Computer Networks/ Networks

DCAP406/DCAP207

Editor
Sarabjit Kumar

LOVELY PROFESSIONAL UNIVERSITY

COMPUTER NETWORKS/NETWORKS

Edited By

Sarabjit Kumar

ISBN: 978-93-87034-66-2

Printed by
EXCEL BOOKS PRIVATE LIMITED
Regd. Office: E-77, South Ext. Part-I, Delhi-110049
Corporate Office: 1E/14, Jhandewalan Extension, New Delhi-110055


+91-8800697053, +91-011-47520129


info@excelbooks.com/projects@excelbooks.com
internationalalliance@excelbooks.com


www.excelbooks.com

for
Lovely Professional University
Phagwara

CONTENTS

SYLLABUS

Computer Networks/Networks

Objectives: To impart the skills needed to establish a computer network and network troubleshooting. To enable the student to understand various network hardware and software. To enable the student to understand network security issues and their implementation details.

DCAP406 COMPUTER NETWORKS

Sr. No.	Description
1.	Introduction to Computer Networks: uses of computer networks,
2.	Network hardware, network software, Reference models, Example networks
3.	Physical Layer : Theoretical Basis for Data Communication, Guided Transmission Media, Wireless Transmission, Communication Satellites
4.	Public Switched Telephone Network, The Mobile Telephone System, Cable television
5.	Data Link Layer: Design Issues, Error Detection and Correction
6.	Elementary data link protocols, Sliding – Window protocols, Protocol verification, Example Data Link Protocols
7.	The Medium Access Control Sub Layer: The Channel Allocation Problem
8.	Multiple Access Protocols, Ethernet, wireless LANs, Bluetooth, Data Link Layer Switching.
9.	Network Layer: Design Issues, Routing Algorithms, Internetworking, network Layer in the Internet, Congestion Control Algorithms, Quality of service
10.	Transport Layer: Transport Service, Elements of Transport Protocols, The internet transport protocols: UDP,TCP Application Layer: DNS ,E-mail, The World Wide Web, Multimedia ,Network Security - Cryptography

DCAP207 NETWORKS

Sr. No.	Description
1.	Introduction to Computer Networks: Uses of computer networks, Network Hardware: LAN, WAN, MAN, Wireless, Home networks, Internetworks. Network topologies: STAR, Ring, BUS etc.
2.	Network Software: Layers, Protocols, Reference models: OSI Model, TCP/IP model, comparison of OSI and TCI reference model.
3.	Physical Layer: Guided Transmission Media: Magnetic media, Twisted pair, Coaxial cables-base band, broadband, optical fiber transmission. Wireless Transmission, Satellites, PSTN
4.	Networking Devices: Hub, Router, Switch, Bridge, Gateway Switching Techniques: Circuit Switching, Message switching, packet switching
5.	Multiplexing: Frequency Division, Time Division Multiplexing Modulation Techniques: Amplitude, Frequency, Phase
6.	Data Link Layer: Design Issues - Services provided to the network layer, framing, error control, flow control, Error Detection and Correction: Error Correcting Codes, Error Detecting Codes
7.	Data link protocols: Elementary Data link protocols, Sliding Window protocols, HDLC, Data link layer in Internet
8.	MAC Sublayer: CSMA/CD, Ethernet: Ethernet Cabling, Fast Ethernet
9.	Network Layer: Design Issues, Routing Algorithms: Optimality principled, shortest path routing, distance vector routing, link state routing Congestion Control Algorithms: General principles, congestion prevention policies
10.	Network Security: Cryptography – Introduction, Substitution ciphers, transposition ciphers

Unit 1: Introduction to Computer Networks

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Describe the various uses of computer networks from the most general types to the possible uses in more specific circumstances
- Discuss different technologies involved in defining the network hardware
- Explain concept of process network software and the significance of layering the communication process and related design issues for the layers

Introduction

The merging of computers and communications has a profound influence on the way systems are organized. The concept of computer center as a room with a large computer to which the users bring their work for processing is now obsolete. The old model of a single computer servicing all the computational needs of an organization has been replaced by the one in which

Notes

a large system of separate but interconnected computers do the job. These systems are called computer networks. The two computers are said to be interconnected if they are able to exchange information. The connection between the computers need not be only via a copper wire or fiber optics or microwaves. A communication satellite can be used for networking the computers.

1.1 History of Computer Networks

Following is a brief history of computers, networking and telecommunication milestones:

- **1897:** CRT (Cathode Ray Tube) credited to Braun
- **1900–1915:** Teletype (telegraph 5 bit)
- **1915–1020:** ARQ (Automatic Repeat request) credited to Van Duuren
- **1930–1940:** ENIAC credited to DOD/MIT
- **1950s:** SAGE (Semi-Automatic Ground Environment) MIT 1950s
- **1960s:** Transistorized Computers–2nd Generation
- **1961:** CTSS (Compatible Time Sharing System) credited to Cobato/MIT
- **1965:** Auto Equalization Techniques of Phone lines credited to Lucky et al.
- **1966:** Fiber Glass credited to Kao & Hockman
- **1967:** Integrated Circuits Computers–3rd Generation
- **1968:** Carterfone–FCC Decision in
- **1969:** A group of DoD researchers linked four computers at UCLA, SRI, University of Utah and the UCSB. They created a network to communicate with one another about government projects. The network was part of the DoD's Advanced Research Project Agency, and was dubbed ARPAnet.
- **1972:** More than 50 universities and military agencies were linked together on the network. For a short period of time, it was a top secret defence project, ensuring that computers could talk to each other in the event of a nuclear attack. The communication system between the sites was called email and was invented by Ray Tomlinson of Bolt, Berank and Newman.
- **1973:** The defence project links were extended to Norway and England.
- **1974:** Transmission Control Protocol (TCP) was published and the military and educational links diverged. Organizations like NASA began to experiment with computer networks, and the networks began to interconnect and the name Internet was coined.
- **1976:** The Queen sends an email from RSRE Malvern.
- **1983:** TCP/IP become the protocol standard for ARPAnet. Scott Fahlman invents the smiley to convey emotions in email.
- **1984:** In the US, the NSF built high speed, long distance lines that connected supercomputer sites across the USA. These eventually replaced the original ARPAnet. In time, NSFnet was joined by other networks at dozens of universities, research laboratories and high-tech companies. The system for assigning names to computers on the network was introduced — DNS. JANet was launched to connect British Universities.
- **1986:** The NSF established its own faster network NSFnet and Network News Transfer Protocol (NNTP) was introduced making on-line interactive discussion a reality. Backbone speed was 56 Kbps.

Notes

- **1987:** 1000th RFC and 10,000th host.
- **1988:** Robert Tappan Morris releases the first Internet Worm and CERT was set up in response to this. Backbone speed upgraded to 1.544 Mbps. IRC developed.
- **1989:** 100,000th host. Cuckoo's Egg released by Cliff Stoll telling true story of East German cracker accessing US installations.
- **1990:** ARPAnet ceased to exist and the Internet effectively took its role.
- **1991:** Gopher, a software program for retrieving information from servers on the Internet was made available by the University of Minnesota. The US Government announced that it no longer intended to restrict activity on the Internet to research. This policy shift was sufficient for 12 companies to co-operate and produce CIX. Phil Zimmerman released PGP. Backbone speed upgraded to 44.736 Mbps.
- **1992:** The World Wide Web became a possibility after CERN, in Switzerland, released hypertext. 1,000,000th Host. The author gets his first dialup email account with Demon Internet (**Nov. 1992**).
- **1993:** Mosaic, a software program to browse Web sites written by Marc Andreesen, was released followed by Netscape.
- **1994:** Shopping Malls arrive on the Internet. The UK Treasury goes on line and the first cyberbank opens. The first banner adverts appeared for Zima (a drink) and AT&T.
- **1995:** Traditional dialup services (AOL, CompuServe etc) start to provide dialup services. The Vatican goes on line. A number of Internet companies go public. Netscape leads the field with the largest ever IPO on NASDAQ. DEC launches AltaVista, which claims to index every HTML page there is. Jeff Bezos launches Amazon.com. eBay is launched.
- **1996:** 9,272 organizations find themselves unlisted after the InterNIC drops their name service as a result of not having paid their domain name fee. Various ISPs suffer extended service outages, bringing into question whether they will be able to handle the growing number of users. AOL (19 hours), Netcom (13 hours), AT&T WorldNet (28 hours - email only). China requires users of the Internet to register with the Police. Saudi Arabia restricts use to universities and hospitals. Domain name *tv.com* sold to CNET for US$15,000. Backbone speed upgraded to 622 Mbps.
- **1997:** 2000th RFC. 16 Million hosts. 1,000,000th Domain name registered (March 6th for Bonny View Cottage Furniture Company).
- **1998:** 3,000,000th Domain name registered. US Postal authorities allow purchase of postage stamps on line for downloading and printing. Gigabit Ethernet standard ratified. Google is launched.
- **1999:** First full service bank opens on the Internet (First Internet Bank of Indiana). First forged web page, looking like Bloomberg, raises the shares of a small company by 31% (7th April). Melissa strikes. 5,000,000th Domain name registered. First Cyberwar starts between Serbia and Kosovo. Shawn Fanning Launches Napster — record labels are furious.
- **2000:** 10,000,000th Domain name registered. French Courts require that 'hate' memorabilia for sale on Yahoo's auction site must be removed. Gnutella is launched. ICANN selects new top level domains. Backbone is upgraded to IPv6.
- **2001:** Forwarding email becomes illegal in Australia (Digital Agenda Act). Napster forced to suspend service after legal action. Taliban bans the Internet in Afghanistan. Nimda released on the Internet.
- **2002:** Distributed denial of Service attack hits 13 DNS root servers, causing national security concerns.

Notes

- **2003:** The first official Swiss online election takes place in Anières (**7 Jan**), SQL Slammer (goes round the world in 10 minutes and takes out 3 of the 13 DNS Servers). Followed by SoBig.F (**19 Aug**) and Blaster (**11 Aug**).
- **2004:** Lycos Europe releases a screen saver to help fight spam by keeping spam servers busy with requests (**1 Dec**). The service is discontinued within a few days after backbone providers block access to the download site and the service causes some servers to crash.

1.2 Defining Network

A network consists of two or more computers that are linked in order to share resources (such as printers and CD-ROMs), exchange files or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites or infrared light beams.

The term of 'computer network' means an *interconnected* collection of *autonomous* computers.

(a) Two computers are said to be interconnected if they are able to exchange information.

(b) The requirement for computers to be autonomous excludes from our definition systems in which there is a clear master/slave relation.

The key difference between a computer network and a distributed system:

- In a distributed system, the existence of multiple autonomous computers is *transparent* to the user. A distributed system looks like a virtual uni-processor to its users.
- With a network, a user must *explicitly* do the followings:
  - log onto one machine (e.g., *rlogin*),
  - submit jobs remotely (e.g., *rsh*),
  - move files around (e.g., *rcp, ftp, uucp*), and
  - generally handle all the network management personally.

In effect, a distributed system is a special case of a network, one whose software gives it a high degree of cohesiveness and transparency.

1.3 Characteristics of Computer Network

The primary purpose of a computer network is to share resources:

(a) You can play a CD music from one computer while sitting on another computer.

(b) You may have a computer with a CD writer or a backup system but the other computer does not have it; In this case, you can burn CDs or make backups on a computer that has one of these but using data from a computer that does not have a CD writer or a backup system.

(c) You may have a computer that does not have a DVD player. In this case, you can place a movie DVD on the computer that has a DVD player, and then view the movie on a computer that lacks a DVD player.

(d) You can connect a printer (or a scanner or a fax machine) to one computer and let other computers of the network print (or scan, or fax) to that printer (or scanner, or fax machine).

(e) You can place a CD with pictures on one computer and let other computers access those pictures.

Notes

You can create files and store them in one computer, then access those files from the other computer(s) connected to it.

1.4 Networking Goals

(a) The main goal of networking is **Resource sharing**, and it is to make all the programs, data and equipment available to anyone on the network without the regard to the physical location of the resource and the user.

(b) A second goal is to provide **high reliability** by having alternative sources of supply. For example, all files could be replicated on two or three machines, so if one of them is unavailable, the other copies could be available.

(c) Another goal is **saving money.** Small computers have a much better price/performance ratio than larger ones. Mainframes are roughly a factor of ten times faster than the fastest single chip microprocessors, but they cost thousand times more. This imbalance has caused many system designers to build systems consisting of powerful personal computers, one per user, with data kept on one or more shared **file server** machines. This goal leads to networks with many computers located in the same building. Such a network is called a **LAN (local area network).**

(d) Another closely related goal is to increase the systems performance as the work load increases by just adding more processors. With central mainframes, when the system is full, it must be replaced by a larger one, usually at great expense and with even greater disruption to the users.

(e) Computer networks provide a powerful communication medium. A file that has been updated/modified on a network can be seen by the other users on the network immediately.

Self Assessment

Fill in the blanks:

1. The main goal of networking is ……..
2. In a distributed system, the existence of multiple autonomous computers is…… to the user.
3. The computers on a …….. may be linked through cables, telephone lines, radio waves, satellites or infrared light beams.
4. You can create files and store them in one computer, then …… those files from the other computer(s) connected to it.
5. A …….. system is a special case of a network, one whose software gives it a high degree of cohesiveness and transparency.

1.5 Network Hardware

There are two important dimensions for classifying networks — **transmission technology** and **scale**.

Transmission technology can be classified into two types:

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

Notes

(a) **Broadcast networks:** These networks have a single communication channel shared by all the machines on the network. They work as follows:

- All the others receive packets sent by any machine.
- An address field within the **packet** specifies for whom it is intended.
- Upon receiving a packet, a machine checks the address field. If it is intended for itself, it processes the packet; otherwise, it is just ignored.

It is also possible to address all **broadcasting** or multicasting a subset of the machines. A common scheme:

(i) The address consisting of all 1 bits is reserved for broadcast.

(ii) All addresses with the high-order bit set to 1 are reserved for multicasting.

(iii) The remaining addresses bits form a bit map corresponding to groups.

(iv) Each machine can **subscribe** to any or all of the groups.

(b) **Point-to-point** networks consist of many connections between individual pairs of machines.

Multiple routes and intermediate machines may exist between a pair of machines; so routing algorithms play an important role here.

Notes A general rule (with many exceptions): smaller and localized networks tend to use broadcasting, whereas larger networks usually are point-to-point.

An alternative criterion for classifying networks is their scale, which is as follows:

1.5.1 Local Area Networks(LAN)

Three distinguishable characteristics for LANs:

(a) **Size:** usually a diameter of not more than a few kilometers, with bounded and known worst-case transmission time, making special design and simple management possible.

(b) **Transmission technology:** usually a shared cable running at speeds of 10 to 100 Mbps (and even higher), with delay of tens of microseconds and few errors.

Allocation of the shared channel:

- Each machine is *statically* allocated a time slot to transmit, and gets its turn by round robin.
- Each machine is *dynamically* allocated a time slot on demand.
- Centralized method uses an arbitration unit to determine who goes next.
- Decentralized method allows each machine to decide for itself.

1.5.2 Metropolitan Area Networks(MAN)

MAN is a bigger version of a LAN and uses similar technology. It uses one or two cables but does not contain switching elements. It covers an entire city and may be related to the local cable TV network.

A MAN standard - DQDB (Distributed Queue Dual Bus) IEEE 802.6.

(a) Two unidirectional buses.

Notes

(b) Each bus has a head-end, which initiates transmission activity.

(c) Traffic to the right uses the upper bus.

(d) Traffic to the left uses the lower bus.

1.5.3 Wide Area Networks(WAN)

A WAN spans a large area, often a country or continent. A WAN consists of two parts:

(a) **Application part:** Machines for running user programs are called **hosts**.

(b) **Communication part:** The hosts are connected by the **communication subnet**, or just **subnet**, whose job is to carry messages from host to host.

The subnet consists of two components:

- Transmission lines (**circuits, channels** or **trunks**) move bits between machines.
- Switching elements (**routers**) are specialized computers used to connect two or more transmission lines.

Main Characters

(i) A WAN contains numerous cables or telephone lines, each one connecting a pair of routers.

(ii) For those without direct connection, communication takes place indirectly via other routers.

(iii) When a message (a **packet**) is sent from one router to another, it is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded.

Did u know? A subnet using this principle is called point-to-point, store-and-forward or packet-switched subnet.

WANs may also use broadcast channels, such as satellites or ground radio systems.

1.5.4 Wireless Networks

Mobile computers, such notebook computers and Personal Digital Assistants (PDSs), are the fastest-growing segment of the computer industry.

Applications using wireless networks:

(a) Portable offices which allow people to send and receive phone calls, faxes and emails, to read remote files or login remote machines, etc., and to do this from land, sea or air.

(b) Of great value to fleets of trucks, taxis and repair-persons for keeping in contact with home.

(c) Important to rescue workers at disaster sites and to the military.

Notes Wireless networking and mobile computing are related but not identical, It is possible to have different combinations of wired and wireless networking.

Notes

1.5.5 Internetworks

A collection of interconnected networks is called an **internetwork** or just **Internet**.

The **Internet** refers to a specific worldwide Internet that is widely used to connect universities, government offices, companies and private individuals.

1.6 Uses of Computer Networks

There are many uses of computer network. Depending upon the users' network has the following uses.

1.6.1 Network for Companies

Resource Sharing: A network is needed because of the desire to make all programs, data, and equipment available to anyone on the network without regard to the physical location of the resource and the user. Load sharing is another aspect of resource sharing.

High Reliability: A network may have alternative sources of supply (e.g., replicated files, multiple CPUs, etc.). In case of one resource failure, the others could be used and the system continues to operate at reduced performance. This is a very important property for military, banking, air traffic control and many other applications.

Saving Money: A network may consist of many powerful small computers, one per user, with data kept on one or more shared **file server** machines, which offers a much better price/ performance ratio than mainframes.

Scalability: The ability to increase system performance gradually by adding more processors (**incremental upgrade**).

Powerful Communication Medium: Networks make cooperation among far-flung groups of people easy where it previously had been impossible.

In the long run, the use of networks to enhance **human-to-human** communication may prove more important than technical goals such as improved reliability.

CSCW (Computer-Supported Cooperative Work) is a rapidly expanding multidisciplinary area based on communication networks.

1.6.2 Networks for People

Starting in the 1990s, computer networks began to start delivering services to private individuals at home.

Access to Remote Information

(a) Home reservations for airplanes, trains, hotels, restaurants, theaters and so on, anywhere in the world with instant confirmation.

(b) Home banking and shopping.

(c) On-line and personalized electronic newspapers, journals and libraries.

(d) Access to WWW (World Wide Web) which contains information about many topics - too many to mention!

All these applications involve interactions between a person and a remote database.

Notes

Person-to-person communication: The 21st Century's answer to the 19th Century's telephone.

- Electronic mails or **emails** for everyone. Emails may contain digitized voice, pictures, moving TV and video images (and even smell!).
- Worldwide newsgroups for the population at large, and cover every conceivable topics.
- Real-time CSCW systems, such as **videoconferencing** and **virtual meeting** environments, allow remote users to communicate with no delay, possibly seeing and hearing each others as well.

It is sometime said that transportation and communication are having a race, and whichever one wins will make the other obsolete.

Interactive entertainment is a huge and growing industry.

(i) **Video on demand** (the killer application): The user can select any movie or TV program ever made, in any country, and have it displayed on his screen instantly.

(ii) **Interactive films:** The user may choose alternative scenarios for the story direction.

(iii) **Live and interactive TV:** Audience may participate in quiz shows and so on.

(iv) **Multiperson real-time games** (maybe the alternative killer application): Hide-and-seek, flight simulators, etc.

If done with goggles and 3-dimensional real-time, photographic-quality moving images, we have a kind of worldwide shared **virtual reality**.

The ability to merge information, communication and entertainment will surely give rise to a massive new industry based on computer networking.

The information revolution may change society as much as the Industrial Revolution did.

Task List the main difference between LAN, WAN and MAN networks in a tabular format.

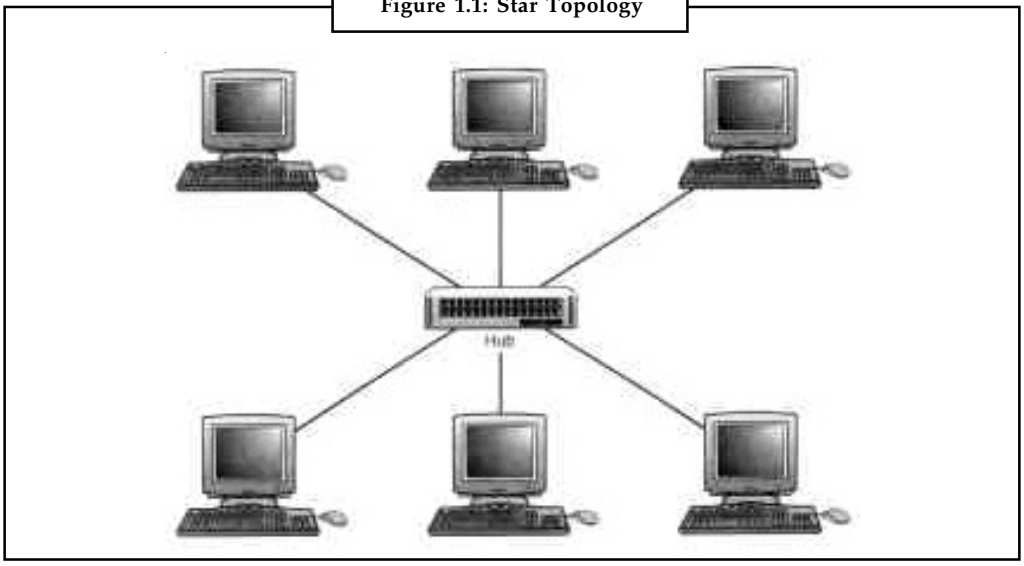
1.7 Network Topologies

A network topology is the basic design of a computer network. It is very much like a map of a road. It details how key network components such as nodes and links are interconnected. A network's topology is comparable to the blueprints of a new home in which components such as the electrical system, heating and air conditioning system, and plumbing are integrated into the overall design. Taken from the Greek work "Topos" meaning "Place," Topology, in relation to networking, describes the configuration of the network; including the location of the workstations and wiring connections. Basically it provides a definition of the components of a Local Area Network (LAN). A topology, which is a pattern of interconnections among nodes, influences a network's cost and performance. There are three primary types of network topologies which refer to the physical and logical layout of the Network cabling. They are:

1. ***Star Topology:*** All devices connected with a Star setup communicate through a central Hub by cable segments. Signals are transmitted and received through the Hub. It is the simplest and the oldest and all the telephone switches are based on this. In a star topology, each network device has a home run of cabling back to a network hub, giving each device a separate connection to the network. So, there can be multiple connections in parallel.

Notes

Figure 1.1: Star Topology



Advantages

- Network administration and error detection is easier because problem is isolated to central node.
- Networks runs even if one host fails.
- Expansion becomes easier and scalability of the network increases.
- More suited for larger networks.

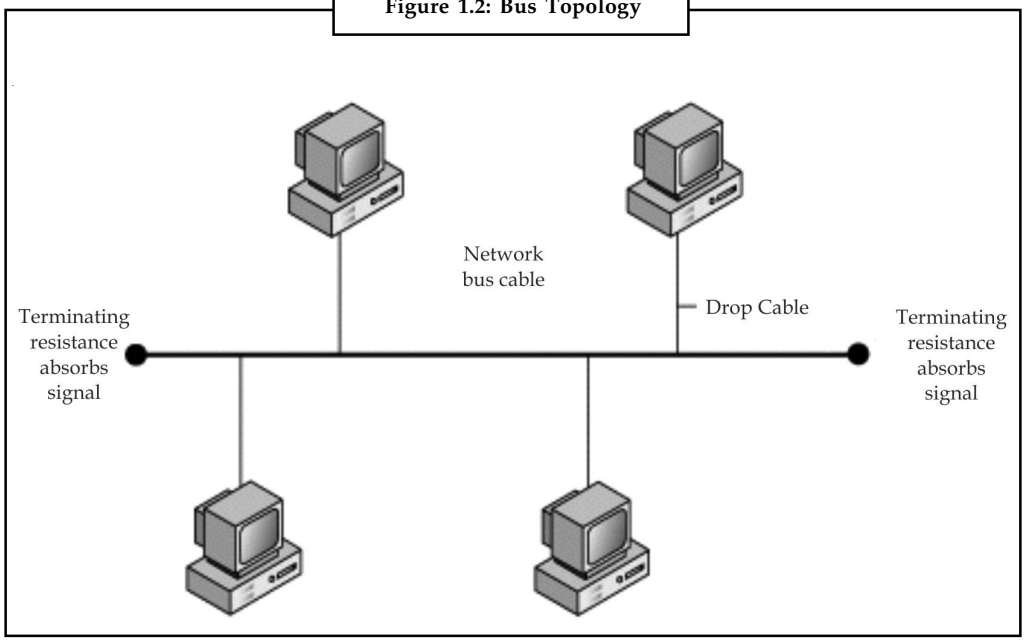
Disadvantages

- Broadcasting and multicasting is not easy because some extra functionality needs to be provided to the central hub.
- If the central node fails, the whole network goes down; thus making the switch some kind of a bottleneck.
- Installation costs are high because each node needs to be connected to the central switch.

2. ***Bus Topology:*** The simplest and one of the most common of all topologies, Bus consists of a single cable, called a Backbone that connects all workstations on the network using a single line. All transmissions must pass through each of the connected devices to complete the desired request. Each workstation has its own individual signal that identifies it and allows for the requested data to be returned to the correct originator. In the Bus Network, messages are sent in both directions from a single point and are read by the node (computer or peripheral on the network) identified by the code with the message. Most Local Area Networks (LANs) are Bus Networks because the network will continue to function even if one computer is down. This topology works equally well for either peer to peer or client server.

Notes

Figure 1.2: Bus Topology



The purpose of the terminators at either end of the network is to stop the signal being reflected back.

Advantages

- Broadcasting and multicasting is much simpler.
- Network is redundant in the sense that failure of one node doesn't effect the network. The other part may still function properly.
- Least expensive since less amount of cabling is required and no network switches are required.
- Good for smaller networks not requiring higher speeds.

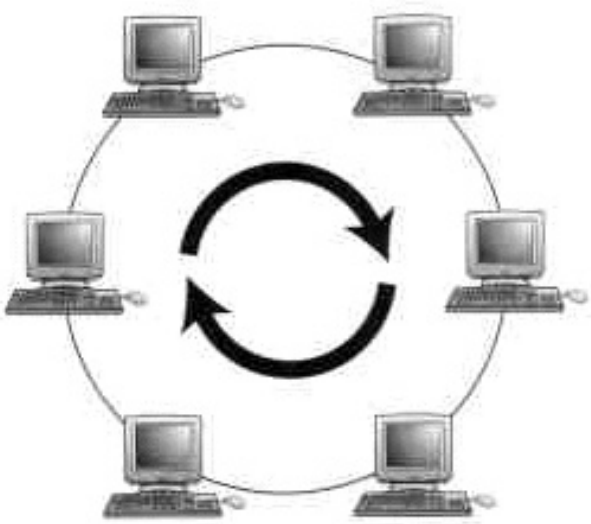
Disadvantages

- Trouble shooting and error detection becomes a problem because, logically, all nodes are equal.
- Less secure because sniffing is easier.
- Limited in size and speed.

3. ***Ring Topology:*** All the nodes in a Ring Network are connected in a closed circle of cable. Messages that are transmitted travel around the ring until they reach the computer that they are addressed to, the signal being refreshed by each node. In a ring topology, the network signal is passed through each network card of each device and passed on to the next device. Each device processes and retransmits the signal, so it is capable of supporting many devices in a somewhat slow but very orderly fashion. There is a very nice feature that everybody gets a chance to send a packet and it is guaranteed that every node gets to send a packet in a finite amount of time.

Notes

Figure 1.3: Ring Topology



Advantages

- Broadcasting and multicasting is simple since you just need to send out one message.
- Less expensive since less cable footage is required.
- It is guaranteed that each host will be able to transmit within a finite time interval.
- Very orderly network where every device has access to the token and the opportunity to transmit.
- Performs better than a star network under heavy network load.

Disadvantages

- Failure of one node brings the whole network down.
- Error detection and network administration becomes difficult.
- Moves, adds and changes of devices can effect the network.
- It is slower than star topology under normal load.

Generally, bus architecture is preferred over the other topologies – of course, this is a very subjective opinion and the final design depends on the requirements of the network more than anything else. Lately, most networks are shifting towards the star topology. Ideally we would like to design networks, which physically resemble the star topology, but behave like bus or ring topology.

Self Assessment

State whether the following statements are true or false:

6. A topology, which is a pattern of interconnections among nodes, influences a network's cost and performance.
7. There are Five primary types of network topologies which refer to the physical and logical layout of the Network cabling.

Notes

8. Bus is the simplest and the oldest and all the telephone switches are based on this.
9. Bus consists of a single cable, called a Backbone that connects all workstations on the network using a single line.
10. The purpose of the terminators at either end of the network is to stop the signal being reflected back.

1.8 Summary

- A network consists of two or more computers that are linked in order to share resources (such as printers and CD-ROMs), exchange files or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites or infrared light beams.
- The primary purpose of a computer network is to share resources. The main goal of networking is **Resource sharing.** A second goal is to provide **high reliability** by having alternative sources of supply. Another goal is **saving money.** Another closely related goal is to increase the systems performance as the work load increases by just adding more processors. With central mainframes, when the system is full, it must be replaced by a larger one, usually at great expense and with even greater disruption to the users. Computer networks provide a powerful communication medium.
- There are two important dimensions for classifying networks — **transmission technology** and **scale**.
- Transmission technology can be classified into two types:
  1. Broadcast networks.
  2. Point-to-point networks.
- **Broadcast networks:** These networks have a single communication channel shared by all the machines on the network.
- **Point-to-point** networks consist of many connections between individual pairs of machines. Multiple routes and intermediate machines may exist between a pair of machines; so routing algorithms play an important role here.
- A collection of interconnected networks is called an **internetwork** or just **Internet**. The **Internet** refers to a specific worldwide Internet that is widely used to connect universities, government offices, companies and private individuals.
- A network topology is the basic design of a computer network. It details how key network components such as nodes and links are interconnected.
- There are three primary types of network topologies which refer to the physical and logical layout of the Network cabling. They are star, ring and bus topology.

1.9 Keywords

Archive: A computer site advertises and stores a large amount of public domain, shareware software and documentation.

Broadcast Networks: They have a single communication channel, which is shared by all the computers on the network and therefore, any message transmitted by a computer on the network is received by all the computers connected to the channel.

Notes

Error Control: The receiving end after completion of receiving the information must also be capable of dealing with and recognizing the corruption.

Local Area Network: A LAN is a form of local (limited distance), shared packet network for computer communications.

Metropolitan Area Network: In MAN, different LANs are connected through a local telephone exchange using one or two cables but not switching elements.

Service Primitives: The primitives enable the service provider to perform some action or report on an action taken by a peer entity.

Wide Area Network: A WAN may be defined as a data communications network that covers a relatively broad geographic area to connect LANs together between different cities with the help of transmission facilities provided by common carriers, such as telephone companies.

1.10 Review Questions

1. What are the major factors that have made the use of computer networks as an integral part of the business?
2. How are computer networks classified? Mention the some of the important reasons for the classification of computer networks.
3. How is LAN characterized? Explain.
4. What are the different technologies available for implementing WAN?
5. What is WAN? How does it differ from LANs and MANs? Give at least two examples of popular WANs.

Answers: Self Assessment

1.	Resource sharing	2.	transparent
3.	network	4.	access
5.	distributed	6.	True
7.	False	8.	False
9.	True	10.	True

1.11 Further Readings

Books

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall

Behrouz A. Forouzan and Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies

Burton, Bill, *Remote Access for Cisco Networks*, McGraw-Hill Osborne Media McGraw-Hill Osborne Media

Rajneesh Agrawal and Bharat Bhushan Tiwari, *Computer Networks and Internet*, Vikas Publication

Unit 2: Network Software

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss concept of process network software and the significance of layering the communication process and related design issues for the layers
- Describe different technologies involved in defining the network hardware
- Explain what are the reference models for computer networks and how they are related with the OSI reference model

Introduction

The development of computer networks took place in gradual manner and is built in a highly structured way. They are designed in such a way so that the network architecture and structure could reduce the design complexity and enable the system designer to scale up and upgrade the networks.

2.1 Network Architecture

Network architecture defines the communications products and services, which ensure that the various components can work together. In the early days of data communication systems, the majority of communications were between the DTE and the host computer. Therefore, transmission control procedures were alone enough as communication protocols. However, recent computer systems link with other systems to form a network, resulting in a situation where in different protocols serving different purposes are required. Hence, the network

Notes

architecture represents a systemization of the various kinds of protocols needed to build a network.

Computer manufacturers have developed different protocols as needed. This means that each type of computer needed to support different protocols. This also necessitated large development and maintenance costs. All computer manufacturers, therefore worked together to standardize and systemize protocols to link their models and thereby reduce the development and maintenance costs. This was how each manufacturer built own network architecture. Since the concept of the network architecture was first introduced to connect the computers of the same manufacture, the process has become easier. However, from user's perspective, the ideal form of network architecture is one, which enables machines of all manufacturers to connect to each other. Therefore, the need of standardization of network architecture arose.

