards based and Open
Web Integration	Not possible	Built in Multimedia
Handling System	Not possible	Possible
Integration	Using proprietary CT server and CT link software	Using open, published APIs and standard interfaces
System Mangement	Proprietary Protocols	SNMP based open interface
Setup & Installation	3 months	2 weeks

Apart from the much lower costs, PC based call centres provide far superior features (see comparison in table above). The most important aspect of the PC based call centres is the flexibility they provide in increasing the scale of operations. In a traditional architecture, adding agents to the system means that additional hardware systems have to be bought unlike PC based systems, where the ACD, IVR and PD are software components, thus one needs to just buy additional licenses.

Key components of call centre technology

- *Automatic call distributor (ACD)*

  ACDs distributed in various ways like Network Directed Routing, Agent Idleness Based Routing and Agent Skill based routing.

- *Predictive dialer*

  A predictive dialer automates outbound calling by using complex algorithms that consider a number of factors such as the number of available telephone lines and operators, the probability of getting a busy signal and the length of an average conversation. PDs can enable tremendous productivity improvements because no answer, busy signals and other incomplete calls are screened out.

- Computer telephony integration (CTI)

  CTI integrates telephone and computer operations by linking databases to the telephone connection. A common use of CTI is a "screen pop", in which customer information "pops up" on an agent's screen as a call is received.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

- Web integration

  Web Integration allows customers to interact with call centre agents through web Callback, Web Chat, and Collaborative Browsing allowing companies to provide live contact to online customers.

- Interactive voice response/Fax on demand (IVR/FOD)

  IVR and FOD provides information to a customer by turning the touch tone pad of a telephone into a keyboard. As a result, many standard queries formerly answered by an agent can be handled by an IVR, free in agents for more complex, value-added work.

- Voice logging and messaging

  Voice Logging allows digital recording of conversations and messaging allows callers to leave messages if agents are not available for handling a call.

- The Future? Internet contact centre

  The term "call centre" itself, will become obsolete. Sales, marketing and customer service are already moving toward multiple methods of interaction including telephone, e-mail, video-conferencing and the Internet; so call centres will evolve into "Contact Centres" allowing multiple media for connecting to customers. E-commerce is coming a reality going beyond the type. But there is a catch, 66 per cent of online transactions are abandoned before a sale is closed. That is where an Internet enabled Call Centre helps companies provide the human touch for providing information assistance, closing sales and servicing customers.

PC based call centres provide the ideal platform for Internet Contact Centres because of the multi media handling capability of the PCs and the close linkage of the PC to the Internet.

[The matter for this chapter is reproduced from LAN MAGAZINE December 1999]

(Courtesy : LAN MAGAZINE, Dec 99)

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

"This page is Intentionally Left Blank"

Copyright © 2009. Global Media. All rights reserved.

Murthy, C.S.V.. Data Communication and Networking, Global Media, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/univ-people-ebooks/detail.action?docID=3011330.
Created from univ-people-ebooks on 2024-09-13 03:58:26.

REFERENCES

1. Barnasel C. Dodosiewicz W and Gburzynski P : "Routing in Multitop Packet Switching Networks; Gb/s Challenge ;"IEEE Network Magazine Vol. 9, May/ June 1995.
2. AT & T and Bell core "Observations of Error Characteristics of Fiber Optic Transmission systems" CCITTSG XVIII, San Diego, Jan. 1989.
3. Bates, R J, Wireless Networked Communications, New York, McGraw - Hill, 1994.
4. Berness - Lee, T, Caillau A. Loutonen, A. Nielsen H.F and SECRET, A; "The World Wide Web" common of the ACM, Vol. 37, August 1994.
5. Bertsekas D; and Gallager, R : Data Networks, 2nd ed., Englewood Cliffs, NJ; Prentice Hall, 1992.
6. Black, U.D. : TCP/IP and Related Protocols, New York, McGraw - Hill, 1995.
7. Data Link Protocols, Englewood Cliffs, NJ : Prentice Hall, 1993.
8. CARL-MITCHELL, S and Quarterman, JS; practical Internet working with TCP/IP and UNIX, Reading, MA; Addison Wesley, 1993.
9. Chao. J.J. Ghosal, D. Saha D and Tripathi S.K, "IP on ATM Local Area Networks", IEEE common magazine Vol. 32, August 1994.
10. Corner D E The Internet Book, Internet working with TCP/IP Vol. 1, 3rd Edn., Englewood Cliffs, NJ, Prentice Hall 1995.
11. Cooper E : Broad band Network Technology, Englewood Cliffs, NJ; Prentice Hall, 1986.
12. Davis P.T. and Mc Guffin C.R, Wireless Local Area Network, New York, McGraw-Hill, 1995.
13. Day J.D. and Zimmermann H - "The OSI Reference Model", proc. of the IEEE, Vol. 71, Dec. 1983.
14. Day J.D. "The (un)Revised OSI Reference Model" comp. commun, Rev.; Vol. 71, Oct. 1995.
15. De Prycker M. Asynchronous Transfer mode, 2nd ed., New York: Ellis Horwood, 1993.
16. FEIT, S : SNMP – A guide to network management, New York, McGraw-Hill, 1995.
17. Goralski WJ – Introduction to ATM Networking, New York, McGraw - Hill, 1995.
18. Handel R, Huber M.N. and Schroder S. ATM concepts, Protocols and applications 2nd eg. Addison - Wesley, 1994.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:02:25.

19. Hong, D and Sada T - 'Congestion Control and Prevention in ATM Networks' IEEE network magazine, Vol. 5 pp. 10–16 July/August 1991.
20. Huitema C, The New Internet Protocol, Englewood Cliffs, NJ, Prentice Hall, 1996 and Routing the Internet (same 1995 edition).
21. Johnson HW : Fast Ethernet – Dawn of a New Network, Englewood Cliffs, NJ, Prentice Hall 1996.
22. Kessler G C and Train D : Metropolitan Area Networks, Concepts, Standards and Services, New York, McGraw - Hill, 1992.
23. KIM JB, SUDAT and Yoshimura M; International standardisation of B-ISDN; Computer networks and ISDN systems, Vol. 27, Oct. 1994.
24. KYAS, O : ATM Networks, London, International Thomas Publishing 1995.
25. Le Bondec J.Y : "The Asynchronous Transfer Mode, A Tutorial" Computer Networks and ISDN Systems, Vol. 24, May 1992.
26. Luotonen and Altio K : "World Wide Web Proxies" Computer Networks and ISDN Systems, Vol. 27, Nov. 1994.
27. Mirchandani S and Khanna R (eds) FDDI technologies and Applications, New York, John Wiley, 1993.
28. Nagle, J "Conjestion Control in TCP/IP Internet works" Computer Commun, Rev. Vol. 14, Oct. 1984.
29. Omidyar C.G. and Aldridge A. Introduction to SDH/SONET, IEEE common, Magazine, Vol. 31, Sept. 1993.
30. Perlman, R. Interconnections : Bridges and Routers Reading MA, Addison - Wesley, 1992.
31. Piscitello DM and Chapin AL, Open Systems Networking, TCP/IP and OSI Addison Wesley, 1993.
32. Shachan N. and Mckenney P : "Packet recovery in high speed networks using coding and buffer management", Proc. Infocom 90 IEEE, 1990.
33. Spragins JD and hammond J.L and Paulikouski K. Telecommunications protocols and Design, Addison Wesley 1991.
34. Stallings W. ISDN and Broadband ISDN with frame relay and ATM, Englewood Cliffs, NJ, Prentice Hall, 1995.
35. Stiller B : 'A Survey of UNI Signalling Systems and Protocols' Computer commun, Rev. Vol. 25, April, 1995.
36. Yang, C–Q and Reddy, AVS : A taxonomy fax congestion Control Algorithms in Packet Switching Networks, Vol. 9, July/Aug. 1975.
37. Andrew S. Tanenbaum Computer networks, 3rd edition 1996, Prentice Hall, NJ, 07458, USA.
38. 'Introduction to Data Communications and Networking' Behronz and Forouzan, Tata McGraw-Hill Publishing Co. Ltd., New Delhi, 1998.
39. Introduction to Data Communications by Jerry Fitzgerald and Alan Dennis John Wiley and Sons, Inc., New York, 1996.

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:02:25.