2.2 Layering the Communications Process

Open Systems Interconnection (OSI) was set up as an international standard for network architecture to reduce their design complexity. Hence, most of the networks are organized as a series of layers or levels. Layering the communications process means breaking it down the communication process into smaller and easier to handle interdependent categories, with each solving an important and somehow distinct aspect of the data exchange process. Each layer has to offer specified services to the higher layers. Thus, layer on one computer carries on a conversation with corresponding layer on another computer in the network. The rules and conventions used in such communications are collectively known as the layer protocol. The entities comprising the corresponding layers on different computers are called peers, which communicate using the protocol. Between each pair of adjacent layers an interface exists that defines primitive operations and services the lower layer offers to the upper one.

The International Organization for Standardization (ISO) took the initiative in setting up OSI. OSI has two meanings. It refers to:

- Protocols that are authorized by ISO
- OSI basic reference model

OSI reference model divides the required functions of the network architecture into several layers and defines the function of each layer.

The group of layers and protocols is called the network architecture. These groups of layers are provided with enough information to allow a software/hardware implementation, which correctly obeys the appropriate protocol.

The objective of this detail is to develop an understanding of the complexity and sophistication that this technology has achieved, in addition to developing the concept for the inner workings of the various components that contribute to the data communications process. The details of the implementation and the specification of the interfaces are never part of the architecture because they are not visible from the outside.

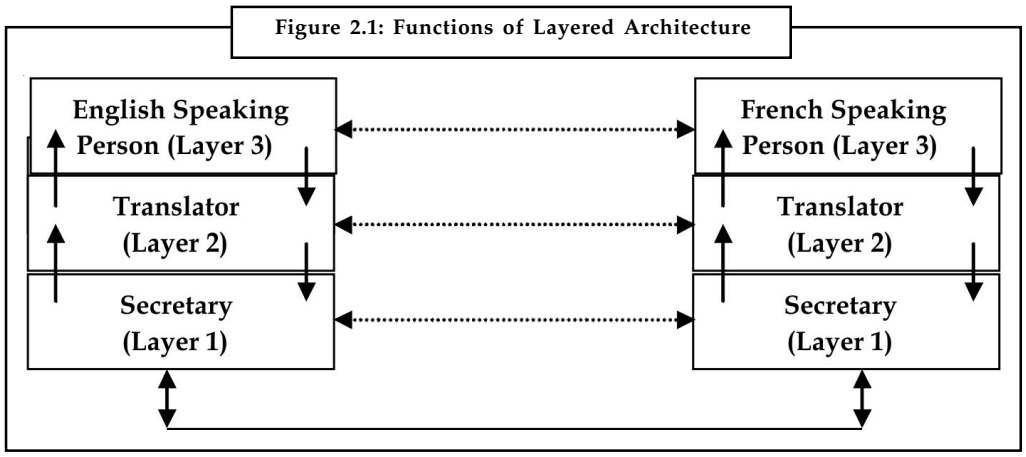
The functions of layered architecture may be comprehended with an example of conservations taking place between two persons with different language of communication, say, English and French. A three-layered architecture as shown in Figure 2.1 explains the concept. Dotted lines from peers to peers indicate virtual connections.

- Two persons (peer processes in layer 3), one speaking English and the other speaking French, want to communicate.
- They are using a translator (peer processes at layer 2).
- A secretary (peer processes at layer 1) facilitates each translator for message transmission.

Notes

- The English person passes his message in English to his translator, who translates it into French or other language, depending on the layer 2 protocol.

Figure 2.1: Functions of Layered Architecture



- The translator then passes the message to secretary at layer 1 to transmit the message by telephone, email, or some other means, depending on layer 1 protocol.
- When the message reaches the destination, the peer secretary passes the message to the peer translator, who translates it into French and passed across the 2/3 interface to French speaking person.
- Thus an effective conversation takes place between two persons, not understanding each other's language. Similarly, two computers on different networks communicate with each other.

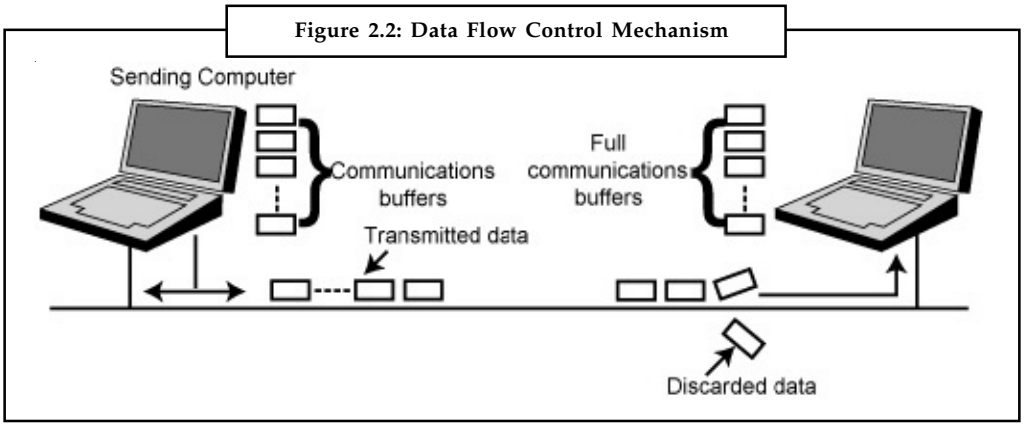
2.2.1 Design Issues for the Layers

In information exchange between computers, communication processes need to have the following to accomplish these aspects of exchange process:

- ***Physical Data Encoding:*** The information exchanged between two computers is physically carried by means of electrical signals assuming certain coding methods. For two computers to reliably exchange data, they must have a compatible implementation of encoding and interpreting data carrying electrical signals.
- ***Multiplexing:*** This uses the same connection for multiple, unrelated conversations. For example, a few physical circuits are used for all virtual connections.
- ***Transmission Media:*** This concern deals with the type of media used (fiber, copper, wireless, and so on), which is dictated by the desirable bandwidth, immunity to noise, and attenuation properties. These factors affect the maximum-allowable media length while still achieving a desirable level of guaranteed data transmission.
- ***Flow Control:*** Data communication process allocates memory resources, commonly known as communications buffers for the sake of transmission and reception of data. It keeps a fast sender from swamping a slow receiver with data. Some kind of feedback from receiver is needed. A proper data flow control technique desires that the receiving process in transmission of data should send a "stop sending" signal to the sending computer whenever it does not have resources to cope with the rate at which data is being transmitted. On the other hand, when receiving device has sufficient resources available, it should send a "resume sending" signal. The resources available at receiving end to cope up with the sending computer are buffers availability. Figure 2.2 shows the mechanism of data flow control.

Notes

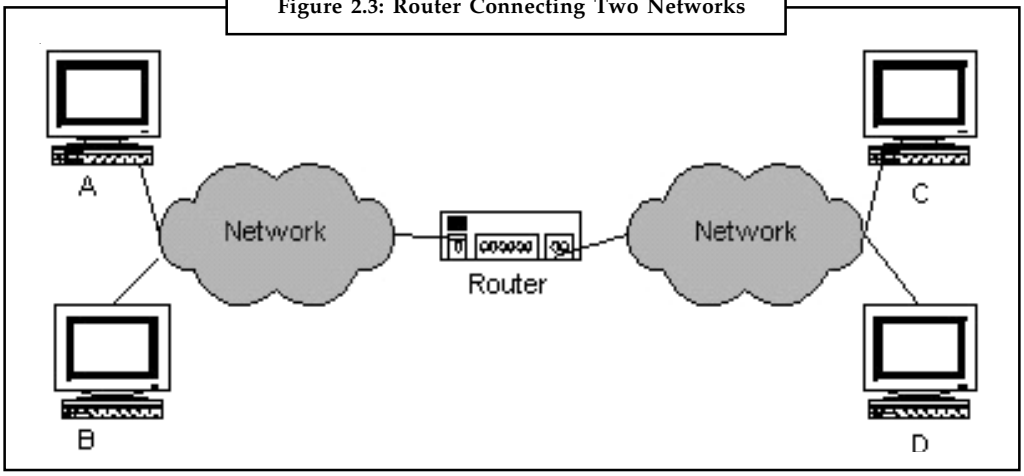
Figure 2.2: Data Flow Control Mechanism



Receiving computer must be capable of distinguishing between information carrying signal and mere noise.

- ***A mechanism for identifying senders and receivers:*** Some form of addressing for both machines and processes to detect whether the information carrying signal is intended for itself or some other computer on the network, or a broadcast (a message that is intended for all computers on the network).
- ***Error control:*** The receiving end after completion of receiving the information must also be capable of dealing with and recognizing the corruption, if any, this corruption could be in the form of noise or electromagnetic interference. Both sides must have the same error-detecting and error-correcting codes. In addition to this, some mechanism is needed to point out which messages have been correctly received and which have not.
- ***Logical channels:*** Protocols should provide at least two logical channels per connection.
- ***Message sequencing or ordering:*** Message are broken into pieces and are numbered before transmission. There should be a mechanism to put them back in order at the receiving end. These packets may take different routes to reach at destination computer and therefore not necessarily be in order.
- ***Routing:*** The routing approach calls on the implementation of various cooperative processes, in both routers and servers, whose main concern is to allow for the intelligent delivery of data to its ultimate destination. Data exchange can take place between any two workstations, whether or not both belong to same network as shown in Figure 2.3.

Figure 2.3: Router Connecting Two Networks



Notes

- ***Inter-process dialog control:*** When two applications engage in the exchange of data, they establish a session between them. Consequently, a need arises to control the flow and the direction of data flow between them for the duration of the session. Depending on the nature of the involved applications, the dialog type may be full duplex, half-duplex, or simplex mode of communication.
- ***Session Recovery:*** Another application-oriented concern is the capability to reliably recover from failures at a minimum cost. This can be achieved by providing a check mechanism, which enables the resumption of activities since the last checkpoint. Check pointing circumvents this requirement by re-transmitting only the affected files, saving time and bandwidth.
- ***Presentation Problems:*** Whenever two or more communicating applications run on different platforms, another concern arises about the differences in the syntax of the data they exchange. Resolving these differences requires an additional process. Good examples of presentation problems are the existing incompatibilities between the ASCII and EBCDIC standards of character encoding, terminal emulation incompatibilities, and incompatibilities due to data encryption techniques.

Self Assessment

State whether the following statements are true or false:

1. The entities comprising the corresponding layers on different computers are called clients.
2. The International Organization for Standardization (ISO) took the initiative in setting up OSI.
3. Data communication process allocates memory resources, commonly known as communications buffers for the sake of transmission and reception of data.
4. The information exchanged between two computers is physically carried by means of chemical signals assuming certain coding methods.
5. OSI reference model divides the required functions of the network architecture into five layers and defines the function of each layer.

2.3 Interfaces and Services

Each layer provides services to the immediate layer above it. There are some associated terms, which are used frequently:

- ***Entities:*** They are active elements. For example, processes, I/O chips, etc. in each layer.
- ***Peer entities:*** They are entities in the same layer on different computers.
- ***Service provider:*** This function of layer provides certain services.
- ***Service user:*** This function of layer uses certain services.
- ***SAP (Service Access Points):*** It is the point from where services can be accessed. Each SAP has a unique address.

Connection-oriented and Connectionless Services

Connection-oriented Service is similar to the telephone system where a dedicated channel is established between sender and receiver before transmission. They are suitable for

Notes

communicating for a long time between senders and receivers. However, they are notable for wastage of bandwidth.

In connection-oriented service, each packet is associated with a source/destination connection. These packets are routed along the same path, known as a virtual circuit.

Connectionless service adopts the mechanism of the postal system. Each message is broken into packets and enclosed in an envelope. The envelope contains the full address. The envelope is then routed independently. The order of the packets is not guaranteed. They are suitable for sending short messages and notable to provide bandwidths in short time intervals.

In connectionless service, a router treats each packet individually. The packets are routed through different paths through the network according to the decisions made by routers.

Quality of Service

Reliable services guarantee the delivery of data, which is implemented by acknowledgements. However, this introduces overheads and thus reducing the efficiency. In case of file transfer, we need a reliable connection-oriented service while an unreliable connection-oriented service is appropriate for digitized voice traffic.

Example: Registered e-mails are example of reliable connectionless service with acknowledgement while an unreliable connectionless service without acknowledgement is appropriate for junk e-mail. They have a high probability of arrival but no guarantee. In the client-server model, the request-reply command is another example of connectionless service.

Service Primitives

The Connection-oriented or connectionless service is specified by a set of primitives available to a service user to interact with the service provider. These primitives enable the service provider to perform some action or report on an action taken by a peer entity. Primitives have parameters to define conditions. For example, *request* and *response* primitives, the sender and the receiver may negotiate some conditions like message size. They are part of the protocol. A confirmed service is defined with a request, an indication, a response, and a confirm primitives. An unconfirmed service has a *request* and an *indication* primitive only.

Relationship of Services to Protocols

Services and protocols are distinct concepts and are important to establish and release connections between sender and receiver.

A service is defined as a set of primitives that are nothing but actions or operations. They are provided to the upper layer by an immediate lower layer. It defines only nature of actions to perform by the layer upper to the service-initiating layer.

A protocol defines set of rules to describe the format and meaning of the frames, packets or messages that are exchanged by the peer entities within the same layer. Entities use protocols to implement their service definitions.

Task What do you understand by layered protocol? Explain, why protocols are layered?

2.4 Reference Models

Notes

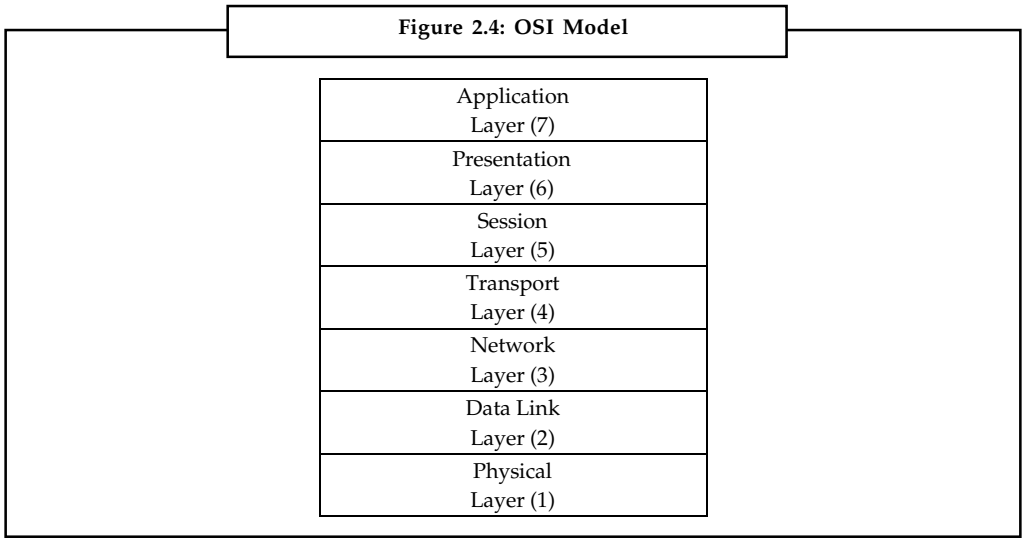
2.4.1 Open Systems Interconnection (OSI) Reference Model

Now you will study the concept of OSI Reference Model.

The International Standardization Organization (ISO) developed the OSI model of data communications in 1984. OSI specifies a seven-layer model as shown in Figure 2.4. In addition to forming the basis of the ongoing development of OSI's own protocols, it is used by the industry as the frame of reference when describing protocol architectures and functional characteristics.

The ISO, in an effort to encourage open networks, developed an open systems interconnect reference model. The model logically groups the functions and sets rules, called protocols, necessary to establish and conduct communication between two or more parties. The model consists of seven functions, often referred to as layers as shown in Figure 2.4.

Figure 2.4: OSI Model



The last three layers are mainly concerned with the organization of terminal software and are not directly the concern of communications engineers. The transport layer is the one, which links the communication processes to this software oriented protocols. The transmitting device uses the top layer, at which point the data is placed into a packet, prepended by a header. The data and header, known collectively as a Protocol Data Unit (PDU), are handled by each successively lower layer as the data works its way across the network to the receiving node. At the receiving node, the data works its way up the layered model, successively higher layers strip off the header information.

Notes The basic philosophy of the 7-layer model is that each layer may be defined independently of every other layer. Thus from the user point of view, interchange takes effect across each operation passes down through the layers of the model until data interchange is affected through the physical connection.

The underlying principles and guidelines that were applied to arrive at the seven layers are given below:

1. A layer is created at different level of abstraction.

Notes

2. Each layer is assigned to perform well-defined functions.
3. The function of each layer is based on internationally standardized protocols.
4. The layer boundaries are chosen to minimize the information flow across the interfaces.
5. The number of layers is kept large enough that distinct functions have different layers. They are also kept small enough that the architecture does not become unwieldy.

Physical Layer (Layer 1)

This layer describes the physical media or communication channel over which the bit stream is to be transmitted with the objective that when sending side sends a 1 bit, it is received by the receiving side as a 1 bit, not as a 0 bit. Hence, it defines the electrical and mechanical aspects of interfacing to a physical medium for transmitting data, as well as setting up, maintaining, and disconnecting physical links. It is primarily concerned with moving bits from one node to next over the physical link. The issues concerning with the physical layer involve amplitude of the pulses to define 1 and 0 level, width of the pulse in microseconds, types and mode of communications, establishment and breaking of connections at the time of communications, types of connectors, etc.

It accepts data from the Data Link layer in bit streams for the subsequent transmission over the physical medium. At this layer, the mechanical (connector type), electrical (voltage levels), functional (ping assignments), and procedural (ha*n*dshake) characteristics are defined. RS-232C/D is an example of a physical layer definition.

Data Link Layer (Layer 2)

It takes the bits that are received by the physical layer and detects error. This establishes an error free communications path between network nodes over the physical channel, frames messages for transmission, checks integrity of received messages, manages access to and use of the channel, ensures proper sequence of transmitted data. Hence, this layer is responsible for the reliable transfer of data across the Physical link. Its responsibilities include such functions as data flow control, breaking the input data, frame formatting, transmission of the frames sequentially, error detection, and link management, etc. In order to provide a reliable service, it also offers processing of the acknowledgement frames, retransmitting lost or damaged frames, etc.

Did u know? Data link layer is further subdivided into Medium Access (MAC) sub layer to deal with the access control over the shared channel in broadcast networks.

Network Layer (Layer 3)

The network layer comprises software that addresses the PDUs and transports them to the ultimate destination, setting up the appropriate paths between the various nodes. Therefore, the main objective of this layer is to control the operation of the subnet. It is the layer, which provides Internet Protocol (IP) to use it. It is mainly responsible for providing routing services from source to destination across the Internet. In doing so, it allows *internetworking* among heterogeneous networks using different addressing, length of packet, protocols, etc. The routing may be static or dynamic. Network layer also plays important role in congestion control.

It also shields the above layers from details about the underlying network (the network topology and road map) and the routing technology that might have been deployed to connect different networks together. In addition to routing, this layer is responsible for establishing and

Notes

maintaining the connection. In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

The next three layers are task oriented and have to do with the operations performed by the user rather than with the network.

Transport Layer (Layer 4)

This layer guarantees the orderly and reliable delivery of data between end systems after accepting data from the session layer. Data is accepted from the Session layer and split up into smaller units, if needed. Session layer passes the data to the Network layer and ensures that the packets arrive correctly at the receiving side.

Basically, it performs connection management based upon the throughput conditions. In normal condition, one network connection corresponds to multiple transport connections. In high throughput condition, one transport connections correspond to multiple network connection. The most popular protocol suite TCP/IP uses this layer. Transport layer also performs additional functions such as data multiplexing and de-multiplexing. This layer divides up a transmitting message into packets and reassembles it at the receiving end. Service offered at this layer includes an error-free point-to-point channel to deliver messages in the order in which they were sent. The transport layer is a true source-to-destination or end-to-end layer. Flow control between hosts is also needed but different from between routers (similar principles will apply to both).

Session Layer (Layer 5)

The session layer is responsible for establishing, maintaining, and arbitrating the dialogs between communicating applications. It also provides enhanced services useful in some applications, for example, remote login, remote file transfer, etc. It is also responsible for the orderly recovery from failures by implementing appropriate check pointing mechanisms.

Presentation Layer (Layer 6)

The presentation layer performs functions related to the syntax and semantics of the information transmitted that include formatting and displaying of received data by terminals and printers. It is concerned with differences in the data syntax used by communicating applications. This layer is responsible for remedying those differences by resorting to mechanisms that transform the local syntax (specific to the platform in question) to a common one for the purpose of data exchange.

For example, it performs encoding of data in a standard agreed upon way to facilitate information exchange among heterogeneous systems using different codes for strings, for example, conversion between ASCII and EBCDIC character codes. It facilitates data compression for reducing the number of bits to be transmitted and encrypts data for privacy and authentication, if necessary.

Application Layer (Layer 7)

The application layer provides support services for user and application tasks. It determines how the user will use the data network. It allows the user to use the network. For example, it provides network-based services to the end user.

Examples of network services are distributed databases, electronic mail, resource sharing, file transfers, remote file access and network management. This layer defines the nature of the task to be performed.

Notes

2.4.2 TCP/IP Reference Model

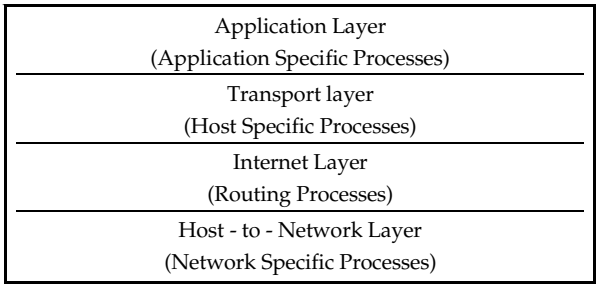
The TCP/IP model is considered the oldest protocol of all computer networks like the ARPANET and its successor Internet. TCP/IP stands for Transmission Control Protocol/Internet Protocol. It was developed with the objective to specify a suite of protocols capable of providing transparent communications interoperability services between computers of all sizes, regardless of the hardware or operating system platforms supporting them. Over the years, TCP/IP has become the most widespread of today's protocols. One reason for TCP/IP's popularity is the public availability of its protocols' specifications. In this sense, TCP/IP can justifiably be considered an open system. Most users rely on TCP/IP for the purpose of file transfers, electronic mail (e-mail), and remote login services.

The TCP/IP model was aimed to connect multiple networks together in a seamless way even in case of breakdown of the subnet hardware. Not only providing seamless communication, but also providing a flexible architecture that should support applications with divergent requirements, ranging from transferring files to real-time speech transmission. These objectives could be achieved because of the inclusion of the research work on packet-switching network to the ARPAnet.

TCP corresponds to the fourth layer of OSI reference model. IP corresponds to the third layer of the same model. TCP provides a connection type service. That is, a logical connection must be established prior to communication to continuously transmit large amount of data with acknowledgement. IP is a connectionless type service and prior to transmission of data, no logical connection is needed.

TCP/IP defines a suite of communications and applications protocols in layer structure, with each layer handling distinct communication services. TCP/IP defines a four-layer model as shown in Figure 2.5 consisting of the internet layer, the transport layer, the application layer and the host-to-network layer. This architecture is based on three sets of interdependent processes, namely, application-specific processes, host-specific processes, and network-specific processes.

Figure 2.5: TCP/IP Communication Architecture



Internet Layer

The packet format and protocol at this layer is called Internet Protocol (IP). IP is a connectionless type service that introduces IP packets into any network. The packets travel independently to the destination. Prior to transmission of data, no logical connection is needed. The TCP/IP Internet layer corresponds to the network layer of the OSI reference model in functionality, as shown in Figure 2.5

Notes

Transport Layer

The transport layer of TCP/IP model corresponds to the transport layer of the OSI reference model. It is represented by two end-to-end protocols namely, TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP is a reliable connection-oriented protocol and UDP is an unreliable connectionless protocol.

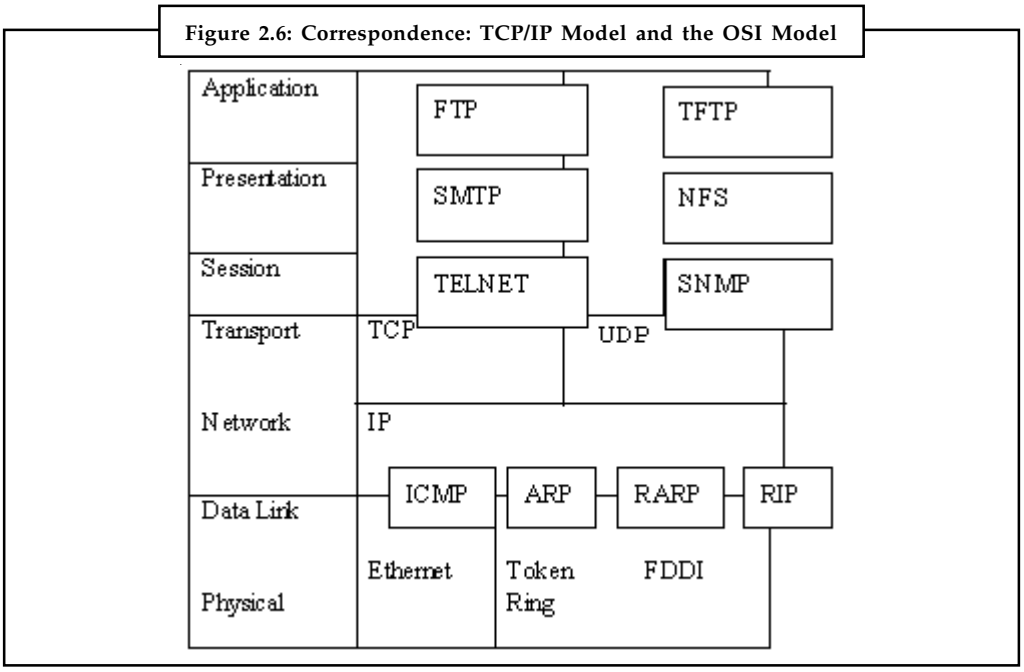
Application Layer

The TCP/IP model was the first of its kind model and therefore did not contain session or presentation layers because of its little use to most of the applications. This layer has all the higher-level protocols, as shown in Figure 2.5.

Host-to-network Layer

The layer below the Internet layer is not defined and varies from host and network to network. The TCP/IP model suggests that the host has to connect to the network using some protocol so it can send IP packets over it.

Figure 2.6: Correspondence: TCP/IP Model and the OSI Model



2.4.3 A Comparison of the OSI and TCP/IP Reference Models

In this section, you will get to know the difference between OSI and TCP/IP Reference Models.

Figure 2.6 shows the similarity between the TCP/IP and OSI reference model. Both the models were developed based on the concept a stack of independent protocols with similar functionality of the layers. In spite of similarity between the two models they also contrast in functionalities provided by services, interfaces and protocols. OSI reference model clearly distinguish them while the TCP/IP model did not explicitly distinguish them. Other differences are:

- The OSI model has seven layers and the TCP/IP model has only four layers.
- The OSI model was developed before the protocols were devised. The TCP/IP model was developed after the development of the protocols.

Notes

- The OSI model has both connection-oriented and connectionless communication in the network layer and connection-oriented communication in the transport layer. The TCP/IP model supports connectionless mode in the Internet layer and both modes in the transport layer.

Self Assessment

Fill in the blanks:

6. The TCP/IP …….. layer corresponds to the network layer of the OSI reference model in functionality.
7. TCP is a …….. protocol and UDP is an unreliable connectionless protocol.
8. OSI reference model divides the required functions of the …….. into several layers and defines the function of each layer.
9. …….. are entities in the same layer on different computers.
10. …….. is the point from where services can be accessed.

2.5 Summary

- The three basic components namely; hardware, protocols (software) and applications (useful software) are mandatory to implement a computer network. It is also explained that the concept of layers is important in networking.
- Each layer with two layers works as the interface and protects the upper layer that each one layer can change with minimum impact on the upper layers. In some cases, this protection is so proficient that an application may not know that it is running on different hardware.
- The OSI network model has seven layers.
- TCP/IP stands for Transmission Control Protocol/Internet Protocol. It was developed with the objective to specify a suite of protocols capable of providing transparent communications interoperability services between computers of all sizes, regardless of the hardware or operating system platforms supporting them.
- Over the years, TCP/IP has become the most widespread of today's protocols. One reason for TCP/IP's popularity is the public availability of its protocols' specifications. In this sense, TCP/IP can justifiably be considered an open system. Most users rely on TCP/IP for the purpose of file transfers, electronic-mail (e-mail), and remote login services.

2.6 Keywords

Internet Protocol: The Internet protocol suite is the set of communications protocols used for the Internet and other similar networks.

Open Systems Interconnection (OSI) Reference Model: The International Standardization Organization (ISO) developed the OSI model of data communications in 1984. OSI specifies a seven-layer model that is used by the industry as the frame of reference when describing protocol architectures and functional characteristics.

TCP/IP: Transmission Control Protocol (TCP) and Internet Protocol (IP) are two distinct network protocols, technically speaking. TCP and IP are so commonly used together; however, that TCP/IP has become standard terminology to refer to either or both of the protocols.

2.7 Review Questions

Notes

1. What are the important design issues for the information exchange among computers?
2. What are the major functions of the network layer in the ISO-OSI model? How the function of packet delivery of network layer is different from data link layer?
3. What is the purpose of layer isolation in the OSI reference model?
4. Why OSI Reference model was widely adopted? What did it make to set itself as a standard for data communication?
5. Highlight the differences between OSI reference model and TCP/IP model.

Answers: Self Assessment

1. False
2. True
3. True
4. False
5. False
6. Internet
7. reliable connection-oriented
8. Network Architecture
9. Peer entities
10. Service access points

2.8 Further Readings

Books

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall

Behrouz A. Forouzan and Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies

Burton, Bill, *Remote Access for Cisco Networks*, McGraw-Hill Osborne Media McGraw-Hill Osborne Media

Rajneesh Agrawal and Bharat Bhushan Tiwari, *Computer Networks and Internet*, Vikas Publication

Notes

Unit 3: Physical Layer

CONTENTS

Objectives

After studying this unit, you will be able to:

- Identify the major types of transmission media
- Describe transmission terms and concepts
- State few advantages and disadvantages of each transmission medium
- Analyze the general properties of each type of bounded transmission media

Introduction

Information has been attached with considerably increased value if it can be conveyed clearly to others. This is a basic principle that is well understood in this information age. The conveyance, or transmission, of information across a distance necessarily involves some form of transmission medium. The selection of physical transmission media that serve to transport the information is critical to its successful conveyance. In interactive communication, the medium can be critical to the message. The transmission of an electrical signal requires the use of a transmission medium, which normally takes the form of a transmission line. There are various ways to transmit the signal. These ways can be broadly categorized into guided and unguided media. The guided media includes all wired media, also referred to as conducted or bounded media. The second category includes all traditional wireless media, also referred to as radiated, or unbounded. In the transmission of signal the data is encoded to energy and then energy is transmitted. Similarly at the receiving end the energy is decoded back to data. This energy can be electrical, light and radio, etc. Therefore this transmitted energy is carried through some sort of medium which depend upon the type of energy being transmitted. The energy in different forms has different properties and therefore cannot be transmitted using the single media. They have different requirements for transmission which may include special hardware for data encoding and connection to transmission medium. Media can be copper and glass as bounded media and air as unbounded media.

3.1 Transmission Concepts and Terms

Notes

Before discussing different kinds of transmission medium, it becomes necessary to know a little about the basic concepts and terminology associated with the transmission of a signal.

- *Frequency Spectrum:*

Table 3.1: Frequency Spectrum

Name of Band	Frequency Range	Wavelength	Usage
Audible	20 Hz–20 kHz	>100Km	Voice
Extremely/Very Low Frequency (ELF/VLF) Radio	3 kHz–30 kHz	100–10 Km	Radio Navigation, Weather, Submarine Communications
Low Frequency (LF) Radio	30 Hz–300 kHz	10–1 Km	Radio Navigation, Maritime Communications
Medium Frequency (MF) Radio	300 kHz–3 MHz	1 Km–100 m	Radio Navigation, AM Radio
High Frequency (HF)	3 MHz–30 MHz	100–10 m	Citizens Band (CB) Radio
Very High Frequency (VHF) Radio	30MHz–300 MHz	10–1 m	Amateur (HAM) Radio, VHF TV, FM Radio
Ultra High Frequency (UHF)	300MHz–3GHz	1 m–10 cm	Microwave, Satellite, UHF TV
Super High Frequency (SHF) Radio	3 GHz–30 GHz	10–1 cm	Microwave, Satellite
Extremely High Frequency (EHF) Radio	30 GHz–300 GHz	1 cm–.1 mm	Microwave, Satellite
Infrared Light	103–105 GHz	300–3µ	Infrared
Visible Light	1013–1015 GHz	1–.3µ	Fiber Optics
X-Rays	1015–1018 GHz	103–107 µ	N/A
Gamma and Cosmic Rays	>1018 GHz	<017 µ	N/A

The symbols in Table 3.1 have the following meanings:

K (Kilo) = 1,000,

M (Mega) = 1,000,000 (1 million),

G (Giga) = 1,000,000 (1 billion)

T (Tera) = 1,000,000,000 (1 trillion)

cm = centimeter (1/100 meter)

mm = millimeter (1/1,000 meter)

µ = micron (1/1,000,000 meter)

In the transmission of data the range of carrier frequencies depends on the nature of the medium and the requirements of the applications supported. Therefore, frequency spectrum may be defined as the range of frequencies being supported by a particular transmission

Notes

medium. The actual range of frequencies supporting a given communication is known as a pass band. These are given in Table 3.1.