INDEX

A

A packets 328
A periodic signals 75
AAL 5, 6, 349
AAL1 343
AAL2 344
AAL3/4 350
AAL5 352
Absolution maximum time (AMT) 261
ACK 209
Active documents 460
Address resolution protocol (ARP) 439
Addressing 400
Aliases 452
Alternate mark inversion (AMI) 97
Amplitude modulation 82, 103, 111
Amplitude shift keying (ASK) 103
Amplitude 81
Analog encoding 110
Analog hierarchy 185
Analog reading 99
Analog services (switched, leased) 183
Analog services over the telephone network 300
Analog signals 76
Analog transmission 74
Analog transmission 74
ANSI 23
Antennas 160
Aperiodic signals 75
Application adaptation layer (AAL) 347
Application layer 67, 425, 444
Archie 454
ARM, ABM 218
ASCII 91
ASK bandwidth 104
Asynchronous protocols 209
Asynchronous TDM 179
Asynchronous transmission mode (ATM) 24, 340
Asynchronous transmission 117
ATM 27, 356
ATM 53, 357
ATM convergence to SONET/SDH 369
ATM design goals 340
ATM encapsulation 356
ATM layer 353
ATM Protocol architecture 347
ATM topology 346
ATM vs Frame relay 341
Authentication 424

B

B packets 328
Backward explicit congest ion notification (BECN) 334
Bandwidth 80, 83
Basic rate interface (BRI) 303, 308
Bell modems 140, 141, 142
Biphase 96
Bipolar 8 zero substitution (B8ZS) 98
Bipolar 97
Bit oriented protocols 215, 216
BRI frame 309
Bridges 374, 376
- encapsulating 380
- Learning 379
- Multiport 379
- Multiprotocol 380
- protocol filtering 380
- Simple 379

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:01:06.

Broad band ISDN (B-ISDN) 315
Brouters 381
Browser architecture 459
BSC 211, 214
BSC control frame 214
BSC frames 213

C

Callcenter technology 487
CCITT 17, 21
Cell networks 343
Cell switching 343
Cellular bands 164
Cellular phone 165
Cellular radio system 164
Cellular telephone 12
Cellular transmission 162
Channels B, D, H 302
Checksum 199
Circuit switch 283
Circuit switching 283, 286
Coaxial cable (COAX) 151
Codec 73
Codes 122
Common gateway interface (CGI) 461
Common management information protocol (CMIP) 428
Common management information service (CMIS) 429
Common management information service elements 429
Communication media 7
Communication model 7
Communication path 282
Communication process 33
Communication satellites 161
Communication standards 20
Communication system 6
Complex signals 79
Compression 416, 417
- Data
- Lossy
- Relative
- Run length
- Statistical
Computer telephony 481
Concatenation 402
Congestion control 337
Connection 410
- Connection establishment 406
- Connection oriented mode 405
- Connection termination 406
Connection oriented network services (CONS) 292, 293
Connection oriented transport service (COTS) 408
Connectionless network services (CLNS) 292, 294
Connectionless transport service (CLTS) 408
Continuous ARQ 216
Control packets 324, 325
CRC generator 202
CRC 199, 200
Cross bar switch 284
CSMA/CD 248

D

Data 3
Data communication networks 9
Data communication over an analog network 299
Data communication standards 16
Data communication systems 9
Data communications 3, 4, 8
Data compression 140, 416
Data encryption standard (DES) 419
Data link control 209
Data link layer 60
Data link protocols 209
Data monopoly 12
Data processing 4
Data transmission
- Full duplex 42
- Half duplex 42
- Simplex 42
Data transparency 215
Datagram 289

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:01:06.

DB 37 132
DB 9 132
DCE 125
De facto 16
De jurc 16
Decryption 418
Device layer relationship 365
Differential encoding 93, 102, 417
Digital communication 118
Digital data service (DDS) 185
Digital hierarchy 185
Digital services 184
Digital signals 81
Digital transmission 74, 118
Dijkstra algorithm 393
Distance vector routing 386, 390
Distributed queue dual bus (DQDB) IEE 802 – 8, 272
Distributed Queues 274
Distributed routing 383
Distributed system 10
Domain 445
- country
- generic
DSAP (Destination service access point) 247
DTE 125
DTE-DCE interface 125, 128, 129
Dual attachment concentrator (DAC) 266
Dual attachment station (DAS) 266
Duplication control 403
Dynamic documents 460

E

EBCDIC 91
EIA 17, 24, 132, 133
EIA-449/RS-449 130
Electronic data interchange 14
Electronic mail 12, 450, 451
E-lines 187, 189
Encoding schemes 92
Encoding 92
Encryption 415, 418, 419
End to end delivery 395
ENQ/ACK 209
Error control 215, 402
Error correction 198
Error detection methods 197
Errors (types, causes) 194, 195
Ethernet segments 251
Ethernet 245, 248
Even parity check bit 123

F

Fast packet multiplexing (FPM) 182
FECN (Forward explicit congestion notification) 334
Fiber optic transmission system 361
Fibre distributed data interface FDDI 245, 260, 263
File transfer protocol (FTP) 448
Flow control 212
Flow control 405
Folded switch 283
Formal standards 16
Frame relay 332
Frame relay addresses 336
Frame relay implementation 337, 338
Frame relay layers 333
Frame relay network 335
Frame relay operation 335
Frames (S, U, I) 220, 221
Frequency – Division multiplexing (FDM) 172, 174
Frequency domain 78
Frequency modulation 83, 105, 111
Frequency spectrum 80
Frequency 77
FSK (Frequency shift keying) 92, 105
FT-1 187

G

Gateways 385
General format identifier (GFI) 323
Go-back – NAR 216
Gopher 454
Guided media 149

H

H DLC 215, 224, 225, 247
Hamming code 201

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:01:06.

Harmonics 81
Hidensity bipolar 99
Hyper text mark up language (HTML) 459
Hyper text transfer protocol (HTTP) 455

I

IEEE 8025 255
IEEE 17, 23
IETF 25
Information packets 323
Information sharing 244
Information 3
Integrated digital network (IDN) 300
Integrated services digital network (ISDN) 298, 301
Internet activities board 25
Internet address 437
Internet classes 437
Internet control message protocol (ICMP) 440
Internet protocol datagram 436
Internet society 25
Internet standards world 25
Internet working services 374
internet 387
Internet 433
Internetwork protocol (IP) 435
Inverse multiplexing 182
Ionosphere 157
IP telephony 467
IRTF 25
ISDN Access 302
ISDN addressing 314
ISDN broad band 315
ISDN layers 306, 308
ISDN services 299
ISO 22
Isochronous transmission 124
ITU-T 17, 19, 21, 140

J

Java 461

L

LAPD 311, 312
Line configuration 32
Line discipline 209
Line overhead 368
Line switching 282
Link state routing 391
Local area networks 43, 44, 244
Logical channel group number (LCGN) 323
Logical channel number (LCN) 322
Logical link control (LLC) 61, 246, 249
Loss control 404
Lossy compression 418
LRC 199, 200
LSP (Link state packet) 392

M

MAC frame 250
Management information bases (MIBs) 453
Media access control (MAC) 61, 246, 265
Message handling system (MHS) 424
Message switching 291
Metropolitan area networks (MAN) 272
Microwaves transmission 159
Mobile computing 161
Modem 73, 136, 137, 138
Multimode (optical cable) 154
Multiple paths 286
Multiplexing 172, 183, 404
Multipoint configuration 32
Multistage switches 286
Multistation access unit (MAU) 260

N

Network 9, 10, 34-41
- Internet 48
- LAN, MAN, WAN, Bn 42
- Mesh, star, tree, hierarchical, bus, ring, centralised, loop, irregular, hybrid 34-41

Network applications 12
Network file system (NFS) 449
Network interface card (NIC) 249
Network layer 62, 63, 292, 435
Network termination (NT1, NT2) 305

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:01:06.

Network to network interface (NNI) 346
Networking 374
Networks 9, 10
NIST 23
Non periodic signals 75
Non return to zero (NRZ) 92
NRM 218
NRZ – I 92
NRZ – L 92
Null modem cable 129
Nyquist theorem 102

O

Odd parity check bit 123
On-off keying (OOK) 104
Open system 54
- functions 58
- organisation 58
Optical fiber 152
OSI layer upper 413
OSI model 17, 21, 53, 59
OSI transport protocol 406

P

Packet layer protocol (PLP) 323
Packet network 342
Packet switching 286, 287, 289
PAM (Pulse amplitude modulation) 92
Path overhead 368
PCM (Pulse code modulation) 92
PDU format 247
Peer to peer network 245
Period 76, 81
Periodic signals 75
Permanent virtual circuit (PVC) 290
Phase modulation 107, 112
Phase 81
Physical layer 58
Physical medium dependent (PMD) 246
PLP packet 323
Polar encoding 95
Poll/select 210
Presentation layer 66, 415
Primary access service 313
Primary rate interface (PRI) 303, 308, 309
Private UNI 346
Project 802 246
Proprietary standards 16
Protocol stacks 401
Protocol 15
PSK (Phase shift keying) 92, 106, 107, 108
Public directory 421
Public key method 421
Public UNI 346

Q

Quadrature amplitude modulation (QAM) 109

R

Radiated media 156
Radio communication 156
Redundancy checks (VRC, LRC, CRC) 199, 200
Redundancy 197
Relative compression 417
Reliable delivery 401
Remote procedure call (RPC) 448
Repeaters 159, 374, 375
Resource sharing 244
Return to zero (RZ) 96
Reverse address resolution protocol (RARP) 440
Routers 374, 380
Routing algorithms 386
Routing concepts 382
Routing link state 390
Routing table 387
RS 232, RS 422, RS 423, RS 449 133, 134
Runlength compression 416

S

Satellite communication 160, 161
Satellite transmission 161
SDLC 215
Section overhead 368
Segmentation 402

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:01:06.