- ***Bandwidth:*** In a very general way, we may say that bandwidth is the difference, expressed in Hertz, between the highest and the lowest frequencies of a band. In general, the higher the bandwidth, the more will be the data transmission rate or throughput. It should be noted that bandwidth and data transmission rate are very closely interrelated to each other. Clearly, any transmission system becomes more attractive if the available bandwidth is greater, introduced errors are fewer, and the maximum distance between various network elements (amplifiers, repeaters, and antennae) is greater.
- ***Distances:*** The higher frequency signals offer greater bandwidth; they also generally suffer to a greater extent from signal attenuation than lower frequencies. This fact results in more errors in transmission, unless the amplifiers/repeaters are spaced more closely together. It clearly demonstrates the close and direct relationship between bandwidth, distance, and error performance.

  Bandwidth, in this context, refers to the raw amount of bandwidth the medium supports. Error performance refers to the number or percentage of errors, which are introduced in the process of transmission. Distance refers to the minimum and maximum spatial separation between devices over a link, in the context of a complete, end-to-end circuit.
- ***Propagation delay:*** Propagation delay refers to the length of time required for a signal to travel from transmitter to receiver across a transmission system. While electromagnetic energy travels at roughly the speed of light (30,000 Kms per second) in free space. In contrast, the speed of propagation for twisted pair or coaxial cable is a fraction of this figure. The nature of the transmission system will have considerable impact on the level of propagation delay. In other words, the total length of the circuit directly influences the length of time it takes for the signal to reach the receiver.
- ***Security:*** Security, in the context of transmission systems, addresses the protection of data from interception as it transverses the network. Particularly in the case of data networking, it also is important that access to a remote system and the data resident on it be limited to authorized users; therefore, some method of authentication must be employed in order to verify that the access request is legitimate and authentic.
- ***Resistance to environmental conditions:*** Resistance to environmental conditions applies most especially to wired systems. Twisted pair, coaxial, and fibre optic cables are manipulated physically as they are deployed and reconfigured. Clearly, each has certain physical limits to the amount of bending and twisting (flex strength) it can tolerate, as well as the amount of weight or longitudinal stress it can support (tensile strength), without breaking (break strength). Fibre optic cables are notoriously susceptible in this regard. Cables hung from poles expand and contract with changes in ambient temperature; while glass fibre optic cables expand and contract relatively little, twisted pair copper wire is more expansive.

  The issue of resistance to environmental conditions also applies to airwave systems, as reflective dishes, antennae, and other devices used in microwave, satellite, and infrared technologies must be mounted securely to deal with wind and other forces of nature. Additionally, the towers, walls and roofs on which they are mounted must be constructed and braced properly in order to withstand such forces.
- ***Physical dimensions:*** The physical dimensions of a transmission system must be considered as well. This is especially true, once again, in the case of wired systems. Certainly, the sheer weight of a cable system must be considered as one attempts to deploy it effectively. Additionally, the bulk (diameter) of the cable is of importance, as conduit and raceway

Notes

space often is at a premium. The physical dimensions of airwave systems also must be considered, as the size and weight of the reflective dish and mounting system (e.g., bracket and tower) may require support.

- ***Cost and ease of Installation:*** Cost issues abound in the selection of an appropriate transmission medium. Such issues include the cost of acquisition, deployment, operation, and maintenance (O&M), and upgrade or replacement. Without a lengthy discussion of each cost issue, it is particularly noteworthy to compare the costs of deployment of wired versus wireless media.

  Wired transmission systems require a right-of-way and this should be secured. Wired transmission involves a cost component in the form infrastructure. The infrastructure includes digging of trenches and boring of holes so that cable can be pulled and poles may be mounted. In addition, amplifiers or repeaters may be placed. Such costs are not trivial.

  Unlike wired system, wireless systems require secured right-of-way and antennae. It may be inferred that the deployment of wired systems certainly speak of a set of cost issues that often can be more problematic.

- ***Selection criteria:*** When choosing the most effective transmission media, consider the above mentioned transmission characteristics which are listed below:
  - Bandwidth/Transmission rate
  - Distances
  - Propagation delay
  - Security
  - Resistance to environmental conditions
  - Physical dimensions
  - Cost and ease of installation

Self Assessment

Fill in the blanks:

1. …….. can be broadly categorized into guided and unguided media.
2. The actual range of frequencies supporting a given communication is known as a .....
3. In general, the higher the ……..., the more will be the data transmission rate or throughput.
4. …… refers to the length of time required for a signal to travel from transmitter to receiver across a transmission system.
5. Bandwidth may be defined as the range of ……..assigned to a channel.

3.2 Bounded Media

Bounded media or wired transmission systems employ physical media, which are tangible. Also known as conducted systems, wired media generally employ a metallic or glass conductor which serves to conduct, some form of electromagnetic energy. For example, twisted pair and coaxial cable systems conduct electrical energy, employing a copper medium. Fibre optic systems

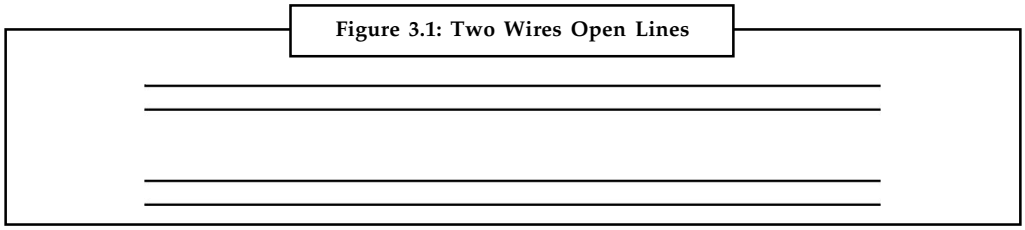
Notes

conduct light or optical energy, generally using a glass conductor. The term bounded or guided media means that the signal is contained within an enclosed physical path. It also refers to the fact that some form of shield, cladding, and/or insulation is employed to bind the signal within the core medium, thereby improving signal strength over a distance and enhancing the performance of the transmission system in the process. Twisted pair (both unshielded and shielded), coaxial and fiber optic cable systems fall into this category.

3.2.1 Twisted Pair (Copper Conductors)

A twisted pair as shown in Figure 3.1 is a pair of copper wires, with diameters of 0.4-0.8 mm, twisted together and wrapped with a plastic coating. The twisting increases the electrical noise immunity, and reduces the error rate of the data transmission. Each conductor is separately insulated by some low smoke and fires retardant substance. Polyethylene, polyvinyl chloride, flouropolymer resin and Teflon are some substances that are used for insulation purposes.

Figure 3.1: Two Wires Open Lines



This twisting process serves to improve the performance of the medium by containing the electromagnetic field within the pair. Thereby, the radiation of electromagnetic energy is reduced and the strength of the signal within the wire is improved over a distance. Clearly, this reduction of radiated energy also serves to minimize the impact on adjacent pairs in a multiple cable configuration. This is especially important in high-bandwidth applications, as higher frequency signals tend to lose power more rapidly over distance. Additionally, the radiated electromagnetic field tends to be greater at higher frequencies, impacting adjacent pairs to a greater extent. Generally speaking, the more twists per foot, the better the performance of the wire.

These are popular for telephone network. The energy flow is in guided media. Metallic wires were used almost exclusively in telecommunications networks for the last 90 years, until the development of microwave and satellite radio communications systems. Therefore, copper wire is now a mature technology, rugged and inexpensive. In certain applications, copper-covered steel, copper alloy, nickel- and/or gold-plated copper and even aluminum metallic conductors are employed.

The maximum transmission speed is limited in this case. The copper conductor that carries analog data can be used to carry digital data also in association with the modem. Modem is a device to convert digital signal into analog signal and vice versa. The data rate in this category is limited to around 28 Kbps. The introduction of the Integrated Services Digital Network (ISDN) led to the use of improved modulation and coding schemes and data rate up to 128 Kbps. Local Area Networks (LANs) also use twisted pairs. These networks also upgraded to support for high bit rate real time multimedia. The Asymmetric Digital Subscriber Lines (ADSL) technology is aimed at using two wire copper loops at data rates of 1.544 Mbps in the network to user direction and about 600 Kbps from the user to network.

The twisted pair cable may be defined in two categories based upon the shielding and without shielding.

Notes

Unshielded Twisted Pair (UTP)

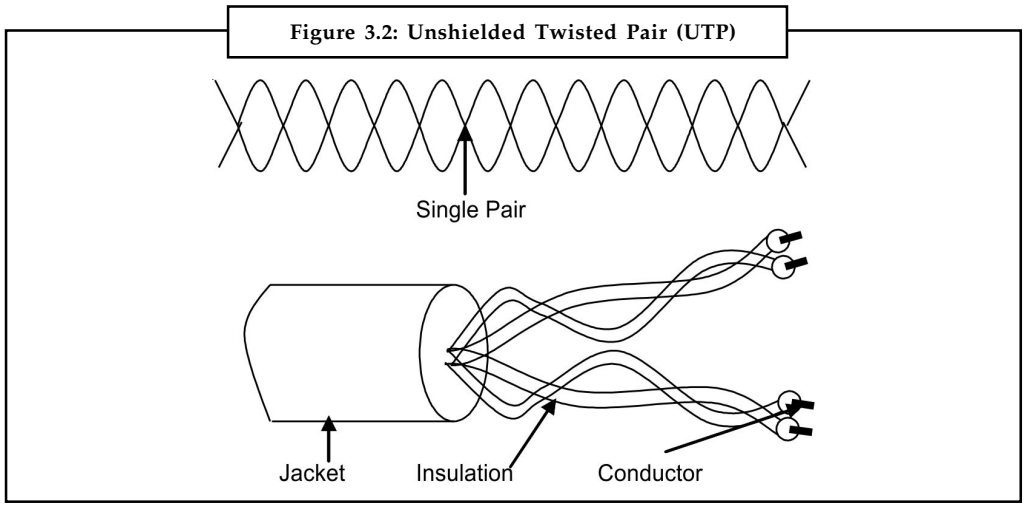
UTP as depicted in Figure 3.2 is the copper media, inherited from telephony, which is being used for increasingly higher data rates, and is rapidly becoming the de facto standard for horizontal wiring. Horizontal wiring specifies the connection between, and including, the outlet and the termination in the communication closet. The horizontal is limited to a maximum of 90 meters. This is independent of the media type so that the communication closet is common to all media and all applications operating over the media. In addition, there is an allowance for 3 meters in the work area and 6 meters for cross connecting in the closet for a total of 99 meters.

The recommended media and connectors for the horizontal are as follow:

- 100-ohm unshielded twisted pair - 4 pairs, 8-pin modular connector (ISDN)
- 150-ohm shielded twisted pair - 2 pairs (IBM connector or RJ45)
- 50-ohm coax (thin) - IEEE 10BASE2, standard BNC connector
- 62.5/125 multi mode fiber

A UTP cable contains from 2 to 4200 twisted pairs. The advantages of UTP are the flexibility, low cost media, and can be used for either voice or data communications. Its greatest disadvantage is the limited bandwidth, which restricts long distance transmission with low error rates.

Figure 3.2: Unshielded Twisted Pair (UTP)

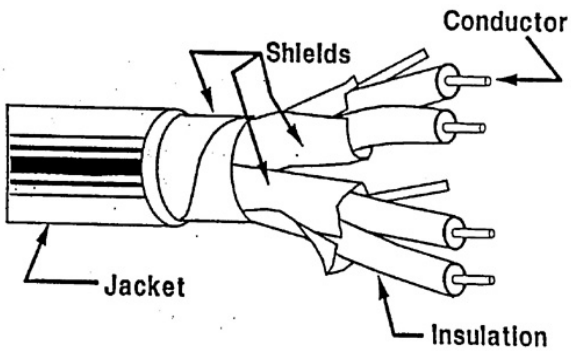


Shielded Copper or STP

Shielded twisted pair (STP) differs from UTP in that a metallic shield or screen surrounds the pairs, which may or may not be twisted. As illustrated in Figure 3.3, the pairs can be individually shielded. A single shield can surround a cable containing multiple pairs or both techniques can be employed in tandem. The shield itself is made of aluminum, steel, or copper. This is in the form of a metallic foil or woven meshes and is electrically grounded. Although less effective, the shield sometimes is in the form of nickel and/or gold plating of the individual conductors.

Notes

Figure 3.3: Shielded Twisted Pair (STP) Configuration



Shielded copper offers the advantage of enhanced performance for reasons of reduced emissions and reduction of electromagnetic interference. Reduction of emissions offers the advantage of maintaining the strength of the signal through the confinement of the electromagnetic field within the conductor. In other words, signal loss is reduced. An additional benefit of this reduction of emissions is that high-frequency signals do not cause interference in adjacent pairs or cables. Immunity from interference is realized through the shielding process, which reflects electromagnetic noise from outside sources, such as electric motors, other cables and wires, and radio systems.

Shielded twisted pair, on the other hand, has several disadvantages. First, the raw cost of acquisition is greater as the medium is more expensive to produce. Second, the cost of deployment is greater as the additional weight of the shield makes it more difficult to deploy. Additionally, the electrical grounding of the shield requires more time and effort.

General Properties of Twisted Pair

- ***Gauge:*** Gauge is a measure of the thickness of the conductor. The thicker the wire, the less the resistance, the stronger the signal over a given distance, and the better the performance of the medium. Thicker wires also offer the advantage of greater break strength. The gauge numbers are retrogressive. In other words, the larger is the number, the smaller is the conductor.
- ***Configuration:*** In a single pair configuration, the pair of wires is enclosed in a sheath or jacket, made of polyethylene, polyvinyl chloride or Teflon. Usually, multiple pairs are so bundled in order to minimize deployment costs associated with connecting multiple devices (e.g., electronic PBX or KTS telephone sets, data terminals, and modems) at a single workstation.
- ***Bandwidth:*** The effective capacity of twisted pair cable depends on several factors, including the gauge of the conductor, the length of the circuit and the spacing of the amplifiers/ repeaters. One must also recognize that a high-bandwidth (high frequency) application may cause interference with other signals on other pairs in close proximity.
- ***Error Performance:*** Signal quality is always important, especially relative to data transmission. Twisted pair is especially susceptible to the impacts of outside interference, as the lightly insulated wire act as antennae and, thereby, absorbs such errant signals. Potential sources of Electro Magnetic Interference (EMI) include electric motors, radio transmissions and fluorescent light boxes. As transmission frequency increases, the error performance of copper degrades significantly with signal attenuation increasing approximately as the square root of frequency.

Notes

- ***Distance:*** Twisted pair is distance limited. As distance between network elements increases, attenuation (signal loss) increases and quality decreases at a given frequency. As bandwidth increases, the carrier frequency increases, attenuation becomes more of a issue, and amplifiers/repeaters must be spaced more closely.
- ***Security:*** Twisted pair is inherently an insecure transmission medium. It is relatively simple to place physical taps on UTP. Additionally, the radiated energy is easily intercepted through the use of antennae or inductive coils, without the requirement for placement of a physical tap.
- ***Cost:*** The acquisition, deployment and rearrangement costs of UTP are very low, at least in inside wire applications. In, high-capacity, long distance applications, such as inter-office trunking, however, the relative cost is very high, due to the requirements for trenching or boring, conduit placement, and splicing of large, multi pair cables. Additionally, there are finite limits to the capacity and other performance characteristics of UTP, regardless of the inventiveness of technologists. Hence, the popularity of alternatives such as microwave and fibre-optic cable.
- ***Applications:*** UTP's low cost including recently developed methods of improving its performance has increased its application in short-haul distribution systems or inside wire applications. Current and continuing applications include the local loop, inside wire and cable, and terminal-to-LAN. Generally speaking, UTP no longer is deployed in long haul or outside the premises transmission systems.

The additional cost of shielded copper limits its application to inside wire applications. Specifically, it generally is limited to application in high-noise environments. It also is deployed where high frequency signals are transmitted and there is concern about either distance performance or interference with adjacent pairs. Examples include LANs and image transmission.

3.2.2 Coaxial Cable

The main limiting factor of a twisted pair cable is caused by a phenomenon known as the skin effect. As the frequency of the transmitted signal increases, the current flowing in the wires tends to flow only on the outer surface of the wire, thus using the less of the available cross section. This increases the electrical resistance of the wires for higher frequency signals leading to higher attenuation. In addition, at higher frequencies, more signal power is lost as a result of radiation effects. Hence for applications that demand higher frequencies, another type of transmission medium must be used. Coaxial cable minimizes both these effects.

Coaxial Cable as shown in Figure 3.4 is a very robust shielded copper wire two-conductor cable in which a solid centre conductor runs concentrically (coaxial) inside a solid outer circular conductor. This forms an electromagnetic shield around the former that serves to greatly improve signal strength and integrity. The two conductors are separated by insulation. A layer of dielectric (nonconductive) material, such as PVC or Teflon then protects the entire cable.

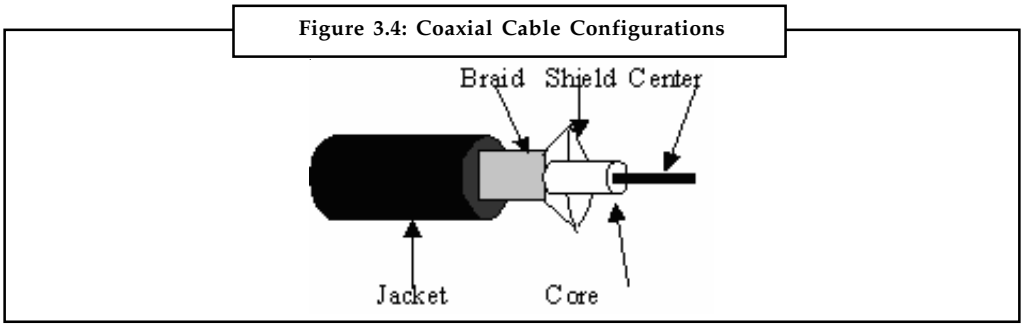
It comes under the category of a bounded media and is still an effective medium to use in data communication. Coaxial cable includes shield for improved performance and therefore is expensive. Cable TV networks use coaxial cable. Local Area Networks can operate over coaxial cable to the 10BASE5, 10BASE2 and 10BASET specifications. In general, coaxial cable enables longer distance transmission at higher data rates than twisted pair cable but is more expensive.

There are two types of coaxial cables:

- ***Baseband:*** It transmits a single signal at a time at very high speed. The signal on baseband cable must be amplified at a specified distances. It is used for local area networks.
- ***Broadband:*** It can transmit many simultaneous signals using different frequencies.

Notes

Figure 3.4: Coaxial Cable Configurations



General Properties of Coaxial Cable

- ***Gauge:*** The gauge of coaxial cable is thicker than the twisted pair. While this increases the available bandwidth and the distance of transmission, it also increases the cost. Traditional coaxial cable is quite thick, heavy and bulky of which Ethernet LAN 10Base5 is an example. Ethernet LAN 10Base2 is of much lesser dimensions but offers less in terms of performance.
- ***Configuration:*** Coaxial cables consist of a single, two-conductor wire, with a centre conductor and an outer shield/conductor, which is of solid metal. Sometimes braided or stranded metal is used. Twin axial cables contain two such configurations within a single cable sheath. As the centre conductor carries the carrier signal and the outer conductor generally is used for electrical grounding. Coaxial cable connectivity can be extended through the use of twisted pair with a BALUN (BALanced/UNbalanced) connector serving to accomplish the interface.
- ***Bandwidth:*** The effective capacity of coaxial cable depends on several factors, including the gauge of the centre conductor, the length of the circuit, and the spacing of amplifiers and other intermediate devices. The available bandwidth over coaxial cable is very significant; hence it is used in high capacity applications, such as data and image transmission.
- ***Error Performance:*** Coaxial cable performs exceptionally well, due to the outer shielding. As a result, it is often used in data applications.
- ***Distance:*** Coaxial cable is not as limited as UTP, although amplifiers or other intermediate devices must be used to extend high frequency transmissions over distances of any significance.
- ***Security:*** Coaxial cable is inherently quite secure. It is relatively difficult to place physical taps on coaxial cable. Radiation of energy is also minimal hence interception of it is not easy.
- ***Cost:*** The acquisition, deployment, and rearrangement costs of coaxial cables are very high, compared with UTP. In high capacity data applications, however, that cost is often outweighed by its positive performance characteristics.
- ***Applications:*** Coaxial cable's superior performance characteristics make it the favored medium in many short hauls, bandwidth-intensive data applications. Current and continuing applications include LAN backbone, host-to-host, host-to-peripheral and CATV.

Self Assessment

State whether the following statements are true or false:

6. Twisted pair (both unshielded and shielded), coaxial and fiber optic cable systems fall into guided transmission media category.

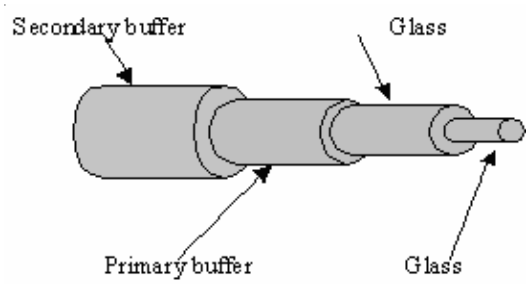
Notes

7. The twisting decreases the electrical noise immunity, and reduces the error rate of the data transmission.
8. A UTP cable contains from 2 to 4200 twisted pairs.
9. Coaxial cable is inherently an insecure transmission medium.
10. Local Area Networks can operate over coaxial cable to the 10BASE5, 10BASE2 and 10BASET specifications

3.2.3 Optical Fiber

We have seen in the previous section that the geometry of coaxial cable significantly reduces the various limiting effects, the maximum signal frequency, and hence the information rate that can be transmitted using a solid conductor, although very high, is limited. This is also the case for twisted lines. Optical fiber differs from both these transmission media in that it carries the transmitted information in the form of a fluctuating beam of light in a glass fiber rather than as an electrical signal on a wire. This type of transmission has become strong support for digital network owing to its high capacity and other factors favorable for digital communication.

Figure 3.5: Fiber Optic Cable – General View

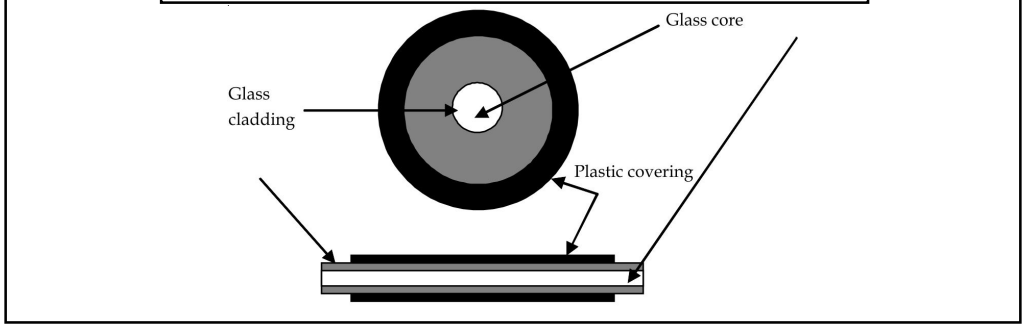


Fiber optic transmission systems are opto-electric in nature. In other words, a combination of optical and electrical electromagnetic energy is involved. The signal originates as an electrical signal, which is translated into an optical signal, which subsequently is reconverted into an electrical signal at the receiving end. Thin glass fiber as shown in Figure 3.5 is very clear and designed to reflect light internally for efficient transmission carries light with encoded data. Plastic jacket allows fiber to bend (some!) without breaking. Light emitting diode (LED) or laser injects light into fiber for transmission. Light sensitive receiver at other end translates light back into data.

The optical fiber consists of a number of substructures as shown in Figure 3.6. In this case, a cladding made of glass with lower refractive index surrounds a core made of glass, which carries most of the light. This bends the light and confines it to the core. The core is surrounded by a substrate layer (in some fibers) of glass, which does not carry light, but adds to the diameter and strength of the fiber. A primary buffer coating and a secondary buffer coating to provide mechanical protection cover all these.

Notes

Figure 3.6: Glass Fiber Optic Cable, Side View, and Cross Section



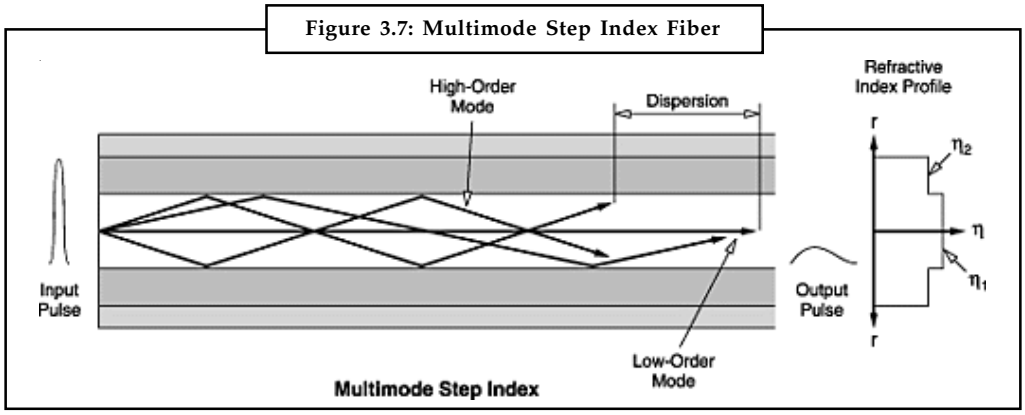
The light pulse travels down the center core of the glass fiber. Surrounding the inner core is a layer of glass cladding, with a slightly different refractive index. The cladding serves to reflect the light waves back into the inner core. Surrounding the cladding is a layer of protective plastic coating that seals the cable and provides mechanical protection. This is shown in Figure 3.6. Typically, multiple fibers are housed in a single sheath, which may be heavily armored.

Light propagates along the optical fiber core in one of the following ways depending on the type and width of core material used.

Multimode Fiber

Here, the core diameter is relatively large compared to a wavelength of light. Core diameter ranges from 50 micrometers (μm) to 1,000 μm, compared to the wavelength of light of about 1 μm. This means that light can propagate through the fiber in many different ray paths, or modes, hence the name multimode. Multimode fiber is less expensive to produce and inferior in performance because of the larger diameter of the inner core. When the light rays travel down the fiber, they spread out due to a phenomenon known as modal dispersion. Although reflected back into the inner core by the cladding, they travel different distances and, therefore, arrive at different times. The received signal thus has a wider pulse width than the input signal with a corresponding decrease in the speed of transmission. As a result, multimode fiber is relegated to applications involving relatively short distances and lower speeds of transmission, for example, LANs and campus environments. Two basic types of multimode fibers exist. The simpler and older type is a "step index" fiber, where the index of refraction (the ability of a material to bend light) is the same all across the core of the fiber.

Figure 3.7: Multimode Step Index Fiber



This is shown in Figure 3.7. With all these different ray paths or modes of propagation, different rays travel different distances, and take different amounts of time to transit the length of a fiber.

Notes

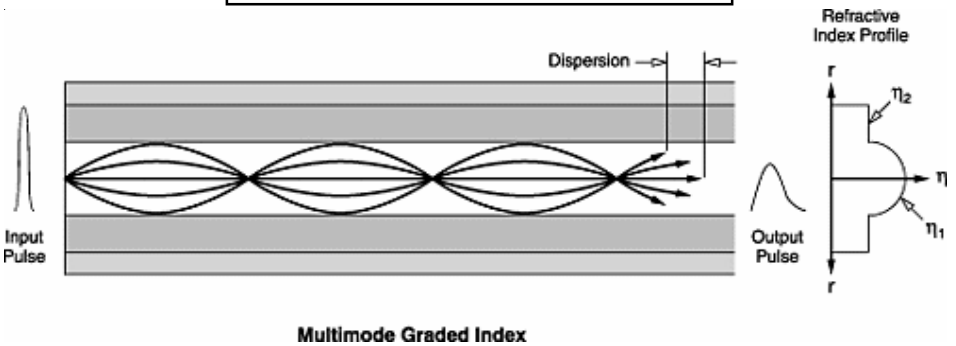
This being the case, if a short pulse of light is injected into a fiber, the various rays emanating from that pulse will arrive at the other end of the fiber at different times, and the output pulse will be of longer duration than the input pulse. This phenomenon is called "modal dispersion" (pulse spreading), and limits the number of pulses per second that can be transmitted down a fiber and still be recognizable as separate pulses at the other end. This, therefore, limits the bit rate or bandwidth of a multimode fiber. For step index fibers, wherein no effort is made to compensate for modal dispersion, the bandwidth is typically 20 to 30 MHz over a length of one kilometer of fiber, expressed as "MHz - km".

Graded Index Multimode Fiber

In the case of a graded index multimode fiber, the index of refraction across the core is gradually changed from a maximum at the center to a minimum near the edges, hence the name graded index. This design takes advantage of the phenomenon that light travels faster in a low-index-of-refraction material than in a high-index material. If a short pulse of light is launched into the graded index fiber, it may spread some during its transit of the fiber, but much less than in the case of a step index fiber. Therefore, dispersion can be reduced using a core material that has a variable refractive index. In such multimode graded index fiber light is refracted by an increasing amount as it moves away from the core as shown in Figure 3.8. This has the effect of narrowing the pulse width of the received signal compared with stepped index fiber, allowing a corresponding increase in the speed of transmission. They therefore can support a much higher bit rate or bandwidth.

Did u know? Typical bandwidths of graded index fibers range from 100 MHz-km to well over 1GHz-km. The actual bandwidth depends on how well a particular fiber's index profile minimizes modal dispersion, and on the wavelength of light launched into the fiber.

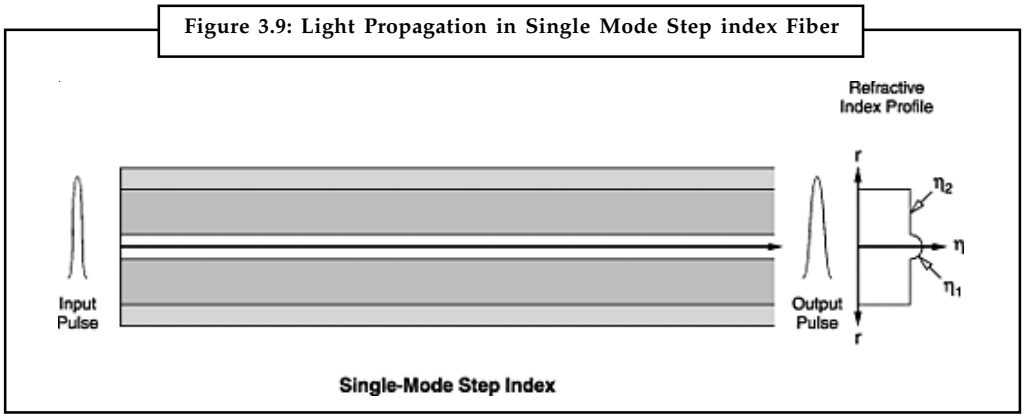
Figure 3.8: Multimode Granded Index



Monomode/Singlemode fiber: This has a thinner inner core. In this case, the core diameter of about 9 µm is much closer in size to the wavelength of light being propagated, about 1.3 µm. This limits the light transmission to a single ray or mode of light to propagate down the core of the fiber as shown in Figure 3.9. All the multiple-mode or multimode effects described above are eliminated. However, one pulse-spreading mechanism remains. Just as in the multimode fibers, different wavelengths of light travel at different speeds, causing short pulses of light injected into the fiber to spread as they travel. This phenomenon is called "chromatic dispersion".

Notes

Figure 3.9: Light Propagation in Single Mode Step index Fiber



It performs better than does multimode fiber over longer distances at higher transmission rates. Due to reduced core diameter all the emitted light propagates along a single path. Consequently the received signal is of a comparable width to the input signal. Although more costly, monomode fiber is used to advantage in long haul, and especially in high bandwidth, applications.

Notes Singlemode fibers have the very broadest bandwidth, lowest cost and lowest attenuation of any available optical fiber. Therefore, they are universally used in long-distance telephony and cable television applications.

Advantages of Optical Fibers

- Immunity to electromagnetic interference and crosstalk
- No electrical ground loop or short circuit problems
- Small size and light-weight
- Large bandwidth for size and weight
- Safe in combustible areas (no arching)
- Immunity to lightning and electrical discharges
- Longer cable runs between repeaters
- Flexibility and high strength
- Potential high temperature operation
- Secure against signal leakage and interference
- No electrical hazard when cut or damaged.