Select 210
Selective – Reject ARQ 218
Sequence control 403
Sequence numbers 403
Session layer 407, 408
Session layer 64, 65, 412, 413
Session protocol data unit (SPDU) 415
Shielded twisted pair cable (STP) 150
Signals 72, 160
Simple mail transfer protocol (SMTP) 444
Simple network management protocol (SNMP) 453
Simplex 42
Sine wave 85
Single attachment station (SAS) 267
Single mode 154
Sliding window ARQ 216
Sliding window 213, 214
Smart buildings 12
SONET frame 365
SONET (SDH) 361
SONET circuit 362
SONET devices 363
SONET layers 364
Source service access point 247
Space & time division switching combination 284
Space division switch 284
Space-time-time-space (STTS) 284
Standard organisations 17
Standards 15, 126
Static documents 459
Statistical compression 417
Statistical time division multiplexing (STDM) 179
Stop and wait ARQ 215
Stop and wait method 212
STS multiplexing 364
Switched 58, 184
Switched multimegabit data services 276
Switched virtual circuit (SVC) 290
Switching 281
Synchrnonous optical network (SONET) 361
Synchronisation points 414
Synchronous protocols 211
Synchronous transmission 120
Synchronous transport module (STM) 363
Synchronous transport signal (STS) 362

T

TCP Segment 443
Tele communication system 3, 5
Telecommunication standard 17
Telecommunications network 15
Telecommuting 13
Teleconferencing 13
TELNET 446
Terminal adapter (TA) 305
Terminal equipment (TE1, TE2) 304
Terminal equipment identifier (TEI) 312
T-Frames 187
Time division multiplexing (TDM) 173, 176, 177
Time division switch 284
Time domain 78
Time registers 261
Time slot interchange (TSI) 285
Time space time (TST) 284
Timers 262
T-lines 187
Token bus 252
Token holding time (THT) 262
Token passing (Access method)
Token ring 245, 255
Token rotation times (TRT) 262
Topology 34
- bus 38
- centralised network 40
- hierarchical 36, 37
- hybrid 41
- irregular network 40
- loop network 40
- mesh 35
- ring 39
- star 36
- tree 36

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:01:06.

Trans border data flow 14
Transmission
- parallel 119
- serial 119
Transmission control protocol (TCP) 405, 432
Transmission control protocol (TCP) 441
Transmission media 167
Transmission mode 42
Transmission protocol (TCP) 432, 433, 441
Transport layer 64, 398, 440
Transport layer duties 400
Transport protocol data unit (TPDU) 407
Troposphere 157
TTRT (Target token rotation time) 261
Twisted pair cable 150
- Shielded (STP) 152
- unshielded (UTP) 150
Twisted pair wire 150

U

U interface 309
Unguided media 156
Unified messaging 482
Uniform resource locator (URL) 458
Unipolar encoding 93, 94
Unshielded twisted pair cable (UTP) 151
Upper OSI layer 413
User datagram protocol (UDP) 434, 442
User diagram protocol 398
User network interface (UNI) 346

V

V.42 bismodems 140
Veronica 454
Virtual channel identifier (VCI) 345
Virtual channel 329
Virtual circuit 290, 343
Virtual Files 426
Virtual path channel (VPC) 355
Virtual path channel switching 355
Virtual path identifier (VPI) 345
Virtual terminal 426, 4471
Virtual tributaries 366, 367, 368
Virtual tributary indicator 368
Voice & data communication over an analog network 299
Voltage 76
VRC 199, 200

W

Wide area information service (WAIS) 455
Wireless LANs 273
World wide web (www) 455-458

X

X.20 135
X.21 135
X.25 layers 322
X.25 321
X-modem 210

Z

Zero-lot LAN 245

Copyright © 2009. Global Media. All rights reserved.

Murthy, C. (2009). Data communication and networking. Global Media.
Created from univ-people-ebooks on 2024-09-13 04:01:06.