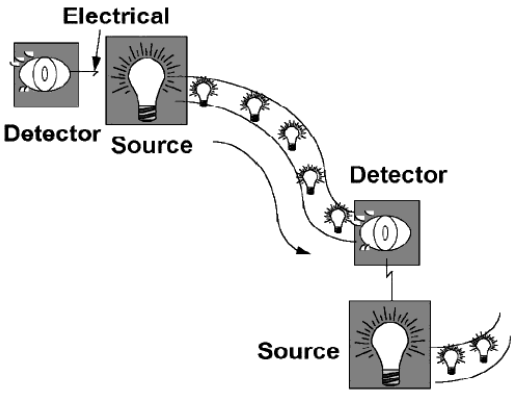
General Properties of Optical Fiber

Configuration: Fiber optic systems consist of light sources, cables and light detectors, as depicted in Figure 3.10. In a simple configuration, one of each is used. In a more complex configuration over longer distances, many such sets of elements are employed. Much as is the case in other transmission systems, long haul optical communications involve a number of regenerative repeaters. In a fiber optic system, repeaters are opto-electric devices. On the incoming side of the repeater, a light detector receives the optical signal, converts it into an electrical signal, boosts

Notes

it, converts it back into an optical signal, and places it onto a fiber, and so on. There may be many such optical repeaters in a long haul transmission system, although typically far fewer than would be required using other transmission media.

Figure 3.10: Fiber Optic Systems



- ***Bandwidth:*** Fiber offers by far the greatest bandwidth of any transmission system, often in excess of 2 Gbps in long haul carrier networks. Systems with 40 Gbps have been tested successfully on numerous occasions. The theoretical capacity of fiber is in the terabit (Tbps) range, with current monomode fiber capacity being expandable to that level.
- ***Error Performance:*** Fibre being a dielectric (a nonconductor of direct electric current), it is not susceptible to Electro Magnetic Interference/Radio Frequency Interference (EMI/RFI). This also does not emit EMI/RFI. The light signal will suffer from attenuation, although less so than other media. Scattering of the optical signal, bending in the fiber cable, translation of light energy to heat, and splices in the cable system can cause such optical attenuation.
- ***Distance:*** Monomode fiber optic systems routinely are capable of transmitting signals over distances in excess of 325 km. Hence relatively few optical repeaters are required in a long-haul system. This will reduce costs, and eliminate points of potential failure.
- ***Security:*** Fiber is intrinsically secure, as it is virtually impossible to place a physical tap without detection because no light is radiated outside the cable. Therefore, interception of signal is almost impossible. Additionally, the fiber system supports such a high volume of traffic that it is difficult to intercept and distinguish a single transmission from the tens of thousands of other transmissions that might ride the same cable system. The digital nature of most fibers coupled with encryption techniques frequently used to protect from interception make fibers highly secure.
- ***Cost:*** While the acquisition, deployment, and rearrangement costs of fiber are relatively high, the immense bandwidth can outweigh that cost in bandwidth-intensive applications. At Gbps speeds, a single set of fibers can carry huge volumes of digital transmissions over longer distances than alternative systems, thereby lowering the transport cost per bit and cost per conversation to fractions of a penny per minute.
- ***Applications:*** Applications for fiber optic transmission systems are bandwidth intensive. Such applications include backbone carrier networks, international submarine cables, backbone LANs (FDDI), interoffice trunking, computer-to-computer distribution networks (CATV and Information Superhighway) and fiber to the desktop (Computer Aided Design).

Notes

Bounded Media Comparison Chart

Table 3.2: Bounded Media Comparison Chart

Media	Advantages	Disadvantages
Twisted Pair Cable	Inexpensive, well established, easy to add nodes	Sensitive to noise, short distances, limited bandwidth, security hazard because of easy interception
Coaxial Cable	High bandwidth, long distances, noise immunity	Physical dimensions, security is better in comparison to twisted pair cable
Optical Fiber Cable	Very high bandwidth, noise immunity, long distances, high security, small size	Connections, cost

Task Give a brief description of the application and limitations of the following types of transmission media:

(a) Two-wire open lines

(b) Twisted pair lines

(c) Coaxial cable

(d) Optical fiber

(e) Microwaves

3.3 Summary

- There are several kinds of transmission media. These media technologies starting from copper wire to wireless and fiber optic has grown-up so rapidly and replacing other very quickly in this information age.
- Transmission media can be brodadly classified into two types: Guided and Unguided transmission media.
- Twisted pair, coaxial cable and optical fiber fall into the category of guided or bounded transmission media.
- Twisted pair is a pair of copper wires twisted together and wrapped with a plastic coating. It is mainly of two types: shielded twisted pair(STP) and Unshielded twisted pair (UTP).
- Shielded twisted pair (STP) differs from UTP in that a metallic shield or screen surrounds the pairs, which may or may not be twisted.
- Coaxial Cable is a very robust shielded copper wire two-conductor cable in which a solid center conductor runs concentrically (coaxial) inside a solid outer circular conductor.
- Optical fiber carries the transmitted information in the form of a fluctuating beam of light in a glass fiber rather than as an electrical signal on a wire. It can be of two types: monomode and multimode fiber.

3.4 Keywords

Notes

Bandwidth: Refers to the range of frequencies assigned to a channel.

Bounded Media: Refers to the wired transmission systems that employ physical media, which are tangible.

Coaxial Cable: It is a very robust shielded copper wire two-conductor cable in which a solid center conductor runs concentrically (coaxial) inside a solid outer circular conductor.

Frequency Spectrum: Refers to the range of frequencies being supported by a particular transmission medium.

Gauge: Gauge is a measure of the thickness of the conductor.

Graded Index Multimode Fiber: In the case of a graded index multimode fiber, the index of refraction across the core is gradually changed from a maximum at the center to a minimum near the edges, hence the name graded index.

Monomode/Singlemode fiber: This has a thinner inner core. In this case, the core diameter of about 9 µm is much closer in size to the wavelength of light being propagated, about 1.3 µm. This limits the light transmission to a single ray or mode of light to propagate down the core of the fiber.

Multimode Fiber: The core diameter is relatively large compared to a wavelength of light.

Optical Fiber: Optical fiber carries the transmitted information in the form of a fluctuating beam of light in a glass fiber rather than as an electrical signal on a wire.

Propagation Delay: Refers to the length of time required for a signal to travel from transmitter to receiver across a transmission system.

Shielded Copper or STP: Shielded twisted pair (STP) differs from UTP in that a metallic shield or screen surrounds the pairs, which may or may not be twisted.

Step Index Multimode Fiber: Different rays travel different distances, and take different amounts of time to transit the length of a fiber.

Twisted Pair: A twisted pair is a pair of copper wires twisted together and wrapped with a plastic coating.

Unbounded Media: Refers to wireless transmission systems do not make use of a physical conductor, or guide, to bind the signal.

Unshielded Twisted Pair (UTP): A UTP cable contains from 2 to 4200 twisted pairs. The advantages of UTP are the flexibility, low cost media, and can be used for either voice or data communications.

3.5 Review Questions

1. What are the different transmission mediums over which data communication devices can provide service?
2. What are the major limitations of twisted pair wire?
3. Describe how satellite communication is different from radio broadcast?
4. A receiver in fiber optic system requires 5 microwatt of power. The length of cable is 5 Km and offers an attenuation loss of 2 dB/km. There is a loss of 1 dB at both the source and the receiver. Calculate the required level of optical power at the optical source.

Notes

5. State with the help of a diagram the different components of typical fiber optic link. Mention the various components of signal loss.
6. What is reflection? What happens to a beam of light as it travels to a less dense medium? What happens if it travels to a denser medium?
7. What advantages do coaxial cables offer over twisted pair cables?
8. Compare fiber optic cable with UTP cable when used as transmission media in LANs.
9. What is the purpose of cladding in an optical fiber? Discuss its density with respect to the core.
10. What is skin effect and how does it affect the performance of TP cables?
11. How does coaxial cable reduce the problem of skin effect and becomes an appropriate media for higher frequency data transmission?
12. Which type of transmission media does find extensive deployment for digital transmission and why?

Answers: Self Assessment

1.	Transmission media	2.	Pass band
3.	Bandwidth	4.	Propagation delay
5.	Frequencies	6.	True
7.	False	8.	True
9.	False	10.	True

3.6 Further Readings

Books

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall

Behrouz A. Forouzan and Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies

Burton, Bill, *Remote Access for Cisco Networks*, McGraw-Hill Osborne Media McGraw-Hill Osborne Media

Rajneesh Agrawal and Bharat Bhushan Tiwari, *Computer Networks and Internet*, Vikas Publication

Unit 4: Physical Layer-2

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Describe the wireless communication media like radio, microwave, VLF, etc. and its applications
- Discuss general properties of the different types of wireless communication systems
- Describe Satellite communication with its general properties and applications
- Describe concepts of public switched telephone network, digital channel and trunk lines
- Know the underlying technologies of cable television and cable modem

Introduction

As you know that there are various ways to transmit the signal. These ways can be broadly categorized into guided and unguided media. The guided media includes all wired media, also referred to as conducted or bounded media. You have already studied about the guided/bounded transmission media in the last unit. Now in this unit you will learn about the second category which includes all traditional wireless media, also referred to as radiated, or unbounded. In the transmission of signal the data is encoded to energy and then energy is transmitted. Similarly at the receiving end the energy is decoded back to data. This energy can be electrical, light and radio, etc. Therefore, this transmitted energy is carried through some sort of medium, which

Notes

depends upon the type of energy being transmitted. Each form of energy has different properties and requirements for transmission. This requires special hardware for data encoding and connection to transmission medium. Media can be copper, glass and air, etc.

4.1 Wireless Transmission

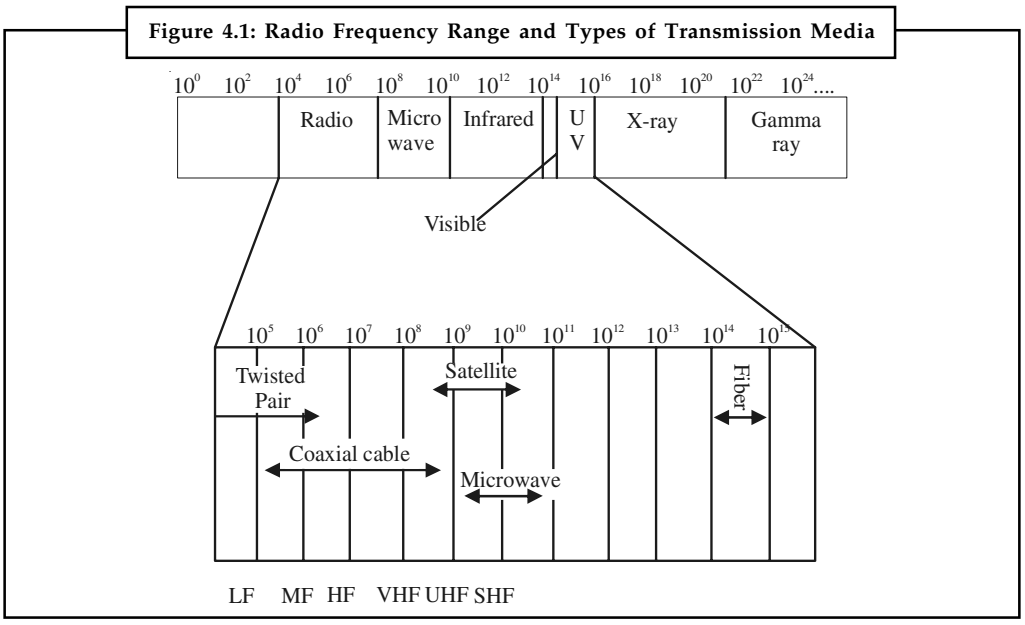
Wireless transmission systems do not make use of a physical conductor, or guide, to bind the signal. In this case, data are transmitted using electromagnetic waves. Therefore, they are also known as unguided or unbounded systems. Energy travels through the air rather than copper or glass. Hence the term radiated often is applied to wireless transmission. Finally, such systems employ electromagnetic energy in the form of radio or light waves that are transmitted and received across space, and are referred to as airwave systems. The transmission systems addressed under this category include microwave, satellite and infrared. There are different techniques to convert the data suitable for this mode of communication. Conceptually similar to radio, TV, cellular phones, radio waves can travel through walls and through an entire building. They can travel for long distance using satellite communication or short distance using wireless communication.

Use of this technology for delivery of real time applications like multimedia material should be treated carefully, because radio links are susceptible to fading, interference, random delays, etc. Non-real time use of this technology is likely to perform as well as current Ethernet LANs.

4.1.1 Radio

It is a technique where data is transmitted using radio waves and therefore energy travels through the air rather than copper or glass. Conceptually, radio, TV, cellular phones, etc. uses radio transmission in one form or another. The radio waves can travel through walls and through an entire building. Depending upon the frequency, they can travel long distance or short distance. Satellite relay is the one example of long distance communication. Therefore, each frequency range is divided into different bands, which has a specific range of frequencies in the Radio Frequency (RF) spectrum. The RF is divided in different ranges starting from Very Low Frequencies (VLF) to Extremely High Frequencies (EHF). Figure 4.1 shows each band with a defined upper and lower frequency limit.

Figure 4.1: Radio Frequency Range and Types of Transmission Media



Notes

Two transmitters cannot share the same frequency band because of mutual interference and therefore band usage is regulated.

Did u know? International use of the radio spectrum is regulated by the International Telecommunication Union (ITU). Domestic use of the radio spectrum is regulated by national agencies such as Wireless Planning and Coordination (WPC) in India. WPC assigns each transmission source a band of operation, a transmitter radiation pattern, and a maximum transmitter power.

Omni directional or directional antennas are used to broadcast radio waves depending upon band. The transceiver unit, which is consisted of transmitter and receiver along with the antenna, determines the power of RF signal. Other characteristics of radio waves is that in vacuum all electromagnetic waves or radio waves travel at the same speed i.e. at the speed of light which is equal to 3 × 108 meter per seconds. In any medium this speed gets reduced and also becomes frequency dependent. In case of copper the speed of light becomes approximately two thirds of the speed of light.

The basic features of the radio waves are that:

- They are easy to generate
- They have same velocity in vacuum
- They may traverse long distances
- They are omni directional
- They can penetrate building easily so they find extensive use in communication both indoor and outdoor
- They are frequency dependent. At low frequency they can pass through obstacles well but the power falls off sharply with distance from the source, as power is inversely proportional to cube of the distance from the source. At HF they travel in straight lines and bounce off obstacles.

4.1.2 Very Low Frequency (VLF)

The VLF method takes advantage of electromagnetic radiation generated in the low frequency band of 3-30 KHz by powerful radio transmitters used in long-range communications and navigational systems. At large distances from the source, the electromagnetic field is planar and horizontal and the electric component E lies in a vertical plane perpendicular to the H component in the direction of propagation and follow the ground. AM uses VLF band. This band of frequencies cannot be used for data transfer because they offer relatively low bandwidth.

4.1.3 Microwave Transmission

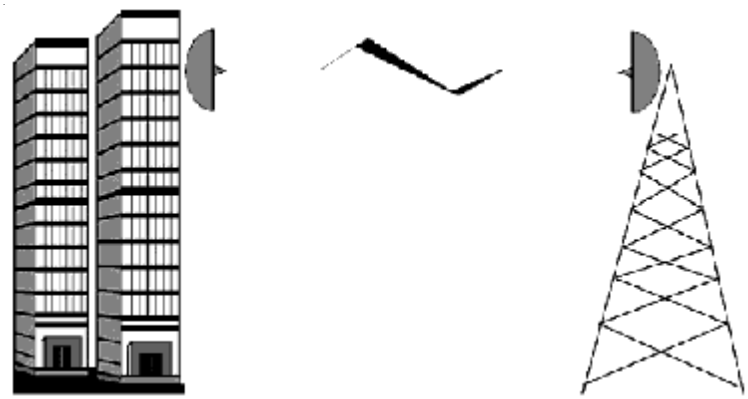
Microwave radio, a form of radio transmission that uses ultra-high frequencies, developed out of experiments with radar (radio detecting and ranging) during the period preceding World War II. There are several frequency ranges assigned to microwave systems, all of which are in the Giga Hertz (GHz) range and the wavelength in the millimeter range. This very short wavelength gives rise to the term microwave. Such high frequency signals are especially susceptible to attenuation and, therefore must be amplified or repeated after a particular distance.

In order to maximize the strength of such a high frequency signal and, therefore, to increase the distance of transmission at acceptable levels, the radio beams are highly focused. The transmit

Notes

antenna is centered in a concave, reflective metal dish which serves to focus the radio beam with maximum effect on the receiving antenna, as illustrated in Figure 4.2. The receiving antenna, similarly, is centered in a concave metal dish, which serves to collect the maximum amount of incoming signal.

Figure 4.2: Point-to-Point Microwave



It is a point-to-point, rather than a broadcast, transmission system. Additionally, each antenna must be within line of sight of the next antenna. Given the curvature of the earth, and the obvious problems of transmitting through it, microwave hops generally are limited to 50 miles (80 km). If the frequencies are higher within the microwave band given in Table 4.1, this impact is more than lower frequencies in the same band.

Table 4.1: Microwave Frequency Bands

Frequency Bands	Maximum Antenna Separation	Analog/Digital
4–6 GHz		Analog
10-12 GHz	16-24 Km	Digital
18-23 GHz	32-48 Km	Digital

General Properties of Microwave Transmission

- ***Configuration:*** Microwave radio consists of antennae centered within reflective dishes that are attached to structures such as towers or buildings. Cables connect the antennae to the actual transmit/receive equipment.
- ***Bandwidth:*** Microwave offers substantial bandwidth, often in excess of 6Gbps.
- ***Error Performance:*** Microwave, especially digital microwave, performs well in this regard, assuming proper design. However, such high frequency radio is particularly susceptible to environmental interference, e.g., precipitation, haze, smog, and smoke. Generally speaking, however, microwave performs well in this regard.
- ***Distance:*** Microwave clearly is distance limited, especially at the higher frequencies. This limitation can be mitigated through special and more complex arrays of antennae incorporating spatial diversity in order to collect more signals.
- ***Security:*** As is the case with all radio systems, microwave is inherently not secure. Security must be imposed through encryption (scrambling) of the signal.

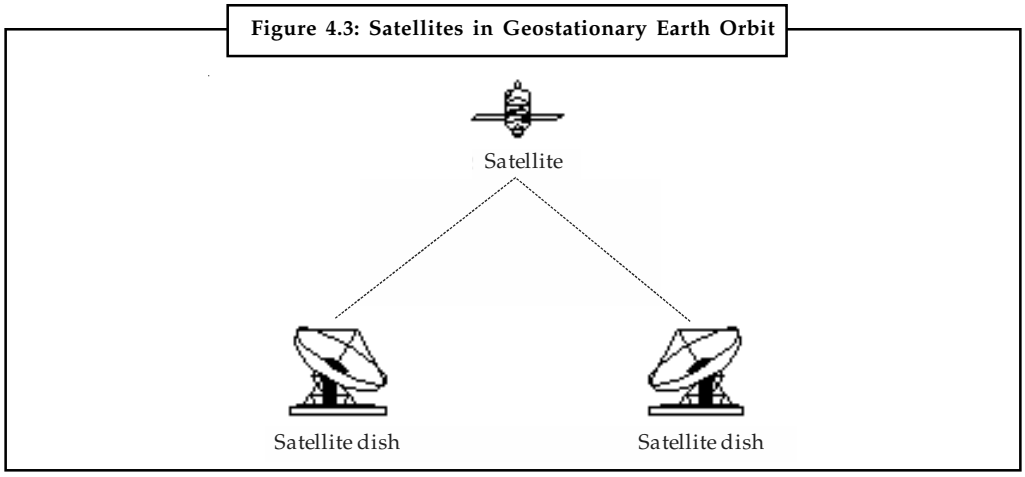
Notes

- *Cost:* The acquisition, deployment and rearrangement costs of microwave can be high. However, it often compares very favorably with cabled systems, which require right-of-way, trenching, conduit, splicing, etc.
- *Applications:* Microwave originally was used for long haul voice and data communications. Competing long distance carriers, microwave was found a most attractive alternative to cabled systems, due to the speed and low cost of deployment where feasible, however, fiber optic technology is currently used in this regard. Contemporary applications include private networks, interconnection of cellular radio switches, and as an alternative to cabled systems in consideration of difficult terrain.

4.2 Satellite Communication

Satellite radio, quite simply, is a non-terrestrial microwave transmission system utilizing a space relay station. Satellites have proved invaluable in extending the reach of voice, data, and video communications around the globe and into the most remote regions of the world. Exotic applications such as the Global Positioning System (GPS) would have been unthinkable without the benefit of satellites.

Figure 4.3: Satellites in Geostationary Earth Orbit



Contemporary satellite communications systems involve a satellite relay station that is launched into a geostationary, geosynchronous, or geostatic orbit. Such satellites are called geostationary satellite. Such an orbit is approximately 36,000 kms above the equator as depicted in Figure 4.3. At that altitude and in an equatorial orbital slot, the satellite revolves around the earth with the same speed as of that the speed of revolution of earth and maintains its relative position over the same spot of the earth's surface. Consequently, transmit and receive earth stations can be pointed reliably at the satellite for communications purposes.

The popularity of satellite communications has placed great demands on the international regulators to manage and allocate available frequencies, as well as the limited number of orbital slots available for satellite positioning are managed at national, regional and international levels. Generally speaking, geostationary satellites are positioned approximately 2° apart in order to minimize interference from adjacent satellites using overlapping frequencies.

Such high frequency signals are especially susceptible to attenuation in the atmosphere. Therefore, in case of satellite communication two different frequencies are used as carrier frequencies to avoid interference between incoming and outgoing signals. These are:

- *Uplink frequency:* It is the frequency used to transmit signal from earth station to satellite. Table 4.2 shows the higher of the two frequencies is used for the uplink. The uplink signal

Notes

can be tailored stronger and therefore can better deal with atmospheric distortion. The antenna at transmitting side is centered in a concave, reflective dish that serves to focus the radio beam, with maximum effect, on the receiving satellite antenna. The receiving antenna, similarly, is centered in a concave metal dish, which serves to collect the maximum amount of incoming signal.

- ***Downlink frequency:*** It is the frequency used to transmit the signal from satellite to earth station. In other words, the downlink transmission is focused on a particular footprint, or area of coverage. The lower frequency, used for the downlink, can better penetrate the earth's atmosphere and electromagnetic field, which can act to bend the incoming signal much as light bends when entering a pool of water.

Table 4.2: Example Uplink/Downlink Satellite Frequencies

Frequency Band	Uplink/Downlink Frequency Range	Example
C–band	6 GHz/4 GHz	TV, Voice, Videoconferencing
Ku–band	14 GHz/11 GHz	TV, Direct Broadcast Satellite/DSS
Ka–band	30 GHz/20 GHz	Mobile Voice

Broadcast: The wide footprint of a satellite radio system allows a signal to be broadcast over a wide area. Thereby any number (theoretically an infinite number) of terrestrial antennae can receive the signal, more or less simultaneously. In this manner, satellites can serve a point-to-multipoint network requirement through a single uplink station and multiple downlink stations.

Recently, satellites have been developed which can serve a mesh network requirement, whereby each terrestrial site can communicate directly with any other site. Previously, all such communications were required to travel through a centralized site, known as a head end. Such a mesh network, of course, imposes an additional level of difficulty on the network in terms of management of the flow and direction of traffic.

General Properties of Satellite Communication

- ***Configuration:*** Satellite communication systems consist of antennae and reflective dishes, much as in terrestrial microwave. The dish serves to focus the signal from a transmitting antenna to a receiving antenna. The send/receive dishes that make up the earth segment are of varying sizes, depending on power levels and frequency bands. They generally are mounted on a tripod or other type of brace, which is anchored to the earth, pad or roof, or attached to a structure such as building. Cables connect the antennae to the actual transmit/receive equipment. The terrestrial antennae support a single frequency band for example, C–band, Ku–band or Ka–band. The higher the frequency bands the smaller the possible size of the dish. Therefore, while C–band TV dishes tend to be rather large, Ku–band DBS (Direct Broadcast Satellite) TV dishes tend to be very small. The space segment dishes are mounted on a satellite, of course. The satellite can support multiple transmit/receive dishes, depending on the various frequencies, which it employs to support various applications, and depending on whether it covers an entire footprint or divides the footprint into smaller areas of coverage through the use of more tightly focused spot beams. Satellite repeaters are in the form of number of transponders. The transponders accept the weak incoming signals, boost them, shift from the uplink to the downlink frequencies, and transmit the information to the earth stations.

Notes

- ***Bandwidth:*** Satellites can support multiple transponders and, therefore, substantial bandwidth, with each transponder generally providing increments in bandwidth.
- ***Error Performance:*** Satellite transmission is susceptible to environmental interference, particularly at frequencies above 20 GHz. Sunspots and other types of electromagnetic interference affect satellite and microwave transmission. Additionally, some satellite frequency bands, for example, C–band needs careful frequency management. As a result of these factors, satellite transmission often requires rather extensive error detection and correction capabilities.
- ***Distance:*** Satellite is not considered to be distance limited as the signal largely travels through the vacuum of space. Further each signal travels approximately 36,000 kms in each direction.
- ***Propagation Delay:*** Geostationary satellites, by virtue of their high orbital altitude, impose rather significant propagation delay on the signal. Hence, highly interactive voice, data, and video applications are not effectively supported via two-way satellite communications.
- ***Security:*** As is the case with all microwave and other radio systems, satellite transmission is inherently not secure. Satellite transmission is especially vulnerable to interception, as the signal is broadcast over the entire area of the footprint. Therefore, the unauthorized user must know only the satellite and associated frequency range being employed. Security must be imposed through encryption (scrambling) of the signal.
- ***Cost:*** The acquisition, deployment, and rearrangement costs of the space segment of satellite systems can be quite high in several million rupees. However, the satellite can be shared by a large number of users, with each user perhaps connecting a large number of sites. As a result, satellite networks often compare very favorably with cabled systems or microwave systems for many point-to-multipoint applications.
- ***Applications:*** Satellite applications are many and increasing rapidly as the traditional voice and data services have been augmented. Traditional international voice and data services have been supplanted to a considerable extent by submarine fiber optic cable system.

Traditional, applications include international voice and data, remote voice and data, television and radio broadcast, maritime navigation, videoconferencing, inventory management and control through VSATs, disaster recovery and paging. More recent and emerging applications include air navigation, Global Positioning Systems (GPS), mobile voice and data because of Low Earth Orbit Satellites (LEOs), Advanced Traffic Management Systems (ATMS), Direct Broadcast Satellite (DBS) TV, Integrated Digital Services Network (ISDN), interactive television, and interactive multimedia.

Self Assessment

Match the following:

S. No.	Column A	S. No.	Column B
1	C–band	1	14 GHz/11 GHz
2	Radio Waves	2	30 GHz/20 GHz
3	Ku–band	3	Satellite Communication
4	Global Positioning System (GPS)	4	3×10^8 meter per seconds.
5	Ka–band	5	6 GHz/4 GHz

Notes

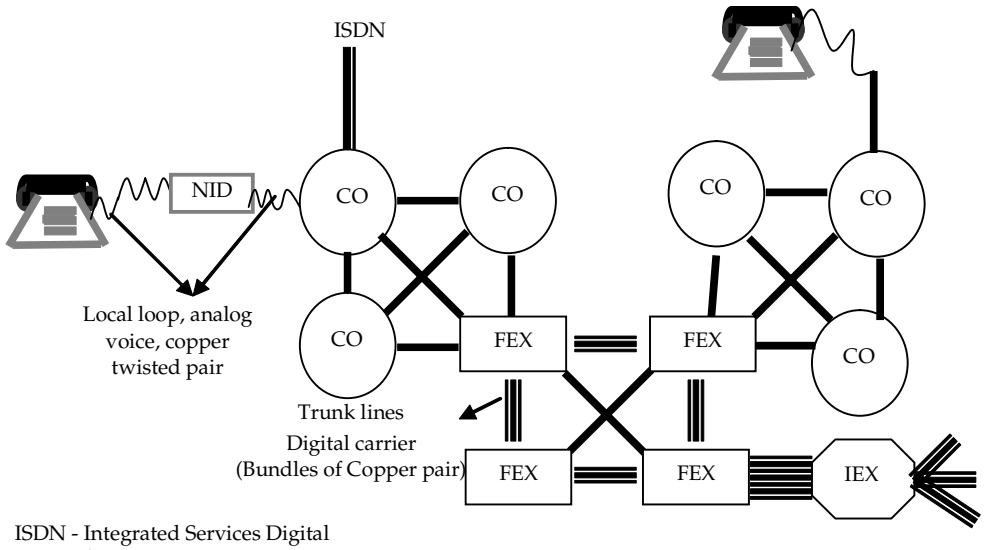
4.3 Public Switched Telephone Network

Generally, a telephone system found in home and offices is a part of the Public Switched Telephone Network (PSTN). It is accessed by telephones, private branch exchange trunks and data arrangements. Hence, PSTN may be referred as a public communication system that provides local, extended local and long distance telephone service to the subscribers. The PSTN uses a circuit-switched telephone almost similar to the IP-based packet-switched network for Internet. The PSTN is made available to the public through a group of common communications carriers who have agreed to exchange calls and connections on behalf of their subscribers as per the international law and the laws of the country of operation.

Notes Originally, PSTN was based on analog circuits but it is now entirely digital in nature and includes fixed line and mobile telephone services.

The PSTN follows technical standards developed by the ITU-T. Its telephone numbers are based on E.163/E.164 addresses. The PSTN has several telephone exchanges networked together to form a nationwide and worldwide) telephone communications system. All telephones in the PSTN are networked in such a way that any phone can make a call to any other phone within the country or outside the country as per international laws prescribed by ITU.

Figure 4.4: PSTN Structure



ISDN - Integrated Services Digital Network
NID - Network Interface Design
CO - Central Office
FEX - Foreign Exchange
IEX - International Exchange

A phone or telephone set acts as an interface device to provide the interface to the PSTN. It enables a subscriber to dial a phone number to make a call. The simple layout of the PSTN as shown in the Figure 4.4 is consisted of the following components:

(a) ***Telephone Set:*** The telephone set provides the dialing function and converts the voice to electrical signal so as to traverse through copper wires and other associated circuits to

Notes

reach at destination. The telephone set at destination converts the electrical signal on the line back into the voice of the calling party. The phone set has passed through various developmental stages from simple magneto systems to electromechanical system to digital system.

(b) ***Local Loop:*** Last mile connections or a local loop (a drop wire from home phone to a connection box of local telegraph pole or cable at the street) is the physical wiring to connect the telephone subscriber to the PSTN. This line may carry voice or data signal or both. The physical wiring for the local loop consists of a pair of twisted copper wires from the telecom service provider's central office (CO) to the subscriber's premise and another pair of twisted copper wires from subscriber's premise to the CO, thus making a loop. The subscriber's telephone connection goes to a connection box outside home that also collects drop wires from other houses in the same area. This connection box is referred to Network Interface Device (NID).

(c) ***NID:*** The NID provides a duplex connection between the home wiring to the local loop wiring to the CO over which an analog electrical signal is passed. The voice signal produced by the microphone in the subscriber's telephone set is converted into a series of electrical pulses to form an analog signal. The house wiring enables this analog signal to reach NID so that it may be passed to the RCU (Remote Concentrator Unit) of CO through local loop wiring.

(d) ***CO:*** At CO, thousand pairs of copper cables merge forming bundle sets of 26 pairs of wires which are split into individual pairs and then punched down into punch blocks mounted on subscriber or loop side in a distribution frame. The other side of the distribution frame is wired to digital cross connect switches to connect the phone calls to the other part of world. Time division multiplexing devices are provided within cross connect switches to multiplex multiple channels into a single higher speed circuit. Some examples are that 24 DS0 circuits are converted to a T1 circuit.

The telephone exchange is considered as a set of one or more cross-connect switches in one or more central offices to respond to a single three digit code. The first three digit code specifies the exchange of the subscribers to which they belong. A central office may serve more than one exchange. A foreign exchange is any exchange outside the subscriber's calling area exchange or local exchange and connected to a local exchange through large, high-speed trunk lines preferably T3 or better. The foreign exchange is referred to extended local calling area.

A foreign exchange is considered as any exchange in a circuit-switched telephone system outside the subscriber's local exchange's calling area. Another local exchange, national exchange and international exchange are examples of a foreign exchange. When a subscriber calls a telephone number outside the local exchange, the subscriber's call is completed by opening a connection to another exchange over a trunk line. The external exchange facilitating the completion of the call is referred to as a foreign exchange.

The national exchange provides connections from the regional telephone providers to the long-distance telephone providers. This exchange defines the area code. The international exchange is the point at which the long distance providers connect to other long distance providers overseas. The international exchange provides country codes. An example of dialing number for Johannesburg, South Africa from U.S.A. will look like as follows:

Country Code	Area Code	Exchange Code	Number
27	11	xx	xxxxxxx

The International dialing codes are comprised of country codes (World Zones), area codes, exchange codes and local numbers.

Notes

4.3.1 Digital Channel

Original telephone networks were based on analog voice connections through manual switchboards. Gradually, digital switch technologies were used to connect digital circuits between exchanges with analog two-wire circuits to connect to most telephones. The basic digital circuit uses Digital Signal 0 (DS0) that is 64 kilobits per second channel to carry a typical phone call from a calling party to a called party. It uses 8-bit Pulse Code Modulation (PCM) with 8 kHz sample rate to digitize the audio sound ranging from 30 Hz to 3300 Hz. In addition to this a guard band of 70 Hz is used to keep the voice clean and clear. Thus, audio sound ranges from 0 Hz to 4,000 Hz. According to sampling theorem, a sampling of twice of the audio signal is required to reproduce the sound. The sound signal is sampled at the rate of 8000 times per second.

4.3.2 Trunk Lines

The trunk lines in telecommunications that are always digital in nature provide high-speed connection between central offices in the PSTN system. The twisted pair wiring between central offices were prone to crosstalk and noise. The twisted pair was also expensive to lay from CO to CO. Gradually development in telecommunication field led to the development of TDM techniques to carry the data over the existing copper lines and subsequently on the optical fiber cables. The fiber cables uses statistical time-division multiplexing, synchronous digital hierarchy, coarse or dense wave division multiplexing and optical switching to further improve transmission speeds. The trunk lines therefore contain thousands of simultaneous calls that have been combined using TDM to carry them from one CO to another CO. A signaling protocol SS7 is used to transmit call from one telephone exchange to another. At CO, they are de-multiplexed and switched through digital access cross connecting switches to reach the proper exchange and local phone number. Some of the examples of trunk lines are T1, T3, DS1, DS3, Tie line, Tie trunk, etc.

T1: A T1 that is considered a dedicated circuit is available as full T1, channelised T1 and fractional T1. A T1 circuit is composed of the local loop of the local service provider and the carrier circuit provided by the same company or different service providers. A full T1 service often referred to as a digital trunk line is usually available as a complete circuit of up to 1.544Mbps total speed either as data or voice but not both. A channelised T1 as it name indicates contains 24 individual channels which are capable of carrying voice or data. The full set of channels provides the same speed as a full T1. The individual channels may be divided into voice lines for telephone services or data lines for Internet services using a device called a Channel Service Unit/Data Service Unit or CSU/DSU. A fractional T1 is available less than a full T1's bandwidth in which one or more channels bundled together. Similar to the channelised T1, individual channels can be voice or data and a CSU/DSU is used to split the channels. A T1 circuit always remains on and therefore is referred to as private lines or dedicated data line.

DS1: Digital Signalling Level 1 (DS1) contains 24 voice TDM into 192-bit frames across single physical connection providing 1.544 Mbps data throughput across a T1 Physical Layer digital voice connection.

DS3: Refers to a telecom circuit that carries multiple calls from one central office to another and also termed as tie trunks or tie lines. A DS3 contains the equivalent of 28 T1/DS1 circuits by decreasing the time slicle allotted for each sample of data and multiplexes the T1's together to form the final DS3 data stream.

4.4 Mobile Telephone System

Notes

The development of mobile telephone system or cellular phones is recent one. This is also known as mobile phone and as its name implies it is designed for mobile users who need to make telephone calls from different locations when they are usually away from home or office. The rapid development in hardware technology helps in designing such kind of portable telephone sets as shown in Figure 4.5 so that user may carry it within their office bag or pocket during movement. Cellular phone uses radio frequencies to talk to a nearby cell site. Cell site acts as an access point for cellular calls and the cellular phone regularly communicates with the nearest cell site to inform the network that it is connected.

Figure 4.5: Cellular Phone

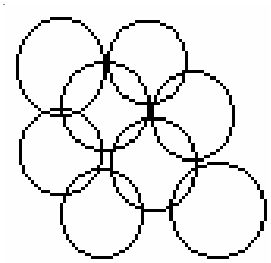
Cell Site

This may be defined as a circular geographical area that handles cellular phones within its defined physical boundary. A cellular network as shown in Figure 4.5 is considered consisting of overlapped cells so that a larger area with low probability of call dropping may be provided. This overlapping structure helps in keeping the call intact as a user moves location from one cell site to another. In this case, the call is transferred to the nearest cell site responsible for that physical area.

Cellular telephones are suitable for larger geographical areas including remote sites. It saves the cost of copper wire and efforts in laying the same in densely populated areas.

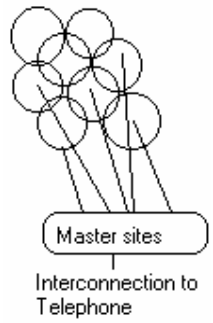
Each cell site shown in Figure 4.6 is connected to a master site, which acts as an access point for a particular cellular network. Master site furnishes an interconnection to the regular telephone network. Calls handled by each cell site are relayed back to the master cell site, which then relays it to the telephone network as shown in Figure 4.7

Figure 4.6: Cellular Network Consisting of Individual Cells



Notes

Figure 4.7: Cellular Network Connection to Telephone Exchange



The forward cell can reuse frequencies used in the previous cell. This helps in sharing the same frequency band. Many calls can be handled by one frequency especially where digital phones are used.

4.5 Cable Television

Cable television or Cable TV uses coaxial cable as the transmission media to transmit television programs to televisions at home or office. Conventional television uses over-the-air broadcasting of signal using radio waves to transmit television programs to television receivers. This system requires a television antenna. On the other hand, cable television system uses radio frequency signals over fixed optical fibers or coaxial cables to transmit television programs to the consumers. Other applications of cable television are FM radio programming, high-speed Internet, telephony, etc.

Did u know? Using coaxial cables provide several advantages because of its huge bandwidth; transmission of bi-directional signal and large amounts of data is possible. Cable television signals require small bandwidth of coaxial lines. Hence, remaining bandwidth may be used for other digital services such as broadband Internet and cable telephony.

Broadband Internet over Coaxial Cable: It is possible because of cable modems that convert the internet data into digital signal that can be transferred over coaxial cable.

Cable Telephone Services: A special telephone interface is installed at the customer's premises to convert the analog signals from the customer's in-home wiring into a digital signal. The analog signal is then sent on the local loop to the switching center. Its advantages include need of less bandwidth, better voice quality and integration to a VoIP network.

Cable Modem

Cable modem works on the principle of modems and provides access to data signal sent through the cable television infrastructure. Cable modems delivers broadband Internet access in the form of cable Internet, taking advantage of unused bandwidth on a cable television network using coaxial cable or optical fiber cable. A cable modem works like a bridge in accordance with IEEE 802.1D for Ethernet networking. The cable modem forwards Ethernet frames between a customer LAN and the coaxial cable network.

Task Give a brief description of the application and limitations of the wireless communication and compare it with bounded transmission media.

Self Assessment

Notes

Fill in the blanks:

6. The velocity of transmission of energy in free space is .....
7. ..... is a serious problem in microwave communication systems.
8. Satellite systems send signals high above the earth from .....
9. The uplink frequency and the down frequency are kept different in satellite communication systems to .....
10. ..... is a larger transmission line that carries data gathered from smaller lines that interconnect with it.
11. ..... a circular geographical area that handles cellular phones within its defined physical boundary.
12. 10-12 GHz microwave frequency range will have maximum antenna separation in the range of ..... for digital transmission.
13. A cable operator usually pick ups TV signal from ..... before distributing it to its subscribers.

4.6 Summary

- There are several kinds of transmission media. These media technologies starting from copper wire to wireless and fiber optic has grown-up so rapidly and replacing other very quickly in this information age. It may be seen that the Public Telephone Switched Network (PSTN) had been evolved from the early use of coaxial cable to interconnect main centers. Gradually, these were replaced with the use of microwave stations because of the cost of copper and related infrastructure.
- Long distance communication could be made affordable, feasible and reliable using high microwave towers coupled with the repeater stations at specified distances. This involves less maintenance and improved reliability because of aerial interface instead of physical lines in the form of coaxial cables. This long distance communication was strengthened with easy availability of omnipresent satellites in sufficient numbers. The satellite communication has large delay problem.
- Now fiber optic cables are being used as a preferred means of interconnecting main centers together. This does not mean that these new media like fiber optic and satellite has completely outdated conventional one. In fact, in this information age, each media is suited to different purposes and each has their place.
- Mobile communication can also be seen in the same perspective, as these services should be available anytime at anywhere.

4.7 Keywords

Cable Modem: It works on the principle of modems and provides access to data signal sent through the cable television infrastructure.

Cell Site: A circular geographical area that handles cellular phones within its defined physical boundary.

Notes

Downlink Frequency: It is the frequency used to transmit the signal from satellite to earth station.

Local Loop: Two sets of wires create a duplex connection between the subscriber's premises and the CO over which an analog electrical signal is passed.

Microwave Radio: It is a form of radio transmission that uses ultra-high frequencies.

PSTN: It may be referred as a public communication system that provides local, extended local and long distance telephone service to the subscribers.

Radio: A technique where data is transmitted using radio waves and therefore energy travels through the air rather than copper or glass.

Trunk Line: It refers to the high-speed digital connection between telephone and CO in the PSTN.

Uplink Frequency: It is the frequency used to transmit signal from earth station to satellite.

Very Low Frequency: It uses electromagnetic radiation generated in the low frequency band of 3-30 kHz.

4.8 Review Questions

1. Describe how satellite communication is different from radio broadcast?
2. Write down any two advantages and disadvantages of using satellite communication.
3. How do cells in mobile communication ensure a low probability of call droppings?
4. How is the microwave signal strengthened to its maximize value to increase the distance of transmission at acceptable levels?

Answers: Self Assessment

1.	5	2.	4
3.	1	4.	3
5.	2	6.	c =
7.	Multipath fading	8.	Ground stations
9.	To avoid interference	10.	Trunk
11.	Cell site	12.	16-24 Km
13.	Satellite		

4.9 Further Readings

Books

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall

Behrouz A. Forouzan and Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies

Rajneesh Agrawal and Bharat Bhushan Tiwari, *Computer Networks and Internet*, Vikas Publication

Unit 5: Networking Devices

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Describe various types of networking devices.
- Discuss concept of routers and their classification
- Describe what are hubs, switches, bridges and gateways.
- Explain different types of switching techniques such as circuit switching, message switching and packet switching.

Notes

Introduction

Network devices are components used to connect computers or other electronic devices together so that they can share files or resources like printers or fax machines. Devices used to setup a Local Area Network (LAN) are the most common type of network devices used by the public. A LAN requires a hub, router, cabling or radio technology, network cards, and if online access is desired, a high-speed modem.

5.1 Routers

Routers are used to connect both similar and dissimilar LANs, as shown in Figure 5.1. Router operates on the network layer of OSI model using the physical layer, data link layer and network layer to provide connectivity, addressing and switching as shown in Figure 5.2. These are highly intelligent devices. In case of TCP/IP network, Internet Protocol (IP) is used as addresses for network; this is the router who interprets the IP address and delivers the packet reliably. Now we may say that router transmits the network layer data and therefore provides transmission of data between LANs that use different data link protocols but using the same network layer protocol. Because of this Ethernet can be connected with token ring network using routers. Additionally, routers provide connectivity to MAN (SMDS) and WAN (X.25, Frame Relay and ATM). Routers are protocol sensitive, typically supporting multiple protocols and large and varying packet sizes such as might be involved in supporting both Ethernet and Token Ring.

A network consisting of routers can have multiple paths unlike bridges. Normally the shortest of all paths in the network is used to transfer packets.

Figure 5.1: Router Network

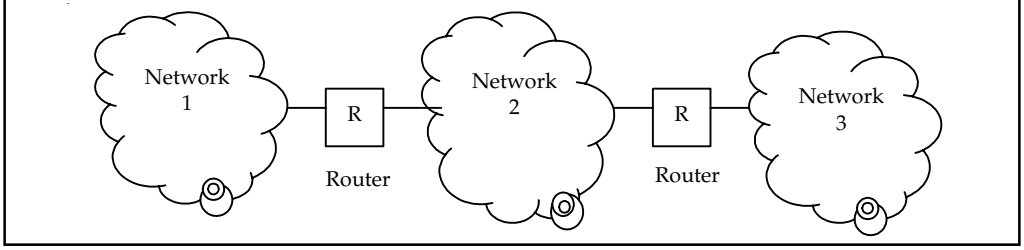
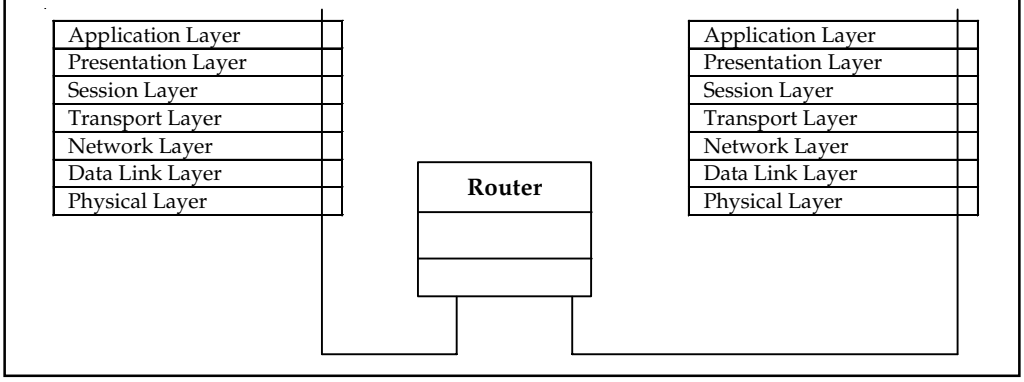


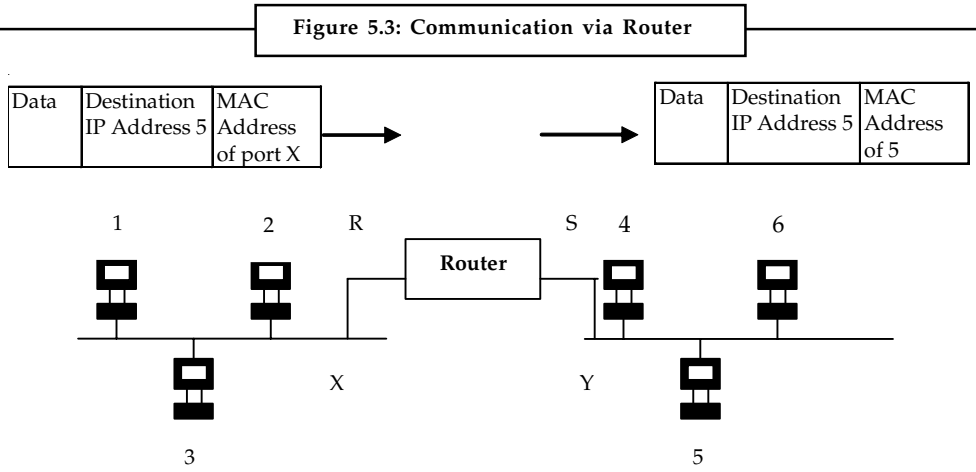
Figure 5.2: OSI Correspondence in Case of Routers



Notes

Consider a case for data transmission from Computer 1 to Computer 5 on the network shown in Figure 5.3. When Computer 1 starts sending the data, it compares its IP address with Computer 5 i.e. destination computer addresses to know whether Computer 5 lies on its own network or not. When Computer 1 finds that it is not on its network it transmits a data packet containing the MAC address R of router in this case. When router receives this packet it sets the MAC address of Computer 5 and sends the packet to the port which has the same IP destination address as given in data packet. In this manner Computer 5 receives the data packet.

Figure 5.3: Communication via Router



Routing Table

Network Address	Port
240.0.0.0	X
241.0.0.0	Y

5.1.1 Characteristics of Routers

1. Routers are multiport devices with high-speed backbones.
2. Routers also support filtering and encapsulation like bridges.
3. Like bridges routers are also self-learning, as they can communicate their existence to other devices and can learn of the existence of new routers, nodes and LAN segments.
4. Routers route traffic by considering the network as a whole. It shows that they use a high level of intelligence to accomplish this task. This characteristic makes them superior than hubs and bridges because they simply view the network on a link-by-link basis.
5. The packet handled by router may include destination address, packet priority level, least-cost route, minimum route delay, minimum route distance, and route congestion level.
6. Routers constantly monitor the condition of the network, as a whole to dynamically adapt to changes in the condition of the network.
7. They typically provide some level of redundancy in order that they are less susceptible to catastrophic failure.

Notes

5.1.2 Router Protocols

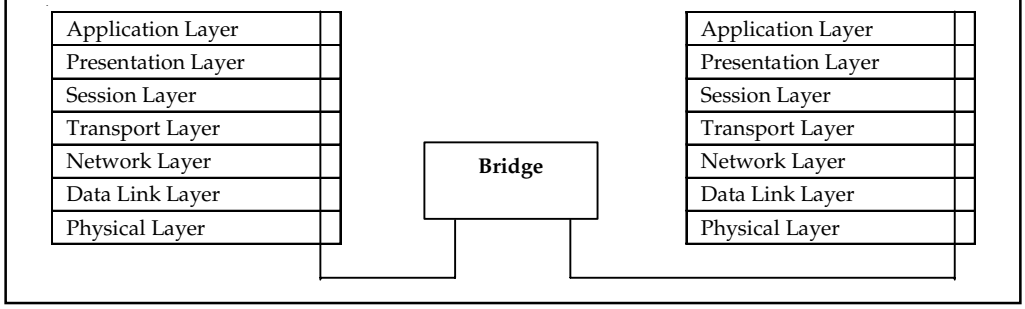
Router protocols consists of both bridging and routing protocols as listed below:

1. ***Inter-router Protocols:*** These are router-to-router protocols that can operate over dissimilar networks. This protocol routes information and stores data packets during periods of idleness.
2. ***Serial Line Protocols:*** This protocol is widely used over serial or dialup links connecting unlike routers. Examples include HDLC, SLIP (Serial Line Interface Protocol), and PPP (Point-to-Point Protocol).
3. ***Protocol Stack Routing and Bridging Protocols:*** This advises the router as to which packets should be routed and which should be bridged.

5.2 Bridges

Like repeaters, bridges are used to connect similar LANs together, for example, Ethernet-to-Ethernet and operate at the bottom two layers of the OSI model i.e. physical layer and data link layer as shown in Figure 5.4. As it operates on second layer of the OSI model therefore it relays only necessary data to other signals. MAC addresses (physical addresses) are used to determine whether data is necessary to transmit to other LAN segments or not. It passes information from one LAN segment to another based on the destination address of the packet. In other words, when a bridge receives data through one of its ports, it checks the data for a MAC address. If this address matches that of the node connected to other port, the bridge sends this data through this port. This action is called forwarding. If the address does not match with any node connected to other port, the bridge discards it. This action is called filtering. This is shown in Figure 5.5. Unlike repeaters, bridges have buffers to store and forward packets in the event that the destination link is congested with traffic.

Figure 5.4: Bridge and OSI Reference Model Correspondence



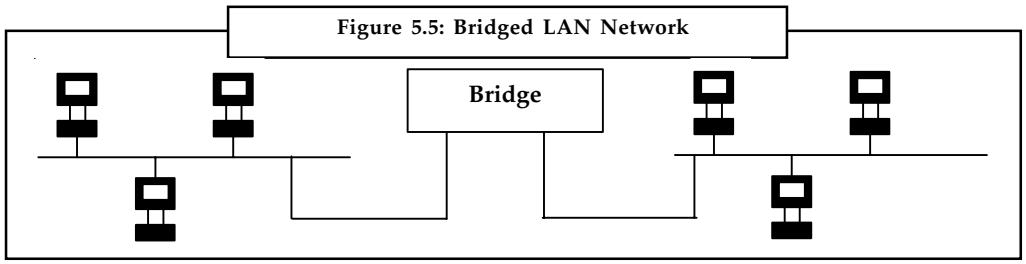
The main advantage of bridge over repeater is that it has filtering action. If any noise on Ethernet occurs because of collision or disturbance in electrical signal, the bridge will consider it as an incorrectly formed frame and will not forward to the segment connected to other port of the bridge.

Notes Note that bridge can relay broadcast packets and packets with unknown destination.

As you know that the maximum four repeaters can be used to connect multiple Ethernet segments. However, if a bridge is provided between repeaters, this limit of four is increased. The maximum number of bridges is not specifically limited.

Notes

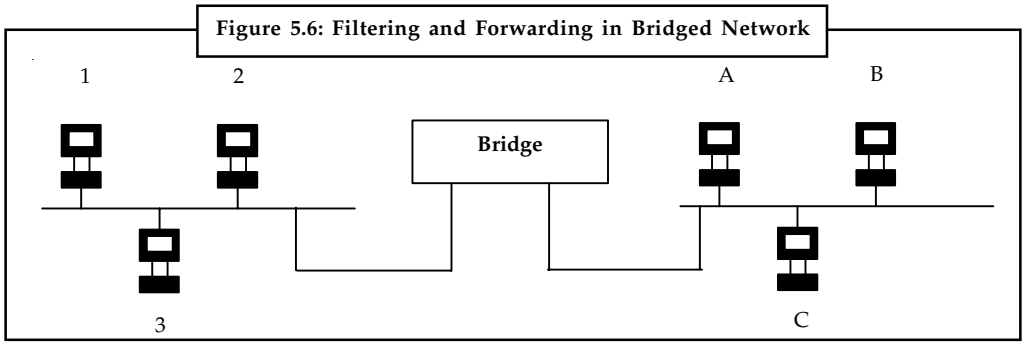
Figure 5.5: Bridged LAN Network



From architecture point of view bridges are protocol independent devices and are very simple. They do not perform complex processes on the data packets traveling through them such as the evaluation of the network as a whole in order to make end-to-end routing decisions. They simply read the destination address of the incoming data packet and forward it along its way to the next link. Therefore, bridges are inexpensive and fast. There are bridges called cascading bridges are used to support multiple LANs connected by multiple media.

Dissimilar LANs such as Ethernet-to-token ring can also be connected with the help of bridge known as encapsulating bridge. The function of encapsulating bridge is also very simple. It encapsulates the originating LAN data along with control information of the end user LAN. Bridges with routing function between LANs are also available.

Figure 5.6: Filtering and Forwarding in Bridged Network



Computer 1 in the Figure 5.6 wishes to talk to Computer 3 on the same network. The packet sent by Computer 1 will contain the physical address of Computer 3 that will also received by the bridge device connecting the two LAN segments. The bridge will read the physical address contained in the packet and observe that this address belongs to the computer on the same LAN segment. Hence bridge will filter this packet and will not allow it to be transmitted on other side of the network. In case Computer 1 wishes to talk with Computer C on other segment, the bridge will know from its table of addresses that this address belongs to the computer attached to other segment of the network. In this case, this will be forwarded to the other segment of the LAN. The bridge learns location of computers attached to the network by watching frames. This will be explained later on in the subsequent discussion. Note that in case of broadcast and multicast packets, bridge forwards these packets to all computers attached to the segment on both sides.

Media Access Control (MAC) Bridge

This is used to connect dissimilar LANs such as Ethernet-to-token ring using encapsulation or translation. This bridge translates the original packet format from the requesting LAN segment by encapsulating or enveloping with control data specific to the protocol of the destination LAN segment.

Notes

Address Table

As explained above, each bridge should have an address table that indicates the location of different computers or nodes on the segments of LAN. More specifically, it indicates the connection between nodes and ports. When a bridge is booted first time, this table is found to be blank. Now this question arises how this table is filled with appropriate addresses of different nodes attached to ports. Most of the bridges are called adaptive or self-leaning bridges because they learn the location of the node and associated port themselves and make a list of nodes attached each segment.

When a bridge receives a data packet from a computer, it first copies the physical address of that computer contained in the packet into its list. Afterward, bridge determines whether this packet should be forwarded or not. In other words, the bridge learns the location of the computer on the network as soon as the computer on the network sends some packet.

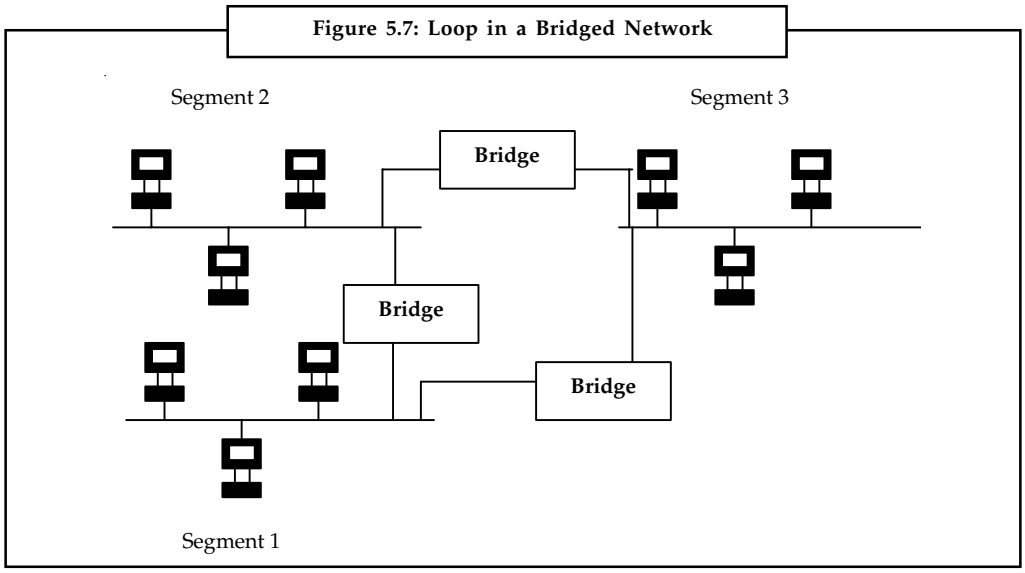
If a computer does not send a packet, the bridge will never be able to determine its position and unnecessarily forwards the packet on network. Fortunately, this cannot happen because a computer with network software attached to a network transmits at least one frame when the system first boots. Furthermore, computer communication is bi-directional, there is always an acknowledgement for each received packets.

5.2.1 Bridge Protocols

Bridge protocols include spanning tree, source routing protocol, and source routing transparent.

Spanning Tree Protocol (STP) Bridge: This is also known as adaptive or self-learning bridges and is defined in IEEE 802.1 standards. It has already been explained in the above section. Ideally, in bridged network, the network tree of the bridge provides only one span (link) for each LAN-to-LAN connection and therefore no network with bridges can form a loop. Sometimes looping can occur. This can be explained with the help of the Figure 5.7.

Figure 5.7: Loop in a Bridged Network



A broadcast data packet sent by the computer attached on segment 1 can reach to all computers attached on segment 2 and 3 without a connection between segment 1 and 3 as shown in Figure 5.7. Sometimes, the bridge connection between segment 1 and 3 or like is provided to give the network more redundancy. Now in this case the same broadcast packet sent by the segment 1 will reach to segment 3 by two routes i.e. from segment 1 to 2 to 3 and another by segment 1 to 3.

Notes

In this manner the computers on segment 3 will receive duplicate packets. In case of large networks some segments may receive many packets and thus causing looping.

A loop, therefore, can cause a broadcast packet or a packet with an unknown destination to circulate through it, thus rendering the network inoperable. This condition is avoided by making some bridges not to forward frames. An algorithm known as Distributed Spanning Tree (DST) accomplishes this task. This algorithm decides which bridge should forward the packets in the network. Under this scheme bridges exchange a control message known as a hello message to select a single transmission route. Remaining bridges maintain a standby position and provide alternate path in case of the some bridge fails in the selected transmission path. In Figure 5.8 bridge connecting segment 1 and 3 will be active only if the bridge connecting segment 2 and 3 fails otherwise it acts as a standby bridge for network. In other words, bridges that support the spanning tree algorithm have the ability to automatically reconfigure themselves for alternate paths if a network segment fails, thereby improving overall reliability.

IBM Source Routing Protocol (SRP) Bridge: These are programmed with specific routes for each packet based on considerations such as the physical location of the nodes, and the number of bridges involved.

Source Routing Transparent (SRT): It is defined in the IEEE 802.1 standard. It is effectively a combination of STP and SRP. The SRT router can connect LANs by either method, as programmed.

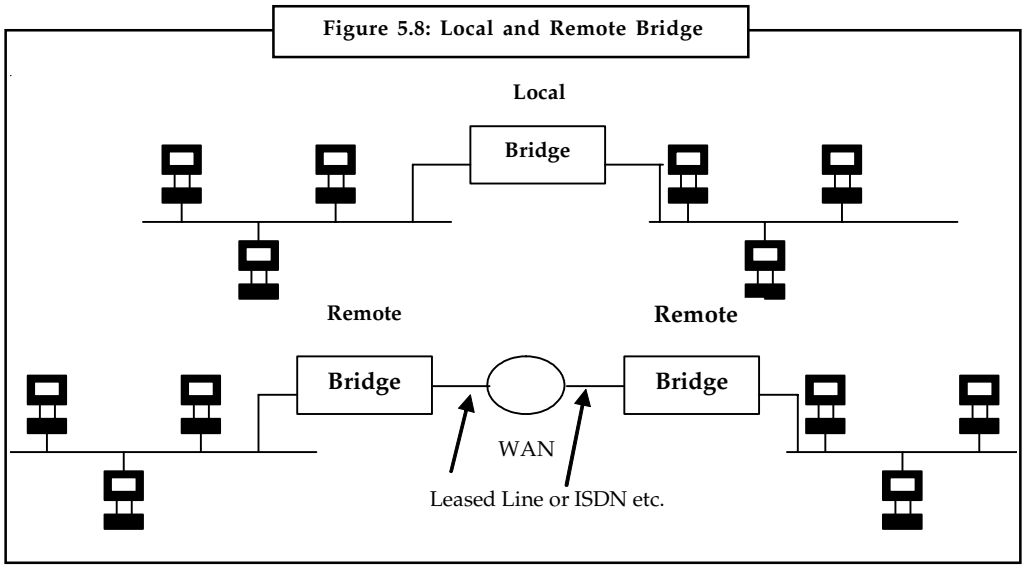
5.2.2 Classification of Bridges

These are classified into local and remote bridges:

- Local brides are ordinary bridges
- Remote bridges are used to connect networks that are far from each other. A WAN is generally provided between two bridges.

Figure 5.8 shows the local and remote bridge connection.

Figure 5.8: Local and Remote Bridge



Task What are bridges? What are different types of bridges?

Notes

5.3 Gateways

Gateway routers are used to connect dissimilar LANs and perform all of the functions of bridges and routers. It operates at all seven layers of the OSI Reference Model as shown in Figure 5.9. These are actually predecessors of nowadays router and are technology wise more expensive and highly functional. They are in general consisting of software, which resides in a host computer, such a midrange or mainframe as shown in Figure 5.9.

Figure 5.9: OSI Correspondence of Gateways

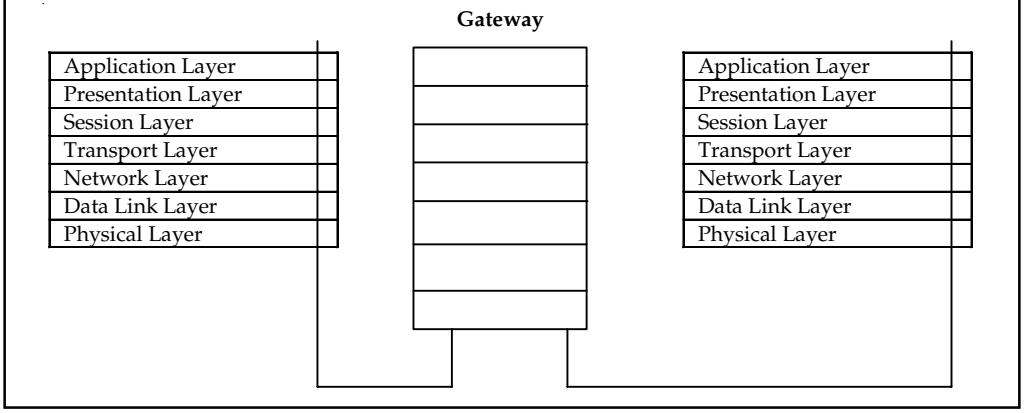
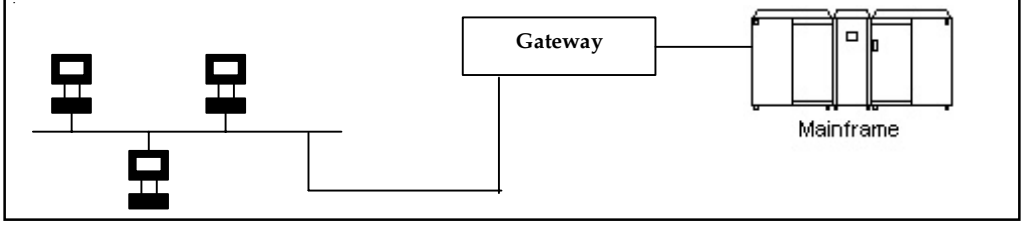


Figure 5.10: Interconnection between Ethernet and Mainframe using Gateway



5.3.1 Characteristics of Gateways

1. Gateways provide full protocol conversion from one proprietary LAN technology to another i.e. ethernet to token ring or FDDI or any other standard or protocol rather than encapsulation.
2. It uses higher layers of the OSI model, perhaps through layer 7, the application layer. IBM SNA, DECnet, Internet TCP/IP and other protocols can be converted from network-to-network.
3. Unlike bridges and routers, gateways operate slowly because of protocol conversion. Consequently, they may create bottlenecks of congestion during periods of peak usage.

5.4 Switches

A switch is a device that incorporates bridge functions as well as point-to-point 'dedicated connections'. They connect devices or networks, filter, forward and flood frames based on the MAC destination address of each frame. Switch operates at datalink layer of the OSI model. They are technically called bridges. They move data without contention. Ethernet switches provide a

Notes

combinations of shared/dedicated 10/100/1000 Mbps connections. Some E-net switches support cut-through switching: frame forwarded immediately to destination without awaiting for assembly of the entire frame in the switch buffer. They significantly increases throughput. They provide express lane for traffic.

Comparison of Switches and Hubs

	Hubs	Switches
1	Collision Domain	Broadcast Domain
2	All of the parts on a hub are part of the same Ethernet	Each part on a switches may be regarded as a separate Ethernet (but all are part of the same local area network)
3	All parts on a hub share the same 10Mb (100 Mb) bandwidth	Each part on a switch has its own 10Mb (100 Mb) bandwidth
4	Any frame appearing on one port of a hub is repeated to all other ports on the hub	A directed frame appearing on one part of a switch is forwarded only to the destination port.
5	A sniffer on any hub port can see all of the traffic on the network	Switched networks are difficult to sniff
6	A hub will repeat defective frames	

5.5 Hubs

If multiple incoming connections need to be connected with multiple outgoing connections, then a hub is required. In data communications, a hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions. Hubs are multi-port repeaters, and as such they obey the same rules as rep eaters. They operate at the OSI Model Physical Layer.

Hubs are used to provide a Physical Star Topology. At the center of the star is the hub, with the network nodes located on the tips of the star.

Star Topology

The Hub is installed in a central wiring closet, with all the cables extending out to the network nodes. The advantage of having a central wiring location is that it's easier to maintain and troubleshoot large networks. All of the network cables come to the central hub. This way, it is especially easy to detect and fix cable problems. You can easily move a workstation in - a star topology - by changing the connection to the hub at the central wiring closet.

The disadvantages to a star topology are given below:

1. Failure of the Hub can disable a major section of the network.
2. The Star Topology requires more cabling than does the ring or the bus topology because all stations must be connected to the hub, not to the next station.

5.5.1 Hub's Segment-to-Segment Characteristics

To understand the Ethernet segment-to-segment characteristics of a hub, let us first determine how the Ethernet Hubs operate. Logically, they appear as a Bus Topology, and physically as a

Notes

Star Topology. Looking inside an Ethernet Hub, we can see that it consists of a electronic printed circuit board. Understanding that inside the Hub is only more repeaters, we can draw the conclusion that all connections attached to a Hub are on the same Segment (and have the same Segment Number). A single repeater is said to exist from any port to any port, even though it is indicated as a path of 2 repeaters.

Cascaded Hub Network

Connecting Hubs together through ports creates Cascading Hubs. One Master Hub (Level 1) is connected to many Level 2 (Slave) Hubs, who are masters to Level 3 (Slave) Hubs in a hierarchical tree (or clustered star). The maximum number of stations in a Cascaded Hub Network is limited to 128.

Backbone Networks

In a Backbone Network, there is no Master Hub. The Level 1 Hubs are connected through their AUI port to a Coax Backbone. For Thin Coax, up to 30 Hubs can be connected together. For Thick Coax, up to 100 Hubs can be connected to the backbone. The Backbone is considered to be a populated segment.

Level 2 Hubs are allowed to be connected to the Level 1 Hubs' 10 BaseT ports. This connection between the 2 Hubs is considered an un populated segment, or link segment. Up to 1024 stations (or nodes) can be attached to the Level 2 Hubs' 10 BaseT ports. All stations and segments would appear as one logical segment, with one network Number.

Caution In the real world, 1024 stations are never attached to one segment; as the resulting traffic would slow the network to a crawl.

5.5.2 Hub's Addressing

Because a Hub is just many repeaters in the same box, any network traffic between nodes is heard over the complete network. As far as the stations are concerned, they are connected on one long logical bus (wire).

Half-Duplex and Full-Duplex Ethernet Hubs

Normal Ethernet operation is Half-Duplex: only 1 station or node is talking at a time. The stations take turns talking on the bus (CSMA/CD -bus arbitration). Full-Duplex Ethernet Hubs are Hubs which allow two-way communication, thus doubling the available bandwidth from 10 Mbps to 20 Mbps. Full duplex Hubs are proprietary products, and normally only work within their own manufacturer's line.

For example, if A wanted to talk to C, a direct 10 Mbps line would be connected through the 2 switching hubs. Simultaneously, if D wanted to talk to B, another direct 10 Mbps line (in the opposite direction) would be connected through the two switching Hubs (doubling the available bandwidth to 20 Mbps). There are no official standards for Full-Duplex Ethernet although proprietary standards do exist.

5.5.3 Switching Hubs

A switch, which resembles a hub, is known as switching hub. But there is stark difference between hub and switching hub or a switch. Hub acts as a LAN concentrators and repeaters.

Notes

It consists of a single box with multiple ports. Each port is connected with a separate computer. A signal transmitted by a computer travels to all ports like a bus topology. With the evolution of bridge technology, a data packet input to one port is first checked for its destination and is outputted accordingly to the respective port. In this manner multiple port can communicate simultaneously with one another using switch.

It can be said, in other words, that a switching hub has multiple buses for multiple LANs as shown in Figure 5.11. The configuration of a switch is shown in Figure 5.12.

Figure 5.11: Switching Hub with Multiple Buses

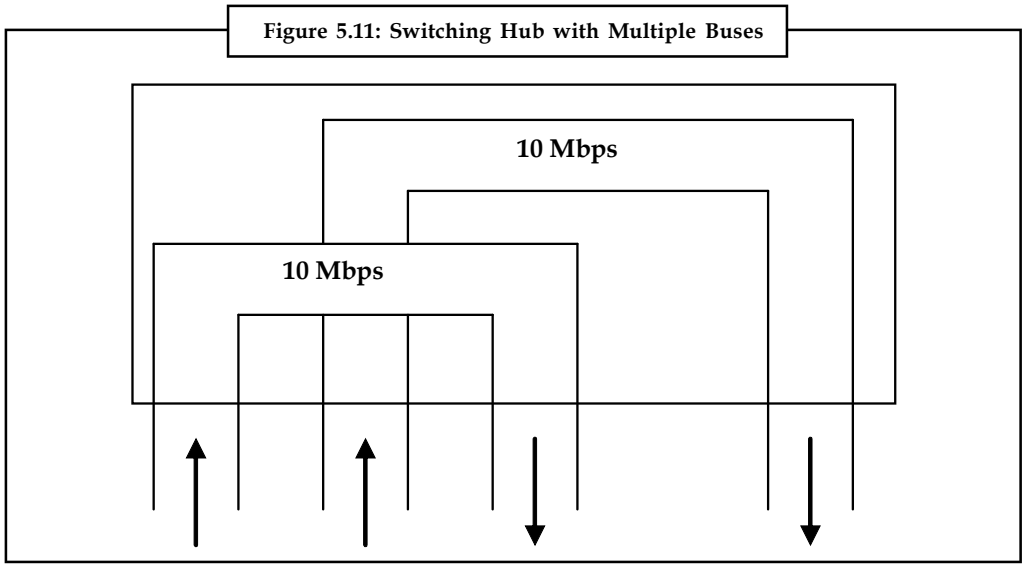
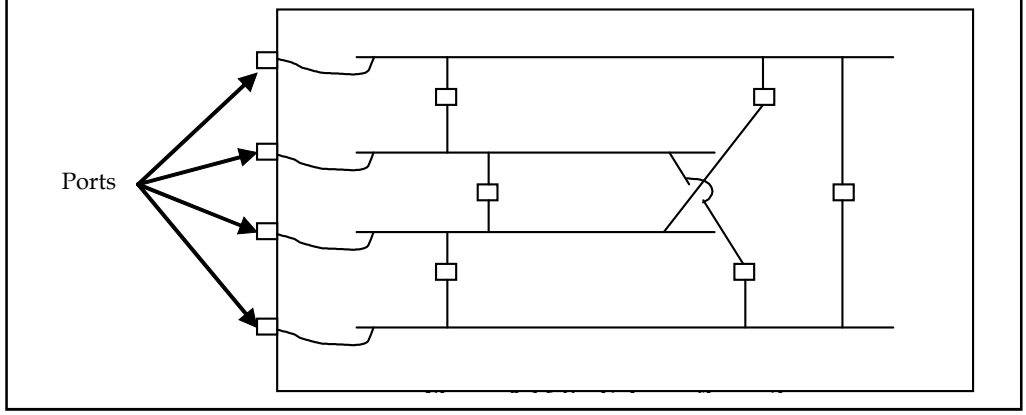


Figure 5.12: Configuration of a Switch



The switching hub interprets the MAC address of the destination computer contained in the data packet and sends the data packet to the appropriate destination computer using appropriate port when hub uses the technique of repeater in doing so. Therefore, switching hub is treated as bridge.

Characteristics of Switching Hub

- A switching hub can operate with multiple media (coaxial cable, UTP, and fiber).
- It can work with different technologies with different speeds.
- It provides routing capabilities too.

Notes

- This is manageable via SNMP (Simple Network Management Protocol) or another appropriate network management protocol.
- Switching hub provides an expanded bandwidth.

Self Assessment

Name the following:

1. A place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions.
2. A device that allows network administrators to segment their networks transparently.
3. A device that incorporates bridge functions as well as point-to-point 'dedicated connections'. They connect devices or networks, filter, forward and flood frames based on the MAC destination address of each frame.
4. Devices used to connect two devices at the network layer of the OSI Model.
5. Devices that are used to connect totally dissimilar networks because they can perform protocol conversion for all seven layers of the OSI Model.

5.6 Switching Techniques

An Ethernet can connect up to only 1024 hosts within a span of only 1500 meters. Therefore, the LAN technologies are not sufficient for building a global network and interconnecting hosts of other networks. In a telephone exchange, a switch provides connection between called and calling party without providing direct line-to-line connection between them. The telephone network uses circuit switching that provides dedicated channel between called and calling party while computer networks use packet switching that does not provide a dedicated channel between the hosts. Figure 5.13 attempts to explain switching technique where any computer may exchange information with any other computer. A switch is used to interconnect different hosts to its several inputs and outputs. The functions of a switch are store and forward, routing and congestion control that are required to accomplish interconnection. The switching techniques enable us to build a MAN or WAN or Internet.

Think how things would be if you could only use your telephone to talk to just one other person! You would not be very productive. So there are requirements for switching systems to route your calls around the world.

There are a number of ways to perform switching:

- Circuit Switching
- Packet Switching
- Message Switching
- Cell Switching

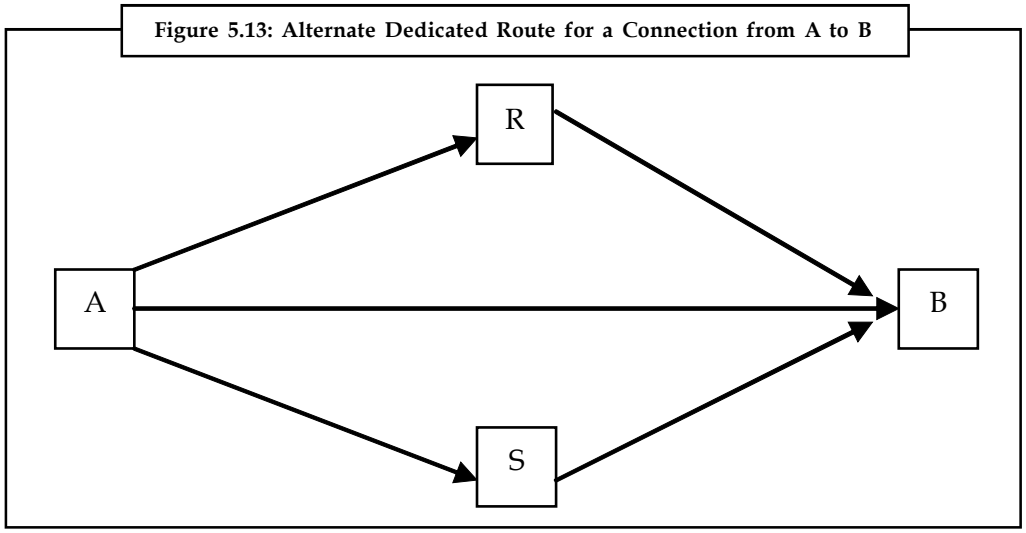
5.6.1 Circuit Switching

The circuit switching technique provides a dedicated physical communication path from source to destination terminal within a network. Therefore, a dedicated bandwidth is created, maintained and terminated for each communication session. The circuit switching session, thus comprises of 3 phases like circuit establishment, data transfer and circuit disconnect. Prior to the data

Notes

transfer, a dedicated connection is established for the transfer of data. At the end of the data transfer, the connection is broken. In this manner, the circuit switching provides a fixed data rate channel for the source and destination devices. The circuit switching technique has disadvantages over packet switching technique because of wastage of bandwidth when there is no data for transmission at any moment of time. Moreover, setting up of connection also takes time. Circuit switching involves datagram and data-stream transmissions. Datagram transmissions have frames that are individually addressed. Data-stream transmissions do not have frames. They have a data stream for which address checking occurs only once. The routing may be either static routing or dynamic routing. Figure 5.13 explains the alternate dedicated routes for the transfer of data from one host to anther.

Figure 5.13: Alternate Dedicated Route for a Connection from A to B



Initially, the circuit switching was developed for voice traffic and found applications in telephone networks to provide a dedicated physical circuit from the beginning of the call to the end of the call. Integrated Services Digital Network (ISDN) is an example of a circuit-switched WAN technology.

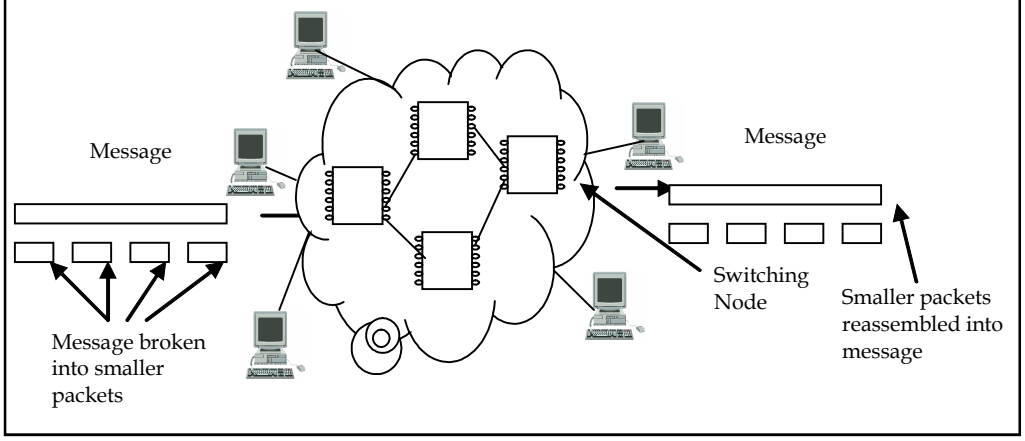
Notes There are three switches methods of circuit switching which are Cut-through, Store and forward and the last is Fragment-free switching.

5.6.2 Packet Switching

The packet switched data networks divides data into one or more message units, called packets at source host before transmitting it to the destination host. The packets have varying length and they include the source and destination addresses and the necessary control information. In a switched network, the switching nodes receive the packets and store them briefly before forwarding to the next node. The switching node examines the destination address contained in the packets that are reaching there. Each switching node maintains a routing directory in the form of a table to determine the outgoing links based on the destination addresses of the received packets. The packets finally reach to the destination node and are forwarded to the destination device. The destination device collects all he packets of the same data reaching it to from different routes and arranges them in sequence according to the sequence number contained in each packet.

Notes

Figure 5.14: Packet Switched Network



Unlike circuit switching, the packet switching does not involve dedicated channel for transfer of information hence, it is prone to encounter with errors and damaged or lost packets in the route from source to destination devices. Therefore, error and flow control procedures are applied on each link by the switching nodes. The advantages of packet switching are channel efficiency, no busy conditions and priorities data transmission. The packet-switched networks make more efficient use of available capacity because several users are able to share the available bandwidth. The packet switching datagram treats each packet independently and the packets take any route to reach at the destination irrespective of their sequence numbers. The destination device reassembles the packets to reproduce the message and recover for the missing packets. Packet switching enables to transmit the same information to more than one receiver at the same time. Packet switching also enables communication between terminals that have different transfer rates and different types of interface. The packets are handled using datagram and virtual circuit and permanent virtual circuit methods.

Datagram: It refers to the self-contained packet of data carrying sufficient information to route it reliably from source to destination devices following any arbitrary route. The destination device collects and reassembles out of the packets in order to reconstruct the information. Chances are that some packet may be lost. The receiving device then requests for missing packets.

Virtual Circuit and Permanent Virtual Circuit

It refers to create virtual connection between source and destination devices. This is in contrast to the circuit switching that creates a dedicated physical connection. The virtual connection so created may either be connection oriented or connectionless. Datagram is an example of connectionless communication. Packet switching uses two types of virtual connections. They are Switched Virtual Circuit (SVC) or Virtual Circuit (VC) and Permanent Virtual Circuit (PVC).

(a) ***Virtual CIrcuit (VC) Connection:*** Like circuit switching, the source device selects the links or route to be used for sending data to the destination device before communication. The links are disconnected as soon as the packets are transferred.

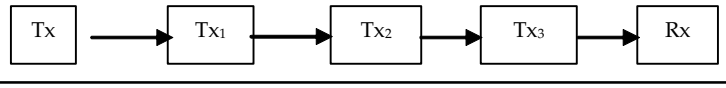
(b) ***Permanent Virtual Circuit (PVC):*** Like leased lines, PVC is a virtual circuit used to establish a long-term connection between sending and receiving end for permanent types of the users who always wish to connect to a logical channel. It eliminates the need for repeated connection set-up and termination. This is provided by the switching nodes that store the information permanently for the transfer of packets between two devices or more.

Notes

5.6.3 Message Switching

In message switching, there is no need for a connection to be established all the way from source to destination. Figure 5.15 shows communication between Tx (sending or transmitting device) and Rx (receiving device) via a number of links as Tx to Tx_1, Tx_1 to Tx_2, Tx2 to Tx_3, Tx_3 to Rx.

Figure 5.15: A Connection between Two Systems Tx and Rx through 3 Links



The switching nodes like Tx1, Tx2 and so on receive the message, store it and forward the message to the adjacent message switching node after creating a connection with the adjacent message switch. Message switching is also known as store-and-forward switching since the messages are stored at intermediate nodes en route to their destinations. The difference between packet switching and message switching may be understood by the size of packets. In case of the packet switching, the size of packet is very short compared to the size of message in message switching. The short size packet takes less time to reach the destination and therefore reassembling of out of order packets does not require a dedicated connection. Thus the packet switching allows packets belonging to other messages to be sent in between other packets. Packet switching uses pipelining to make a continuous flow of packets from source to destination devices via intermediate switching nodes. Therefore, a link from source to destination devices and intermediate nodes are used to transmit packets simultaneously. This enhances the channel efficiency and reduces the total delay for transmission across a packet network as compared to message switching.

5.6.4 Cell Switching

Cell switching, associated with Asynchronous Transmission Mode (ATM) is considered to be a high speed switching technology to overcome the speed problems for real time applications. Cell switching uses a connection-oriented packet-switched network. In cell switching, a connection is known as signaling. The cell switching uses a fixed length of packets of 53 bytes out of which 5 bytes are reserved for header. The packet switching technique uses variable length packets. Like packet switching, the cell switching technique also divided the message into smaller packets but of fixed length. The advantages are high performance, common LAN/WAN architecture, multimedia support, dynamic bandwidth and scalability. High performance is achieved because of the use of hardware switches. The cell switching also possesses connection-oriented service features of circuit switching. The connection oriented virtual circuits for each phase allocates specified resources for different streams of traffic.

5.6.5 Difference between Circuit Switching and Packet Switching

The concept and idea of switching data (into circuit switching network) into the small blocks or packets according to the match of their size, content or structure was firstly represented by *"Paul Baran"* in early years of 1960's. On other hand, Packet switching which is also known as virtual switching is also in the content of the feature of networking.

Circuit Switching Vs. Packet switching is actually defines the differences between the two different methods of switching. Circuit Vs. Packet Switching is an absolute comparison between the both switching. Circuit Vs. Packet switching is taking place on the basis of different features of the two different kinds of switching. The difference of old and the new technology use is also a main comparative feature between the both which supports Circuit switching Vs. Packet Switching.

Notes

Packet Switching is more modernize and new technology of switching and is a suitable and affordable method of switching, while the circuit switching is an old and expensive method of switching, which makes a prominent difference line between both and supports the topic of Circuit Vs. Packet switching. The other Circuit Vs. Packet switching feature is the contention of reliability and non-reliable method of switching.

Did u know? Circuit switching is more reliable then packet switching. Circuits switching is reliable and ideal in all while the packet switching is ideal for VOIP (voice over internet protocol).

A switching power supply circuit is an electronic power supply (PSU is the unit) which automatically converts the characteristics of volts and current to another. Switching power supply circuit also incorporates the switching regulator in order to be highly efficient. The main advantage of the switching power supply circuit is to get the great provision of efficiency because the switching transistor dissipates the little power and energy when it's outside of the range of its actual region. So, that the switching power supply circuit has an individual importance of its and its efficiency remains same if the challenging situation of Circuit switching Vs. Packet switching happens too.

Task Give one example each of the following:

1. Circuit switching
2. Packet switching
3. Message switching
4. Cell Switching

Self Assessment

Fill in the blanks:

6. The classic "forward voice mail" capability in some voice mail systems is an example of …….. switching.
7. A …… power supply circuit is an electronic power supply (PSU is the unit) which automatically converts the characteristics of volts and current to another.
8. Circuit switching is …….. reliable then packet switching.
9. Packet switching which is also known as …… switching.
10. …… is ideal for an integrated environment and is found within Cell-based networks such as ATMs.

5.7 Summary

- In this unit you have studied about various types of connecting devices such as hubs, bridges, switches, routers and gateways.
- Bridges are used to interconnect multiple LANs two devices at the data link layers of the OSI model. Switches are used for performing bridges functions as well as point-to-point dedicated connections.

Notes

- Hubs are used to interconnect various incoming connections with different outgoing connections at the Physical layer of the OSI model.
- Router are used to connect two devices at the network layer of the OSI Model. Routers are used to connect both similar and dissimilar LANs and operates layer 3. Router protocols consist of both bridging and routing protocols like inter-router, serial line protocols and protocol stack routing and bridging protocols.
- Gateways are used to connect totally dissimilar networks because they can perform protocol conversion for all seven layers of the OSI Model. Gateway routers are used to connect dissimilar LANs and perform all of the functions of bridges and routers. It operates at all seven layers of the OSI Reference Model. A switching hub can operate with multiple media (coaxial cable, UTP, and fiber).
- There are a number of ways to perform switching such as circuit Switching, Packet Switching, Message Switching and Cell Switching.

5.8 Keywords

Bridges: It is used to connect similar LANs together and operates at the bottom two layers of the OSI model. It uses MAC addresses (physical addresses) are used to determine whether data is necessary to transmit to other segments or not.

Encapsulating Bridge: Dissimilar LANs such as Ethernet-to-token ring can be connected with the help of bridge.

Gateways: Gateway routers are used to connect dissimilar LANs and perform all of the functions of bridges and routers. It operates at all seven layers of the OSI Reference Model.

Inter-router Protocols: These are router-to-router protocols that can operate over dissimilar networks. This protocol routes information and stores data packets during periods of idleness.

Media Access Control (MAC) Bridge: This is used to connect dissimilar LANs such as Ethernet-to-token ring using encapsulation or translation.

Protocol Stack Routing and Bridging Protocols: This advises the router as to which packets should be routed and which should be bridged.

Repeaters: It amplifies the signal, which has got attenuated during the course of transmission because of the physical conditions imposed by the transmission media.

Routers: Routers are used to connect both similar and dissimilar LAN and operates on the network layer of OSI model using the physical layer, data link layer and network layer to provide connectivity, addressing and switching.

Serial Line Protocols: This protocol is widely used over serial or dialup links connecting unlike routers.

Spanning Tree Protocol (STP) bridge: This is also known as adaptive or self-learning bridges and is defined in IEEE 802.1 standards.

Switching Hubs: A switch, which resembles a hub, is known as switching hub.

5.9 Review Questions

1. What is the main purpose of using router in a network?
2. Why does hub fall under the category of bus topology while physically it comes under star topology type?

Notes

3. How is bridge different from hub?
4. Explain with one advantage of static and dynamic routing why they are used.
5. Routers, bridges and repeaters are used to connect differing networks. Under what circumstances would each of these technologies be used?
6. How does a bridge differ from a switch?
7. What happens when you replace a hub with a switch?
8. What do you mean by switching? Explain the four types of switching.

Answers: Self Assessment

1.	Hub	2.	Bridge
3.	Switch	4.	Router
5.	Gateway	6.	Message Switching
7.	switching	8.	more
9.	virtual	10.	Cell Switching

5.10 Further Readings

Books

Andrew S. Tanenbaum, *Computer Networks,* Prentice Hall

Behrouz A. Forouzan, Sophia Chung Fegan, *Data Communications and Networking,* McGraw-Hill Companies

Burton, Bill, *Remote Access for Cisco Networks,* McGraw-Hill Osborne Media

Rajneesh Agrawal and Bharat Bhushan Tiwari, *Data Communication and Computer Networks,* Vikas Publishing House, New Delhi

Unit 6: Multiplexing

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss various multiplexing and different multiplexing techniques such as SDM, FDM, TDM, STDM and CDM
- Describe AM, FM and PM concepts for analog to analog modulation
- Explain modem modulation techniques.

Introduction

In data communication system, digital and analog communication together plays a very important and integrated role irrespective of many advantages of digital communications over analog. Figure 6.1 shows the integrated role of digital and analog communication to complete data communication system.

Notes

Figure 6.1: Data Communication System

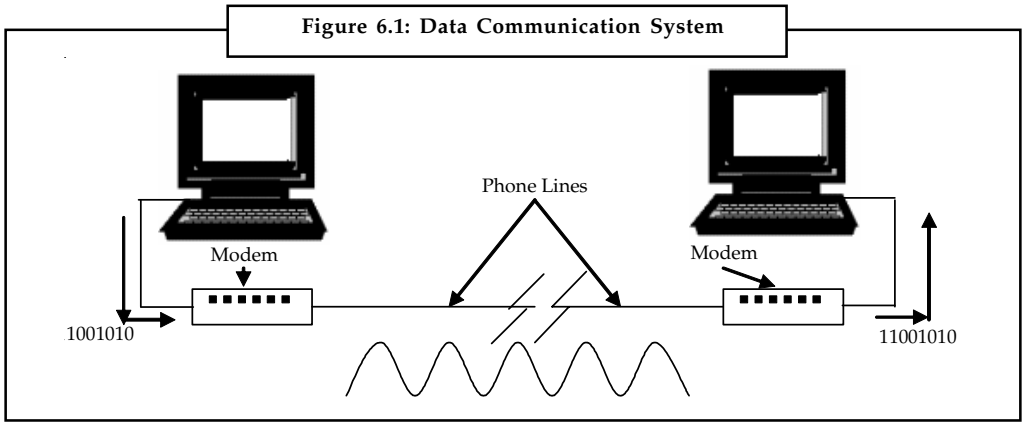
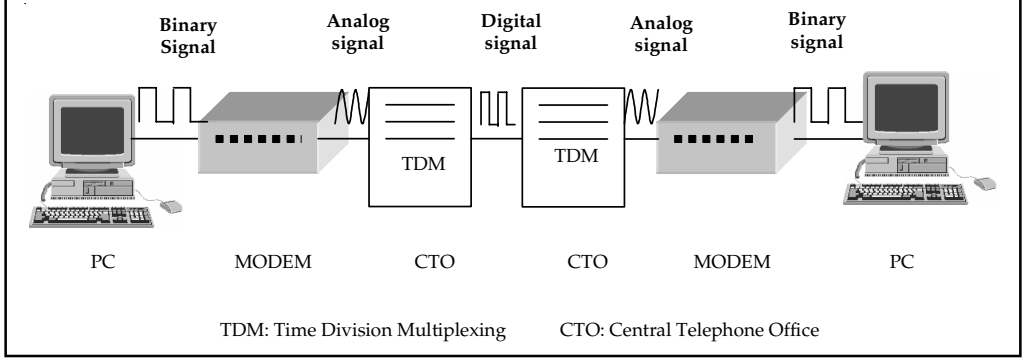


Figure 6.1 shows that the link between modems is modulated analog signal created by the modem. Likewise we may consider Figure 6.2 where data communication system is presented in a wider sense. The communication from PC to modem is consisted of binary signal whereas the communication between Central Telephone Office (CTO) and modem takes place in modulated analog signal. The communication between CTO to another CTO is by digital signal using time division multiplexers. Thereafter CTO feeds modulated analog signal to modem and modem converts it into binary signal for the PC. We may now say that different types of signals emerging on the communication link and reaching to CTO on their way across a city. These can be multiplexed to share the same communication link for transmitting to destination.

Figure 6.2: Data Communication Systems in a Wider Sense



Analog transmission refers to conveying voice, data, image, signal or video information using a continuous signal which varies in amplitude, phase or some other property in proportion to that of a variable. The information may be conveyed using wired or wireless medium like twisted-pair or coax cable, fiber-optic cable, air, water, etc. Amplitude modulation and frequency modulation are the two basic types of analog transmission methods. They are based on how they modulate data to combine an input signal with a carrier signal. Until recently, the telephony and voice communication was analog in nature as well as television and radio transmission. The analog transmission is still being used for shorter distances because of significantly lower costs. The digital transmission seeks complex multiplexing and timing equipment which not required for analog transmission.

6.1 Circuits, Channels and Multichanneling

A circuit is a path between two or more points along which an electrical current flows. In data communication, a circuit is considered as a specific path between two or more points along

Notes

which signals is carried. The signals may be analog, binary or digital. This has been shown in the Figures 6.1 and 6.2. In Figure 6.1 and Figure 6.2 the link between PC and modem, modem, link between modem and CTO and so on constitute a circuit. The circuit may be a physical path consisting of wires or it may be wireless. A network, which is wired or wireless involves a number of circuits consisting of a number of intermediate switches. A circuit is classified based upon its uses like dial up connection, leased line, etc. The connections between two or more points are also established virtually unlike to the connection made by dial up and leased line as physical in nature. Such circuits are defined as Virtual Circuit (VC) based upon the type and nature of the connection. A virtual circuit is a logical path selected out of many possible physical paths available between two or more points. However, the connection in a virtual circuit is not guaranteed. The virtual circuits that ensure a permanent connection between two points is referred as Permanent Virtual Circuit (PVC). The PVC provides guaranteed connection between two or more points when needed without having to reserve a specific physical path in advance. A Switched Virtual Circuit (SVC) is similar to a permanent virtual circuit and allows users to dial in to the network of virtual circuits. A circuit may contain many channels together. The Integrated Services Digital Network (ISDN) supports 2 Basic Rate Interface (BRI) service channel and 1 signaling channel. A Digital Signal 1 (DS1) circuit supports 24 64-Kb/s channels, while a DS3 circuit supports 612 64-Kb/s channels. These numbers of channels on a single circuit are possible because of multiplexing techniques.

6.2 Multiplexing

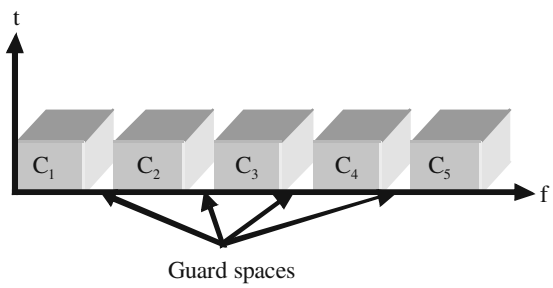
Multiplexing is the process in which multiple channels are combined for transmission over a common transmission path. There are following different techniques for multiplexing:

- Frequency Division Multiplexing (FDM)
- Time Division Multiplexing (TDM)
- Code Division Multiplexing (CDM)
- Wavelength Division Multiplexing (WDM)

6.2.1 Frequency Division Multiplexing (FDM)

Multiple channels are combined together for transmission over a single channel. The channels are separated by their frequency. It is explained in the Figure 6.3 where a frequency dimension is divided into several non-overlapping frequency bands. Each channel ci is allotted its own frequency band as depicted in Figure 6.3.

Figure 6.3: Frequency Division Multiplexing



There are always some unused frequency spaces between channels. They are known as guard bands and also shown in Figure 6.3. They are used to reduce the effects of overlapping between adjacent channels. Overlapping of adjacent channels tends to produce crosstalk.

Notes

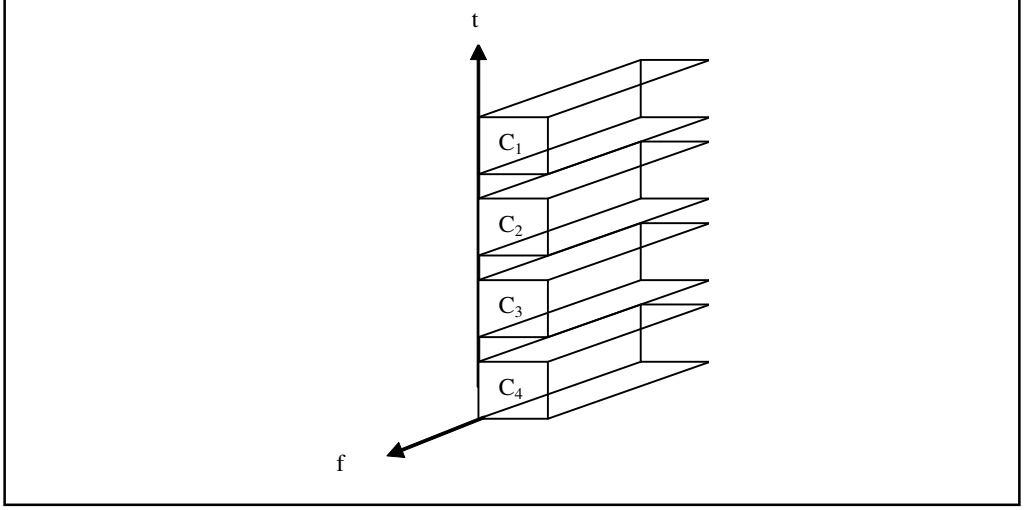
FDM was the first multiplexing scheme that was widely used in network deployment. They are still in use today and are used with analog transmission. However, Time Division Multiplexing is preferred over FDM. The main disadvantage of FDM is the wastage of frequency resources as it was dedicated to a particular channel for all time. This also puts an upper limit on the number of channels.

6.2.2 Time Division Multiplexing (TDM)

In digital transmission, Time Division Multiplexing (TDM) and Code Division Multiplexing (CDM) are widely used. TDM is a process to merge data from several sources into a single channel for communication over transmission media like telephone lines, microwave system or satellite system. TDM is implemented in two ways. They are synchronous TDM and asynchronous TDM. Asynchronous TDM is known as Statistical TDM (STDM). The synchronous TDM techniques divides a single channel into time slots and each transmitting device is assigned at least one of the time slots for its transmission as shown in Figure 6.4. Time slots are assigned in such a way that each transmitting device gets its required share of the available bandwidth. Because of this time-bandwidth multiplexing technique, TDMs are protocol insensitive and are capable of combining various protocols onto a single high-speed transmission link. In other words we can say that multiplexer allocates exactly the same time slot to each device at all times whether the device is active or idle. Some devices, such as voice and video systems may require more slots to ensure that data arrives at the distant link-end without becoming distorted from slower data rates. These different time slots are grouped into frames. A frame consists of one complete cycle of time slots. Alternatively Figure 6.4 explains more clearly the concept of TDM in a data communication environment where three PCs are sharing the common circuit. The packets generated by each PC are multiplexed on the common line as A1, B1, C1 and so on.

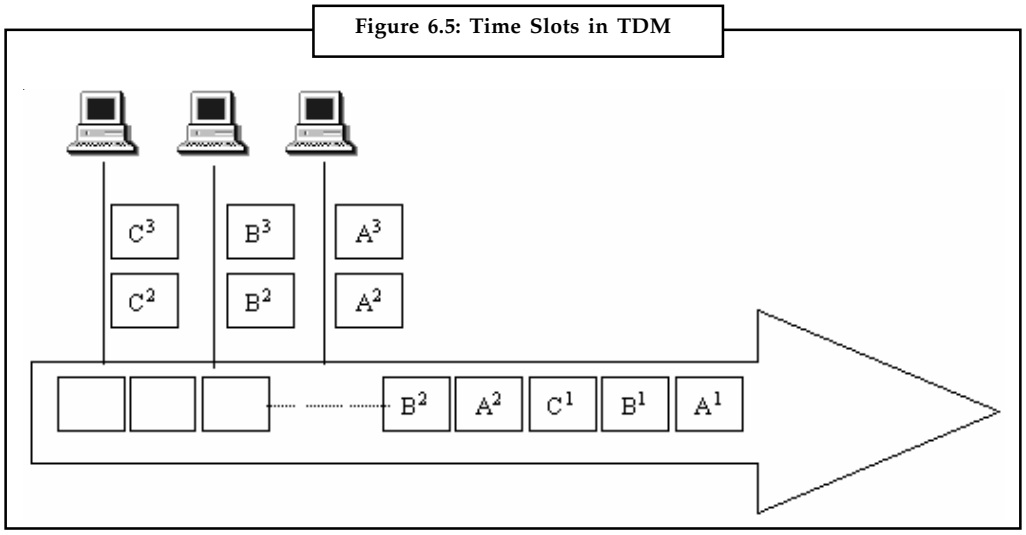
It is more flexible than the FDM. Unlike to FDM, the whole bandwidth for a certain amount of time is provided to the user. All the users are using the same frequency but at a different time. This time allotment may be varied as per the requirement and priority of the users' services. In the Figure 6.4 spaces between different time slots are shown, these are known as guard spaces in time dimension. These are used to eliminate co-channel interference.

Figure 6.4: Time Division Multiplexing



Notes

Figure 6.5: Time Slots in TDM



The main disadvantage of this scheme is that a precise synchronization between different senders is necessary to avoid co-channel interference.

Statistical Time Division Multiplexing (STDM)

In case of TDM, time slots are allocated to channels, even if they have no information to transmit. This is just wastage of the bandwidth and to overcome this inefficiency of standard TDM, a techniques known as STDM is implemented in which time is allocated to lines only on demand. This is achieved with the uses of intelligent devices that are capable of identifying when a terminal is idle and statistically compensates for normal idle time so that more lines can be connected to a transmission medium. During the peak traffic period a buffer memory temporarily stores the data so high-speed line time can be effectively utilized with active channels. It adopts a methodology where each transmission has identification information (a channel identifier). This increases the overheads, which are handled by grouping a number of characters for each channel together for transmission. It is also referred as "Intelligent" TDM. In this case, data rate capacity is well below the sum of connected capacity of each channel because it utilizes the idle time very effectively. It is digital only and requires more complex framing of data. It is widely used for remote communications with multiple terminals. The additional services such as data compression, line priority, mixed speed lines, host ports sharing, network port control, automatic speed detection etc are available with STDM techniques.

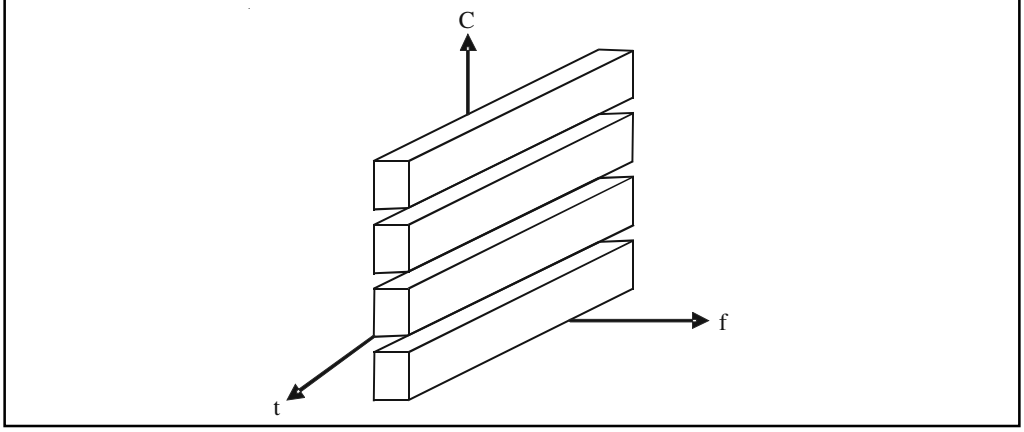
6.2.3 Code Division Multiplexing (CDM)/Spread Spectrum

CDM is widely used in so-called second-generation (2G) and third-generation 3G wireless communications. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands. This is a combination of analog-to-digital conversion and spread spectrum technology. CDM may be defined as a form of multiplexing where the transmitter encodes the signal using a pseudo random sequence. CDM involves the original digital signal with a spreading code. This has the effect of spreading the spectrum of the signal greatly and reducing the power over any one part of the spectrum. On the other hand, the receiver knows about the code generated and transmitted by the transmitter and therefore can decode the received signal. Each different random sequence corresponds to a different communication channel from multiple stations.

Notes

Code Division Multiplexing assigns each channel its own code to make them separate from each other. These unique underlying codes, which when decoded restore the original desired signal while totally removing the effect of the other coded channels. Guard spaces are realized by using codes with orthogonal codes. In case of TDM and FDM, channels are isolated by separate time or frequency slots, which are occupied in common by all users. Figure 6.6 explains how all channels Ci use the same frequency at the same time for transmission.

Figure 6.6: Code Division Multiplexing (CDM)



A single bit may be transmitted by modulating a series of signal elements at different frequencies in some particular order. These numbers of different frequencies per bit are called as the chip rate. If one or more bits are transmitted at the same frequency, it is called as frequency hopping. This will happen only when the chip rate is less than one because chip rate is the ratio of frequency and bit. At the receiving side, receiver decodes a 0 or a 1 bit by checking these frequencies in the correct order.

A disadvantage of CDM is that each user's transmitted bandwidth is larger than the digital data rate of the source. The result is an occupied bandwidth approximately equal to the coded rate. Therefore CDM and spread spectrum are used interchangeably. The transmitter and receiver require a complex electronics circuitry. The main advantage of CDM is protection from interference and tapping because only the sender the receiver knows the spreading code.

6.2.4 Wavelength Division Multiplexing (WDM)

Fiber optic technology is considered to meet the ever-increasing demand of bandwidth for the exchange of information and WDM provides solutions for the ever-increasing demand of bandwidth through optical networks. In optical communications, the analog of FDM is referred to as wavelength-division multiplexing (WDM).

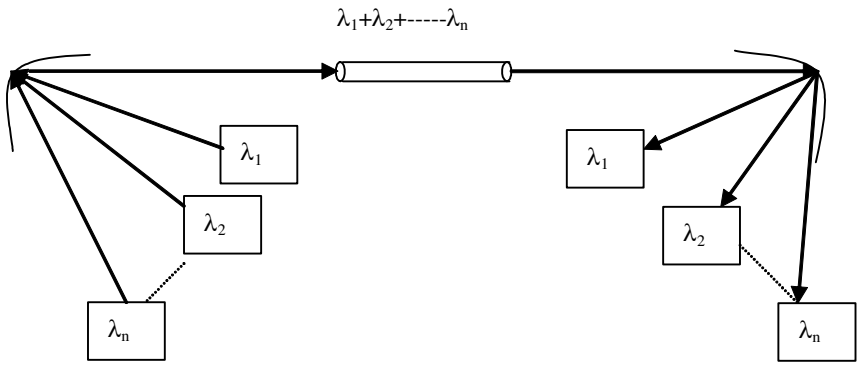
WDM may be defined as the fiber-optic transmission technique that employs two or more optical signals having different wavelengths to transmit data simultaneously in the same direction over one fiber, and later on is separated by wavelength at the distant end. WDM allows transmission of analog or digital signals up to a few GHz or Gbits/s on a carrier's very high frequency around 190 THz (infrared). In fact, using several carrier waves that are propagating without significant interaction on the same cable can increase the bit rate further. These carrier waves correspond to different wavelengths. This is the reason it is called Wavelength Division Multiplexing (WDM). The relationship between frequency and wavelength is given as follows:

$l = c/f$ where c and f are the velocity and frequency of the signal in the medium.

Notes

In WDM several sources emitting at different wavelengths say λ_1, λ_2, λ_3 and so on are coupled into the same optical fiber and these are separated after transmission on the fiber toward different detectors at the fiber end. Figure 6.7 explains the technique of WDM.

Figure 6.7: Wavelength Division Multiplexing showing different Wavelengths getting Multiplexed In and Out of the Fiber



Self Assessment

Fill in the blanks:

1. CDM is widely used in so-called second-generation (2G) and third-generation 3G …….. communications.
2. In optical communications, the analog of FDM is referred to ……..
3. TDM is a process to merge data from several sources into a single channel for communication over ……..
4. A ……. is a logical path selected out of many possible physical paths available between two or more points.
5. A ……. is considered as a specific path between two or more points along which signals is carried.

6.3 Modem Modulation Techniques

Until recently, the telephony and voice communication was predominantly analog in nature and communication channels like telephone lines are analog transmission media. Analog media is considered a bandwidth-limited channel. The usable bandwidth of telephone lines falls in the range of 300 Hz to 3300 Hz. Digital signal that are in the form of discrete values could not be transmitted over analog media. Therefore, digital signals are converted into analog signals so as the communication channels can carry the information from one place to another. The technique that enables this conversion is called *modulation.* There are basically following types of modulation used in modems. These are as follows:

ASK – Amplitude Shift Keying

FSK – Frequency Shifted Keying

PSK – Phase Shift Keying

QPSK – Quadrature Phase Shifted Keying

Notes

DPSK – Differential Phase Shift Keying

QAM – Quadrature Amplitude Modulation

Modems use a combination of the above modulation techniques and compression to achieve high data transfer rates.

6.4 Modulation of Digital Signal

A digital transmission uses low pass channel with high bandwidth. Similarly, analog transmission is also possible on band pass channels that require converting of binary data or a low pass analog signal into a band pass analog signal. This technique is called modulation. Thus, modulation of binary data or digital to analog modulation is carried over by changing one of the characteristics of the analog signal in accordance with the information in the digital signal. The information in the digital signal is always in the form of 0 and 1. The characteristics of analog signal that are altered are amplitude, frequency and phase of the analog waveform. Based on the change in one of the characteristics, the digital to analog modulation may be of amplitude shift keying (ASK), frequency shift keying (FSK) and phase shift keying (PSK) types. Quadrature amplitude modulation is the fourth category that combines changes in both amplitude and phase to provide better efficiency.

Data Rate

Bit rate is the number of bits (0 or 1) transmitted during 1 second of time. The number of signal changes per unit of time to represent the bits is called the data rate of the modem. That rate is usually expressed in terms of a unit known as a baud. A signal unit may have 1 or more than 1 bits. Therefore, the baud is the number of times per second the line condition can switch from "1" to "0". Baud rate and bit rate, which are expressed in bits per second, usually are not the same, as several bits may be transmitted through the channel by the modem in each signal change (a few bits can be transmitted as one symbol). The relation between bit rate and baud is expressed that bit rate equals the baud rate times the number of bits represented by each signal unit. Bit rate is always more or equal than baud rate. The reason for baud rate is that it determines the bandwidth required to transmit the signal. The signal may be in the form of pieces or block that may contain bits. A fewer bandwidth required to move these signal unit with large bits for an efficient system. To understand the relation between bit and baud rate, we consider an analogy of car, passengers and highway with signal units, bits and bandwidth respectively.

A car has capacity of carrying 5 passengers maximum at a time. Suppose a highway may support only 1000 cars per unit time without congestion. When each car on the highway carries 5 passengers, it is considered that the highway is capable of providing services without congestion. Thus highways services are treated efficient. Consider another case, when all these 5000 passengers wish to go in separate cars, they require 5000 cars and highway can only support 1000 cars at a time. The services offered get deteriorated because highway's capacity is meant only for 1000 cars. It does not bother as to whether these 1000 cars are carrying 1000 passengers or 5000 passengers or more. To support more cars, the highway needs to widen. Similarly, the number of bauds determines the bandwidth.

Carrier Signal

The carrier signal that is a high frequency signal plays a significant role in the modulation and data transmission. It is the base signal generated by the sending device whose one of the characteristics is altered in accordance with the digital signal to be modulated. The modulating signal or digital signal riding over the carrier signal is transmitted to the receiving device. The receiving device is tuned to the frequency of the carrier signal. Other advantages of the carrier

Notes

signal are that it provides efficient transmission between sending device and receiving device and needs smaller sizes of antenna because of higher frequency of transmission.

6.4.1 Amplitude Shift Keying (ASK)

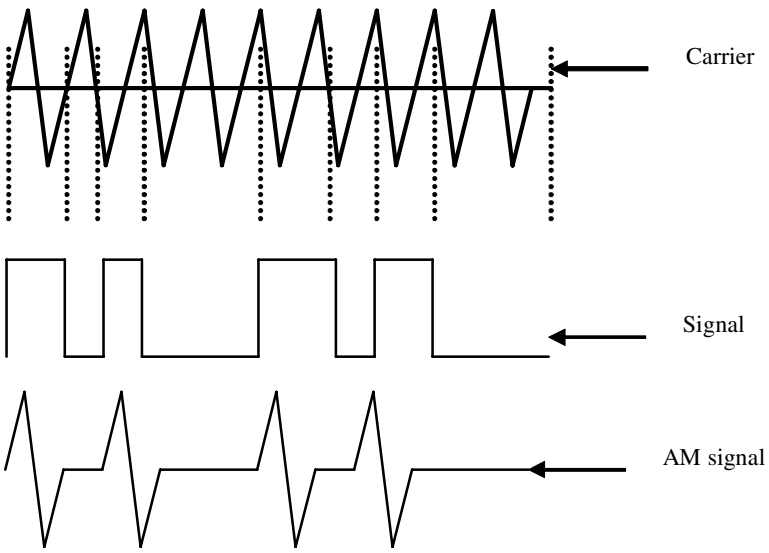
ASK describes the technique how the carrier wave is multiplied by the digital signal f (t) so that the strength of the carrier wave is varied to represent binary 0 and 1. In ASK, both the frequency and phase of an analog waveform are kept uniform while amplitude is changed in accordance with the digital signal.

Notes Mathematically, the modulated carrier signal y(t) is:

$y(t) = f(t) \times \sin(2pfct + j)$ where fc is a carrier frequency and t is instantaneous time.

Figure 6.8 shows the technique of amplitude modulation.

Figure 6.8: Amplitude Modulation



The main advantage of ASK is that it is easy to produce and detect. The disadvantages of ASK are that it is highly susceptible to noise interference that changes the amplitude of the signal. A 0 can be changed to 1 and vice versa. Other drawbacks are that the speed of the changing amplitude is limited by the bandwidth of the line and the small amplitude changes suffer from unreliable detection. Telephone lines limit amplitude changes to some 3000 changes per second. The disadvantages of amplitude modulation causes this technique to no longer be used by modems, however, it is used in conjunction with other techniques.

Notes The bandwidth for an ASK signal is mathematically given by:

$$\text{Bandwidth (BW)} = (1 + d) \times \text{Nbaud}$$

Where Nbaud is the baud rate and d is the modulating index and may have minimum value as 0.

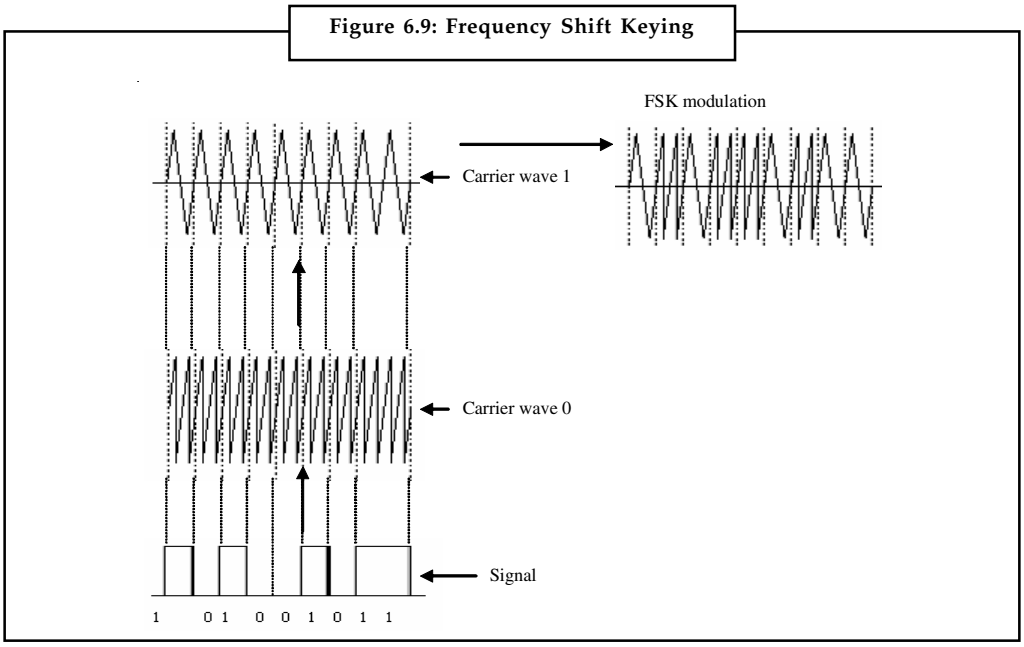
Notes

6.4.2 Frequency Shift Keying

FSK describes the modulation of a carrier (or two carriers) by using a different frequency for a 1 or 0. In this technique the frequency of the carrier signal is changed according to the data while keeping the amplitude and phase constant. The transmitter sends different frequencies for a 1 than for a 0 as shown in Figure 6.9. The resultant modulated signal may be regarded as the sum of two amplitude modulated signals of different carrier frequency.

Mathematically, the modulated wave y(t) can be shown as y(t) = f1(t) sin(2pfc1t + j) + f2(t) sin(2pfc2t + j) where fc1 and fc2 are different carrier frequencies of two different signals. FSK is classified as wide band if the separation between the two carrier frequencies is larger than the bandwidth of the spectrums. Narrow-band FSK is the term used to describe an FSK signal whose carrier frequencies are separated by less than the width of the spectrum than ASK for the same modulation.

Figure 6.9: Frequency Shift Keying



The advantage of FSK is that it provides better immunity from noise because the receiving device looks for specific frequency changes over given number of periods and frequency is almost unaffected from noise. The disadvantages of this technique are that again as it was with amplitude modulation. The rate of frequency changes is limited by the bandwidth of the line, and that distortion caused by the lines makes the detection even harder than amplitude modulation. Today this technique is used in low rate asynchronous modems up to 1200 baud only.

The bandwidth for FSK signal is the sum of the baud rate of the signal and the frequency shift. The frequency shift is the difference between the two carrier frequencies.

6.4.3 Phase Shift Keying (PSK)

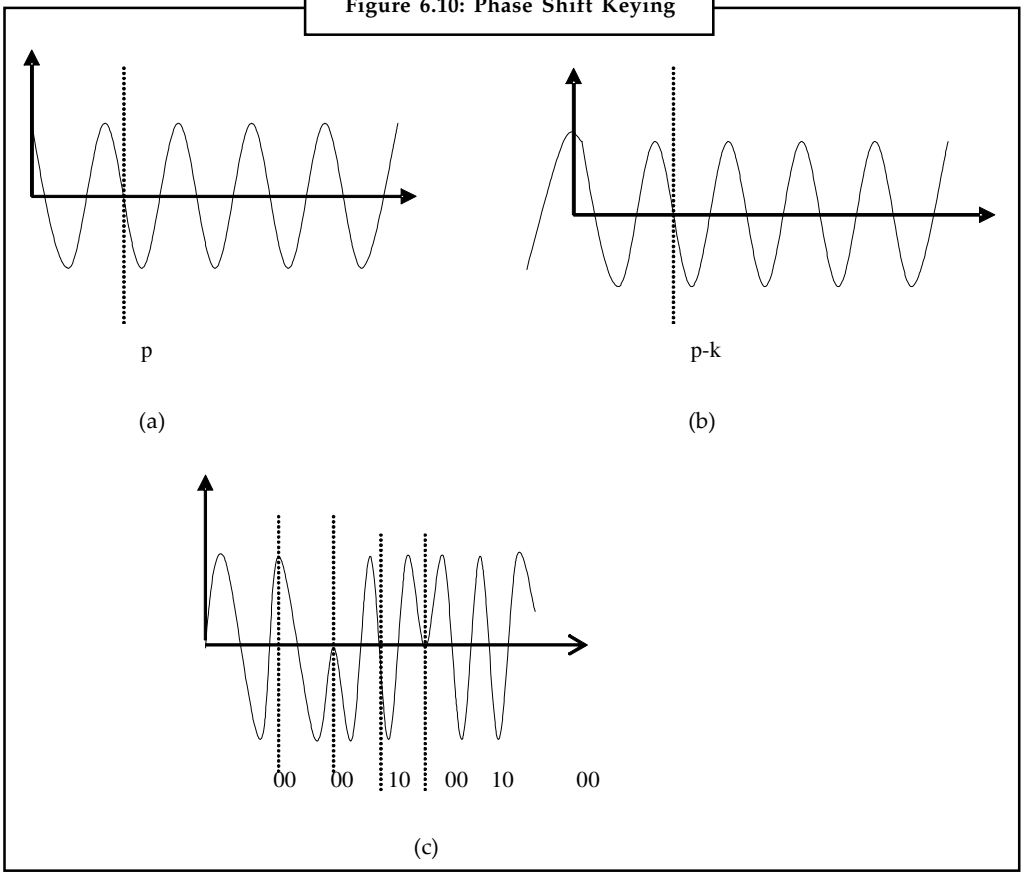
In this modulation method a sine wave is transmitted and the phase of the sine wave carries the digital data or the phase of sine wave is varied to represent binary 1 or 0 and both the amplitude and frequency of the analog waveform are kept constant. For a 0, a 0 degrees phase sine wave is transmitted. For a 1, a 180 degrees sine wave is transmitted. As this method involves two states of phase changes, it is called binary PSK or 2-PSK. This technique, in order to detect the phase of each symbol, requires phase synchronization between the receiver's and transmitter's phase.

Notes

This complicates the receiver's design. The advantages of PSK are that it is immune to noise and is not band limited.

Differential Phase Modulation: A sub method of the phase modulation is *differential phase modulation*. In this method, the modem shifts the phase of each succeeding signal in a certain number of degrees for example, a 0 for 90 degrees and 1 for 270 degrees as illustrated in Figure 6.10.

Figure 6.10: Phase Shift Keying



PSK is a technique, which shifts the period of a wave. The wave shown in Figure 6.10 (a) has a period of p starting from 0. The wave shown in Figure 6.10 (b) is the same wave as shown in Figure 6.10 (a), but its phase has been shifted. Notice that the period starts at the wave's highest point 1 on the vertical axis. It just so happens that we have shifted this wave by one quarter of the wave's full period. We can shift it another quarter, if we want to, so the original wave would be shifted by half of its period. And we could do it one more time, so that it would be shifted three quarters of its original period.

This means there exist 4 separate waves and therefore each wave is provided for some binary value. Since there are 4, 2 bits are provided to each wave which is represented below:

Bit value	Amount of Shift
00	None
01	¼
10	½
11	¾

Notes

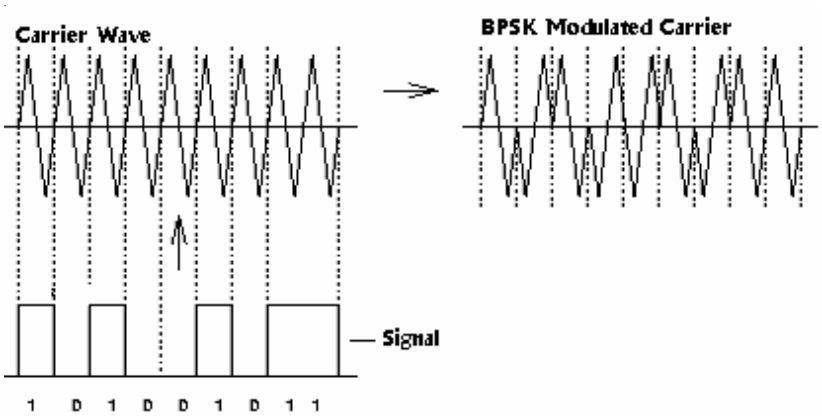
This technique of letting each shift of a wave represent some bit value is phase shift keying. But the real key is to shift each wave relative to the wave that came before it. PSK describes the modulation technique that alters the phase of the carrier. Mathematically, it can be represented as y(t) = f(t) sin(2pfct + j(t)) where jc is phase shift. This method is easier to detect than the previous one. The receiver has to detect the phase shifts between symbols and not the absolute phase.

Binary Phase Shift Keying (BPSK): In the case of two possible phases shift the modulation will be called BPSK - binary PSK. In the case of 4 different phase shifts possibilities for each symbol which means that each symbol represents 2 bits the modulation will be called quadrature PSK (QPSK), and in case of 8 different phase shifts the modulation technique will be called 8-PSK.

A single data channel modulates the carrier. A single bit transition, 1 to 0 or 0 to 1, causes a 180-degree phase shift in the carrier. Thus, the carrier is said to be modulated by the data. As this has only two phases, 0 and 1. It is therefore a type of ASK with taking the values -1 or 1 and its bandwidth is the same as that of ASK. Phase shift keying offers a simple way of increasing the number of levels in the transmission without increasing the bandwidth by introducing smaller phase shifts. Quadrature phase-shift-keying (QPSK) has four phases such as 0, p/2, p, 3p/2. Consequently, M-ary PSK has M phases given by 2pm/M; m = 0,1…M-1. For a given bit-rate, QPSK requires half the bandwidth of PSK and is widely used for this reason.

Did u know? The number of times the signal parameter (amplitude, frequency, and phase) is changed per second is called the signaling rate. It is measured in baud. 1 baud = 1 change per second. With binary modulations such as ASK, FSK and BPSK, the signaling rate equals the bit-rate. With QPSK and M-ary PSK, the bit-rate may exceed the baud rate.

Figure 6.11: Binary Phase Shift Keying



Quadrature Phase Shift Keying (QPSK)

Two data channels modulate the carrier. Transitions in the data cause the carrier to shift by either 90 or 180 degrees. This allows transmission of two discrete data streams, identified as I channel (In phase) and Q channel (Quadrature) data. In this method four different phase angles are used.

Notes In QPSK, the four angles are usually out of phase by 90°.

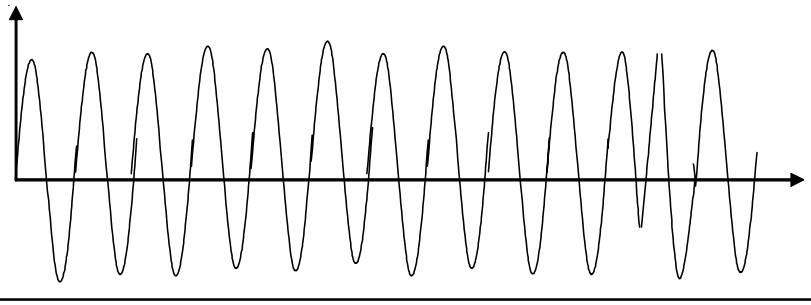
Notes

Differential Phase Shift Keying (DPSK)

DPSK changes the phase of the carrier wave instead of frequency. This is used for digital transmission in which the phase of the carrier is discretely varied in relation to the phase of the immediately preceding signal element and in accordance with the data being transmitted. The shift in phase takes place from the present phase rather than from an absolute standard therefore this technique is called DPSK. A disadvantage of DPSK is higher BER vs. SNR than BPSK (by about 1 dB).

Figure 6.12 shows DPSK using two phase changes i.e. 0 is a 00 phase shift and 1 is a 1800 phase change.

Figure 6.12: DPSK with Two Phase Angles



QAM (Quadrature Amplitude Modulation)

This technique is based on the amplitude modulation and phase modulation to improve the performance of the amplitude modulation. Theoretically, any number of changes in amplitude can be associated with any number of changes in phase. For example, two carrier signals are transmitted simultaneously at the same frequency with a 90 degrees phase shift. The QAM intends to combine the benefits of the amplitude and phase shift keying modulation. It involves fewer number of amplitude shifts than phase shift because the amplitude modulation is susceptible to the noise. The minimum bandwidth required for QAM is equivalent to the minimum bandwidth required for ASK and PSK.

Task How does AM differ from ASK?

6.5 Modulation of Analog Signal

The modulation is the act of translating some low-frequency (base band signal) such as voice, data, etc. to a higher frequency. The modulation/demodulation is a nonlinear process in which two different sinusoids are multiplied. In the modulation process, some characteristic of a high-frequency sinusoidal carrier fc as shown in Figure is changed in direct proportion to the instantaneous amplitude of the base band signal as fm in Figure 6.13. Let us assume the two sinusoids as shown in Figure 6.13 as fm and fc as base band signal and carrier respectively and are represented as:

$f_m = A \sin\omega_m t + \phi_1$ ...(1)

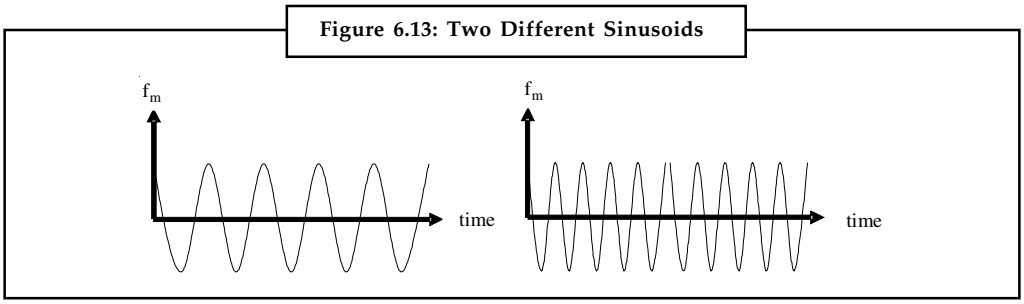
$f_c = B \sin\omega_c t + \phi_2$ ...(2)

In equation 2, either amplitude B or angular frequency wc may be varied in accordance with equation 1 and thus producing either amplitude modulation or frequency modulation or phase

Notes

modulation respectively. The angular frequency is defined as the 2p times of the frequency of carrier signal.

Figure 6.13: Two Different Sinusoids



In other words, modulation is used to superimpose a message (voice, image, data, etc.) on to a carrier wave for transmission. The frequencies that comprise the message (base band) are translated to a higher range of frequencies. The frequencies that comprise the message is preserved, that is, every frequency in that message is scaled by a constant value as explained above. Modulation is necessary for data communication because of several reasons. It allows the simultaneous transmission of two or more base band signals by translating them to different frequencies. It also reduces the size of antenna for higher frequencies with the greater efficiency.

Inter Modulation

Inter modulation is a special case where two (or more) sinusoids effect one another to produce undesired products, that is, unwanted frequencies (noise). Again, this can only occur when both waves share the same non-linear device. The non-linearity results in several even or odd harmonics. Harmonics are the multiple of the fundamental frequency, that is, the message frequency. The modulating index is the ratio of the peak of the modulating signal to the peak of the carrier in case of amplitude modulation. In angular modulation, the ratio of the frequency deviation of the modulated signal to the frequency of a sinusoidal modulating signals.

Did u know? The modulation index is numerically equal to the phase deviation in radians.

6.5.1 Amplitude Modulation

This describes the technique in which the carrier wave is multiplied by the digital signal f(t). Mathematically, the modulated carrier signal y(t) is: y(t) = f(t) sin(2p ¦ct+j) where fc is a carrier frequency and t is instantaneous time. Figure 6.14 shows the technique of amplitude modulation.

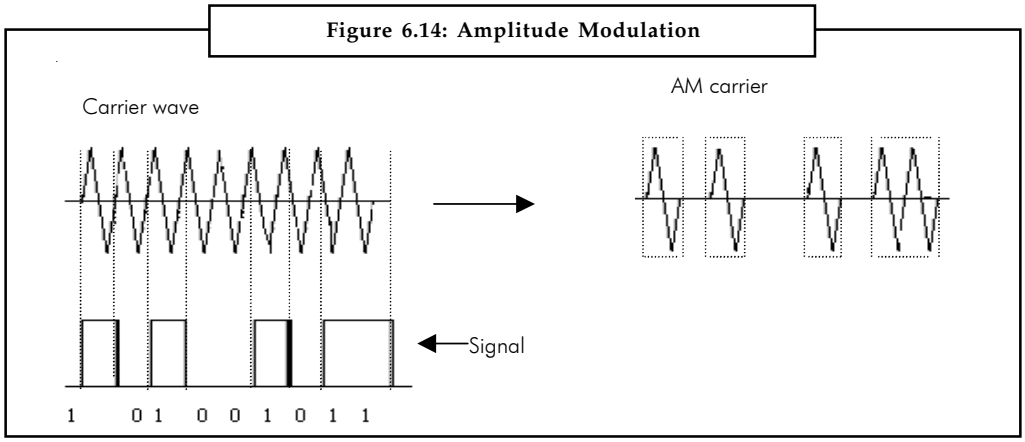
The main advantage of this technique is that it is easy to produce such signals and also to detect them. This technique has two major disadvantages. The first is that the speed of the changing amplitude is limited by the bandwidth of the line. The second is that the small amplitude changes suffer from unreliable detection. Telephone lines limit amplitude changes to some 3000 changes per second. The disadvantages of amplitude modulation causes this technique to no longer be used by modems, however, it is used in conjunction with other techniques.

QAM (Quadrature Amplitude Modulation)

This technique is based on the basic amplitude modulation. This technique improves the performance of the basic amplitude modulation. In this technique two carrier signals are transmitted simultaneously. The two carrier signals are at the same frequency with a 90 degrees phase shift.

Notes

Figure 6.14: Amplitude Modulation



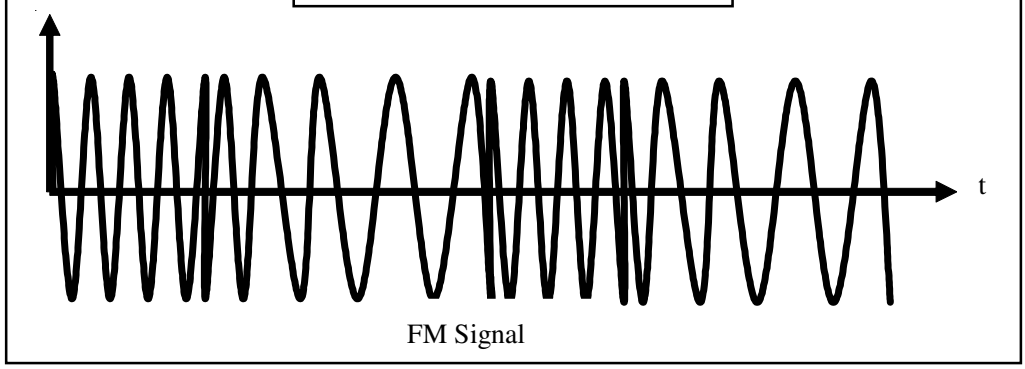
6.5.2 Frequency Modulation

Frequency Modulation involves the modulation of the frequency of the analog sine wave where the instantaneous frequency of the carrier is deviated in proportion of the deviation of the modulated carrier with respect to the frequency of the instantaneous amplitude of the modulating signal. It may be said in a simple word that it occurs when the frequency of a carrier is changed based upon the amplitude of input signal. Unlike AM, the amplitude of carrier signal is unchanged. This makes FM modulation more immune to noise than AM and improves the overall signal-to-noise ratio of the communications system. Power output is also constant, differing from the varying AM power output. The amount of analog bandwidth necessary to transmit FM signal is greater than the amount necessary for AM, a limiting constraint for some systems. The modulating index for FM is given as below:

$\beta = f_p/f_m$, where

β = Modulation index, f_m = frequency of the modulating signal and f_p = peak frequency deviation

Figure 6.15: Frequency Modulation



From the Figure 6.15, it is inferred that the amplitude of the modulated signal always remains constant, irrespective of frequency and amplitude of modulating signal. It means that the modulating signal adds no power to the carrier in frequency modulation unlike to amplitude modulation. FM produces an infinite number of side bands spaced by the modulation frequency, fm that is not in case of AM. Therefore, AM considered a linear process whereas FM as a nonlinear process. It is necessary to transmit all side bands to reproduce a distortion free signal. Ideally, the bandwidth of the modulated signal is infinite in this case. In general the determination of the frequency content of an FM waveform is complicated, but when b is small, the bandwidth of the

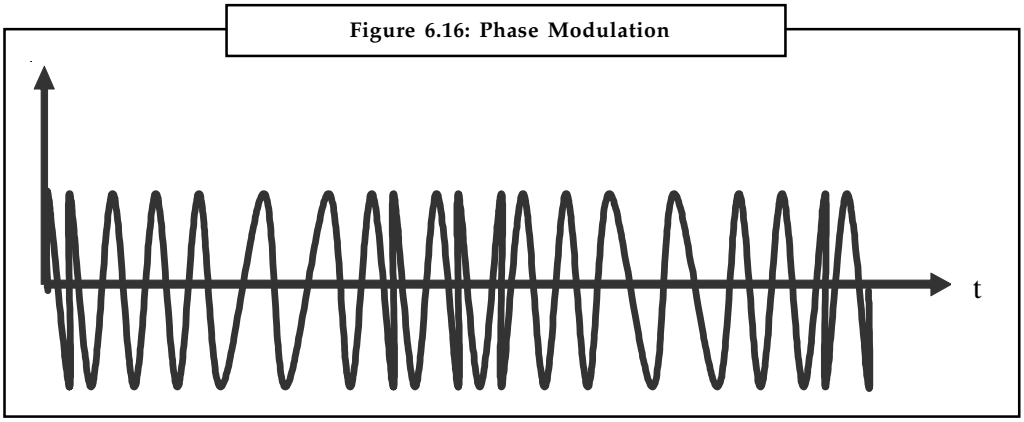
Notes

FM signal is 2fm. On the other hand, when b is large, the bandwidth is determined (empirically) as 2 fm (1 + b).

6.5.3 Phase Modulation

Phase Modulation (PM) is similar to frequency modulation. Instead of the frequency of the carrier wave changing, the phase of the carrier wave changes. In PM the phase of the carrier is made proportional to the instantaneous amplitude of the modulating signal. Modulating index for PM is given as b = Dj, where Dj is the peak phase deviation in radians. As in the case of angular modulation argument of sinusoidal is varied and therefore we will have the same resultant signal properties for frequency and phase modulation. A distinction in this case can be made only by direct comparison of the signal with the modulating signal wave, as shown in Figure 6.16.

Figure 6.16: Phase Modulation



Caution Phase modulation and frequency modulation are interchangeable by selecting the frequency response of the modulator so that its output voltage will be proportional to integration of the modulating signal and differentiation of the modulating signal respectively. Bandwidth and power issues are same as that of the frequency modulation.

A comparison of FM and AM

The main advantages of FM over AM are:

1. Improved signal to noise ratio (about 25dB) w.r.t. to man made interference.
2. Smaller geographical interference between neighboring stations.
3. Less radiated power.
4. Well defined service areas for given transmitter power.

The disadvantages of FM are:

1. Much more Bandwidth (as much as 20 times as much).
2. More complicated receiver and transmitter.

Self Assessment

Notes

State whether the following statements are true or false:

6. The modulation is the act of translating some high-frequency (base band signal) such as voice, data, etc. to a lower frequency.
7. Amplitude Modulation (AM) involves the modulation of the amplitude of the carrier as analog sine wave.
8. FM considered a linear process whereas AM as a nonlinear process.
9. In PM the phase of the carrier is made proportional to the instantaneous amplitude of the modulating signal.
10. Analog to analog signal conversion involves amplitude modulation and frequency modulation techniques only.

6.6 Summary

- A circuit is a path between two or more points along which signals is carried. The circuit may be a physical path consisting of wires or it may be wireless. A network, which is wired or wireless involves a number of circuits consisting of a number of intermediate switches.
- A virtual circuit is a logical path selected out of many possible physical paths available between two or more points.
- Multiplexing is the process in which multiple channels are combined for transmission over a common transmission path.
- In FDM multiple channels are combined together for transmission over a single channel.
- TDM is a process to merge data from several sources into a single channel for communication over transmission media like telephone lines, microwave system or satellite system. Asynchronous TDM is known as Statistical TDM (STDM). The synchronous TDM technique divides a single channel into time slots and each transmitting device is assigned at least one of the time slots for its transmission.
- CDM is defined as a form of multiplexing where the transmitter encodes the signal using a pseudo random sequence.
- WDM is defined as the fiber-optic transmission technique that employs two or more optical signals having different wavelengths to transmit data simultaneously in the same direction over one fiber, and later on is separated by wavelength at the distant end.
- SDMA is most popular access technology for satellite communication where dish antennas are frequently and widely employed.
- FDMA divides the frequency band into various channels based on the FDM techniques. Each of these can carry a voice conversation or, with digital service, carry digital data.
- TDMA is digital transmission technology that allows a number of channels to access a single radio frequency (RF) channel without interference by allocating unique time slots to each channel.

Notes

- The digital transmission requires a low pass channel with high bandwidth. The analog transmission can be carried on band pass channels. The different methods that convert binary data or a low pass analog signal into a band pass analog signal is called modulation.
- The digital to analog conversion includes ASK (Amplitude Shift Keying), FSK (Frequency Shift Keying), PSK (Phase Shift Keying), QPSK (Quadrature Phase Shift Keying), QAM (Quadrature Amplitude Modulation) and have been explained under the section Modem Modulation Techniques.
- Analog to analog signal conversion involves amplitude modulation, frequency modulation and phase modulation techniques.

6.7 Keywords

Amplitude Modulation: It involves the modulation of the amplitude of the carrier as analog sine wave.

Amplitude Shift Keying: ASK refers to technique how the carrier wave is multiplied by the digital signal f(t) so that the strength of the carrier wave is varied to represent binary 0 and 1.

Baud Rate: It is the number of times per second the line condition can switch from "1" to "0".

Binary Phase Shift Keying: BPSK involves two possible phases shift for the modulation.

Carrier Signal: It is the base signal generated by the sending device whose one of the characteristics is altered in accordance with the digital signal to be modulated.

Differential Phase Shift Keying: In this method, the modem shifts the phase of each succeeding signal in a certain number of degrees.

FDM: In frequency division multiplexing, multiple channels are combined together for transmission over a single channel.

FDMA: This divides the frequency band into various channels based on the FDM techniques. Each of these can carry a voice conversation or, with digital service, carry digital data.

Frequency Modulation: Frequency Modulation involves the modulation of the frequency of the analog sine wave.

Frequency Shifted Keying: FSK describes the modulation of a carrier (or two carriers) by using a different frequency for a 1 or 0.

Inter modulation: It involves two (or more) sinusoids effect one another to produce undesired products, that is, unwanted frequencies (noise).

Modems: Refers to the modulator and demodulator that converts analog signal to digital signal and vice versa.

Modulation: It is the act of translating some low-frequency (base band signal) such as voice, data, etc. to a higher frequency.

Multiplexing: Refers to the process in which multiple channels are combined for transmission over a common transmission path.

Phase Modulation: Phase Modulation (PM) is similar to frequency modulation. Instead of the frequency of the carrier wave changing, the phase of the carrier wave changes.

Phase Shift Keying: In this modulation method a sine wave is transmitted and the phase of the sine wave carries the digital data or the phase of sine wave is varied to represent binary 1 or 0 and both the amplitude and frequency of the analog waveform are kept constant.

Notes

Quadrature Amplitude Modulation: This technique is based on the amplitude modulation and phase modulation to improve the performance of the amplitude modulation.

Quadrature Phase Shifted Keying: In the case of 4 different phase shifts possibilities for each symbol which means that each symbol represents 2 bits the modulation will be called quadrature PSK (QPSK).

Space Division Switching: Refers to the kind of switch developed for analog environment. Crossbar switch is the simplest possible space division switch where each packet takes a different path through the switch depending on its destination. Time division switching is based on multiplexing for digital transmission.

TDM: Refers to the process to merge data from several sources into a single channel for communication over transmission media like telephone lines, microwave system or satellite system.

TDMA: This is a digital transmission technology that allows a number of channels to access a single radio frequency (RF) channel without interference by allocating unique time slots to each channel.

Virtual circuit: This is a logical path selected out of many possible physical paths available between two or more points.

WDM: This is defined as the fiber-optic transmission technique that employs two or more optical signals having different wavelengths to transmit data simultaneously in the same direction over one fiber, and later on is separated by wavelength at the distant end.

6.8 Review Questions

1. When a channel is called a circuit?
2. How does multi-channeling help broadband transmission?
3. How can a single transmission be shared among different signals? Describe any two methods.
4. Why are TDM and FDM methods employed for use in the telephone system, but not for computing networks?
5. What is the purpose of guard band in FDM?
6. How can a single transmission be shared among different signals? Describe any two methods.
7. Why are TDM and FDM methods employed for use in the telephone system, but not for computing networks?
8. Why do we normally use a sinusoidal wave as a carrier wave to transmit information?
9. How is it possible to transmit the output produced by a computer over a computer network connected via telephone lines?
10. What is modulation? How does modulation help in reducing the size of antenna for transmission?

Answers: Self Assessment

1. Wireless
2. wavelength-division multiplexing (WDM).

Notes

3. transmission media
4. virtual circuit
5. circuit
6. False
7. True
8. False
9. True
10. False

6.9 Further Readings

Books

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall

Behrouz A. Forouzan and Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies

Burton, Bill, *Remote Access for Cisco Networks*, McGraw-Hill Osborne Media McGraw-Hill Osborne Media

Rajneesh Agrawal and Bharat Bhushan Tiwari, *Computer Networks and Internet*, Vikas Publication

Unit 7: Data Link Layer

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

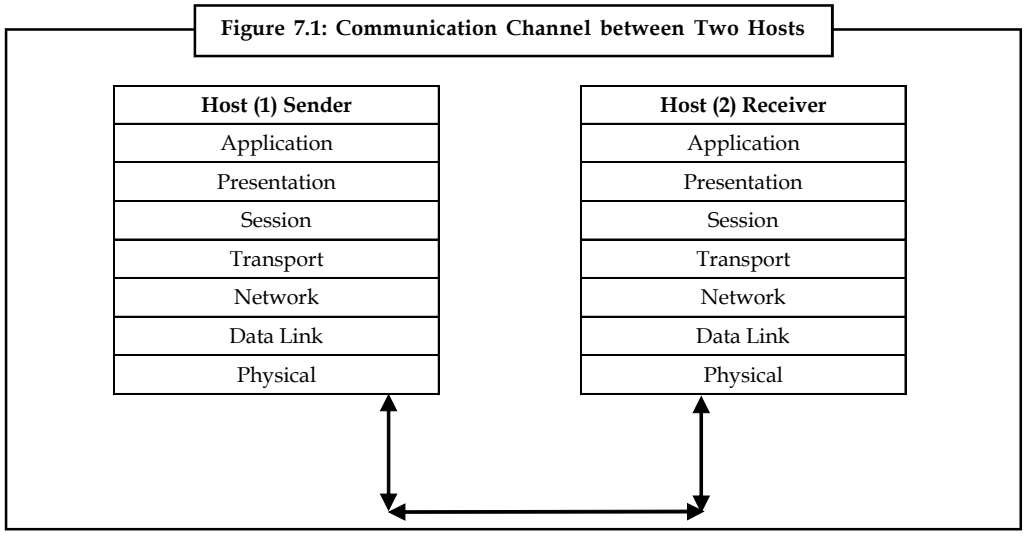
- Explain the significance & functions
- Discuss data link layer design issues including services provided to the network layer, framing, error control and flow control
- Describe error detection and correction techniques along with error-correcting codes and error-detecting codes

Introduction

Data link layer is the second layer after physical layer in the OSI reference model. It describes the techniques to access a shared communication channel and reliable transmission of data frame in computer communication environment. It receives a raw stream of bits for the physical layer at sender machine. The raw stream of data is created using different technologies like cable, DSL, wireless, optical fiber, etc. The data link layer transforms data free of undetected transmission errors to the network layer. Data link layer accomplishes this task by using acknowledgment frames and error detection algorithms. In other words, the task of the data link layer is to transmit the bits to the destination machine. The data link layer of the destination machine, then, hand over thus received data to the network layer for processing. The communication between any two hosts that are physically connected via a channel can be shown in Figure 7.1.

Notes

Figure 7.1: Communication Channel between Two Hosts



Briefly, the data-link layer provides transfer of a datagram across a communication channel between two adjacent machines. Its main tasks, which will be described in this unit, are framing, checksums, error detection and correction, acknowledgement, flow control, well-defined reliable service interface to the network layer, encapsulating packets from network layer to frames, etc. There are many different types of link-level technologies that can be used to connect two nodes or machines. Examples of link-layer protocols are Ethernet, token ring, FDDI, and PPP.

7.1 Data Link Layer Design Issues

7.1.1 Services Provided to Network Layer

The data link layer provides well-defined interface to network layer, handles transmission errors, regulate flow of data and keeps sender and receiver in harmony by offering the following functionalities:

To provide a well-defined and reliable service interface to the layer 3 or network layer that will also be dependent on the efficiency and error rate of the underlying physical layer. The data link layer accomplishes these activities in the following manner:

(a) *Unacknowledged connectionless service:* This involves independent frames from source host to the destination host without any acknowledgment mechanism. It does not include any connection setup or release. It does not deal with frame recovery due to channel noise.

(b) *Acknowledged connectionless service:* Communication channel is more error prone. This necessitates acknowledgement service for each frame sent between two hosts to ensure that the frame has arrived correctly. However, the transport layer also sends a message for acknowledgement.

(c) *Acknowledged connection-oriented service:* The data link layer provides this service to the network layer by establishing a connection between the source and destination hosts before any transfer of data takes place. The order of each frame is maintained and guaranteed the receipt of frame by receiving hosts. Communication between source and destination hosts completes in three phases. They are connection setup, actual frame transmission and connection release.

Notes

7.1.2 Framing

The data link layer receives a raw bit stream from the physical layer that may not be error free. To provide a reliable transfer of bit streams to the network layer the data link layer breaks the bit stream into frames. It then computes the checksum for each frame, which is transmitted with the frame. The destination host receives a frame and computes another checksum from its data to compare with the transmitted frame. This ensures the data link layer of the receiver to detect and correct frames. However, some of the checksum method does not provide correction.

7.1.3 Error Control

It also involves sequencing frames and sending control frames for acknowledgement. A noisy channel may cause flipping of bits, losing bits from a frame, introducing new bits in the frame, frames completely disappearing, etc during communication. For reliable communication, the destination host sends positive or negative acknowledgements accordingly to the source host within a specified time limit. The source host has a timeout to resend the frame again if it does not receive an acknowledgement in a given time period from destination host. Also, each outgoing frame is assigned a sequence number to prevent the destination host data link layer from passing the same frame more than once to the network layer. This entire affair is an integral part of data link layer design.

7.1.4 Flow Control

Another important issue in the design of the data link is to control the rate of data transmission between two source and destination hosts. If there is mismatch between the source and destination hosts data sending and receiving speed, it will cause dropping of packets at the receiver end. It further causes the sender to timeout on the acknowledgement packets, causing retransmission. Thus making the network less efficient.

Task What are the services provided by data link layer to the network layer?

7.2 Error Detection and Correction

It is a collection of methods involving coding to detect errors in transmitted or stored data and to correct them. We must have studied earlier some of the simplest form of error detection where we add a parity bit or we perform a cyclic redundancy check. In case of using multiple parity bits, we can not only detect the error, but also which bits have been inverted, and should therefore be re-inverted to restore the original data. The more extra bits are added, the greater the chance that multiple errors will be detectable and correctable. There are different methods depending upon single error correction, double error detection (SECDEC).

7.2.1 Error Detection Codes

Redundancy

One error detection mechanism that would satisfy these requirements would be to send every data unit twice. The receiving device would then be able to do a bit-for-bit comparison between the two versions of the data. Any discrepancy would indicate an error, and an appropriate

Notes

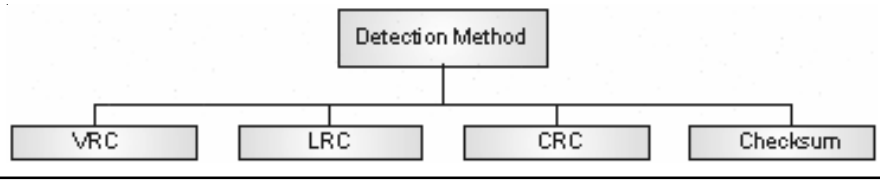
correction mechanism could be set in place. This system would be completely accurate (the odds of errors being introduced into exactly the same bits in both sets of data are infinitesimally small), but it would also be insupportably slow. Not only would the transmission time double, but the time it takes to compare every unit bit by bit must be added.

The concept of including extra information in the transmission solely for the purposes of comparison is a good one. But instead of repeating the entire data stream, a shorter group of bits may be appended to the end of each unit. This technique is called redundancy because the extra bits are redundant to the information: they are discarded as soon as the accuracy of the transmission has been determined.

Figure shows the process of using-redundant bits to check the accuracy of a data unit. Once the data stream has been generated, it passes through a device that analyzes it and adds on an appropriately coded redundancy check: The data unit, now enlarged by several bits, travels over the link to the receiver. The receiver puts the entire stream through a checking function. If the received bit stream passes the checking criteria, the data portion of the data unit is accepted and the redundant bits are discarded.

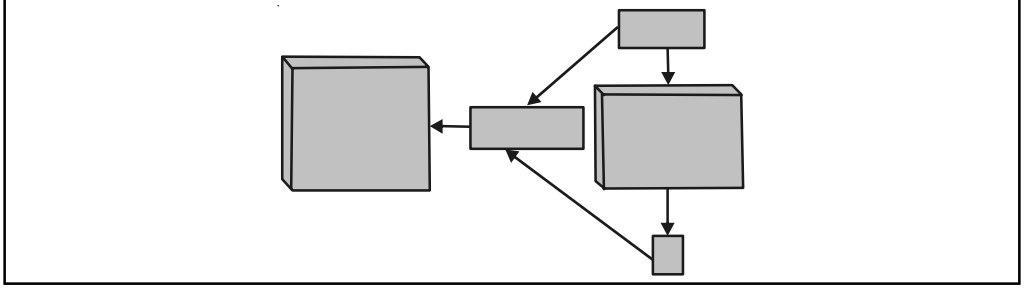
Four types of redundancy checks are used in data communication: vertical redundancy check (VRC) (also called parity check), longitudinal redundancy check (LRC), cyclical redundancy check (CRC), and checksum. The first three, VRC, LRC and CRC are normally implemented in the physical layer for use in the data link layer. The fourth, checksum, is used primarily by upper layers.

Figure 7.2: Four Types of Redundancy Check



(a) ***Vertical Redundancy Check***: The most common and least expensive mechanism for error detection is the vertical redundancy check (VCR), often called a parity check. In this technique, a redundant bit, called a parity bit, is appended to every data unit so that the total number of bit is in the unit (including the parity bit) becomes even.

Figure 7.3: Even Parity VRC Concept

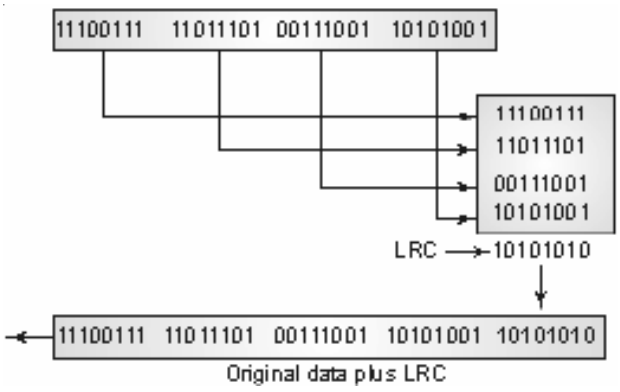


Suppose we want to transmit the binary data unit 1100001. Adding together the number of 1s gives us 3, an odd number. Before transmitting, we pass the data unit through a parity generator. The parity generator counts the 1st and appends the parity bit (a 1 in this case) to the end. The total number of is now four, an even number. The section now transmits the entire expended unit across the network link. When it reaches its destination, the

Notes

receiver puts all the eight bits through an even-parity checking function. If the receiver sees 11100001, it counts for 1st, an even number, and the data unit passes. But what if the data unit has been damaged in transit? What if, instead of 11100001, the receiver sees 11100101? The receiver known that an error has been introduced into the data somewhere and therefore rejects the whole unit. Note that for the sake of simplicity, we are discussing here even-parity checking, where the number of 1s should be an even number. Some system may use odd-parity checking, where the number of 1s should be odd. The principle is the same; the calculation is different.

Figure 7.4: Original Data plus LRC



(b) ***Longitudinal Redundancy Check:*** In longitudinal redundancy check (LRC), a block of bits is organized in a table (rows and columns). For example, instead of sending a block of 32 bits, we organize them in a table made of four rows and eight columns, as shown in figure. We then calculate the parity bit for each column and create a new row of eight bits, which are the parity bits for the whole block.

Notes Note that the first parity bit in the fifth row is calculated based on all forst bits. The second parity bit is calculated based on all second bits, and so on. We then attach the eight parity bits to the send them to the receiver.

(c) ***Cyclic Redundancy Check:*** The third and most powerful of the redundancy checking techniques if the cyclic redundancy check (CRC). Unlike VRC and LRC, instead of adding bits together to achieve a desired parity, a sequence of redundant bits, called the CRC and CRC remainder, is appended to the end of a data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At its destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be intact and is therefore accepted. A remainder indicated that the data unit has been damaged in transit and therefore must be rejected.

The redundancy bits used by CRC are derived by dividing the data unit by a predetermined divisor, the remainder is the CRC. To be valid, a CRC must have two qualities: it must have exactly one less bit than the divisor, and appending it to the end of the data string must make the resulting bit sequence exactly divisible by the divisor. Both the theory and the application of CRC error detection are straightforward. The only complexity is a deriving the CRC. In order to clarify this process, we will start with an overview and add complexity as we go. Figure 7.5 provides an outline of the three basic steps.

Notes

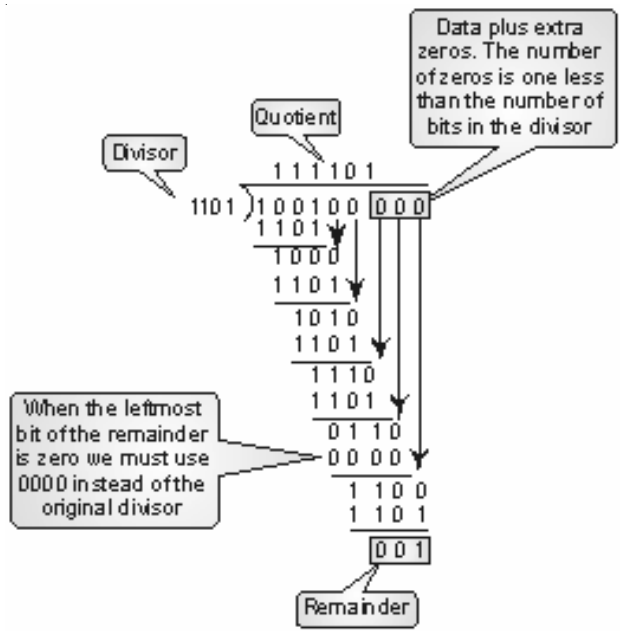
- First, a string of numbers is appended to the data unit. The number *n* is one less than the number of bits in the predetermined divisor, which is n + 1 bit.
- Second, the newly elongated data unit is divided by the divisor using a process called binary division. The remainder resulting from this division is the CRC.
- Third, the CRC of n bits derived in step 2 replaces the appended 0s at the end of the data unit. Note that the CRC may consist of all 0s.

The data unit arrives at the receiver data first, followed by the CRC. The receiver treats the whole string as a unit and divides it by the same divisor that was used to find the CRC remainder.

If the string arrives without error, the CRC checker yields a remainder of zero and the data unit passes.

If the string has been changed in transit, the division yields a non-zero remainder and the data unit does not pass.

Figure 7.5



The CRC Generator

A CRC generator used modulo-2 division, Figure shows the process. In the first step, the four-bit divisor is subtracted from the first four bits of the dividend. Each bit of the divisor is subtracted from the corresponding bit of the dividend without disturbing the next higher bit. In our example, the divisor, 1101, is subtracted from the first four bits of the dividend, 1101. Yielding 1001. Yielding 100 (the leading 0 of the remainder is dropped off).

The next unused bit from the dividend is then pulled down to make the number of bits in the remainder equal to the number of bits in the divisor. The next step, therefore, is 1000-1101, which yields 101, and so on.

In this process, the divisor always begins with a 1; the divisor is subtracted from a portion of the previous dividend/remainder that is equal to it in length; the divisor can only be subtracted

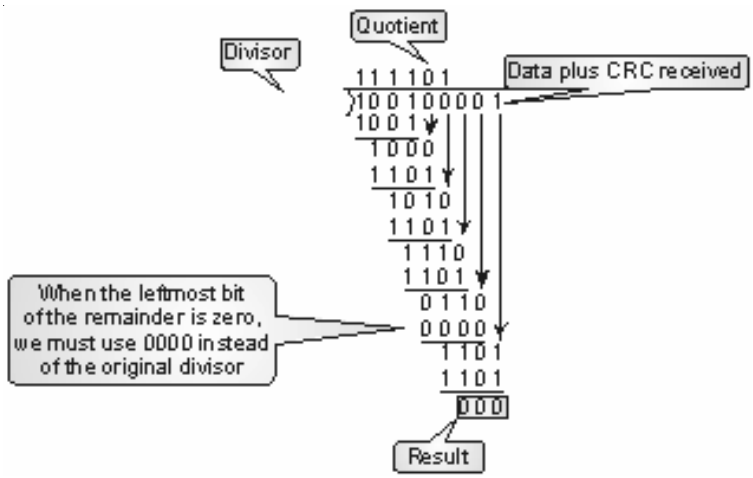
Notes

from a string of 0s, of the same length as the divisor, replaces the divisor in that step of the process. For string of 0s, of the same length as the divisor, replaces the divisor in that step of the process. For example, if the divisor is four bits long, it is replaced by four 0s. (Remember, we are dealing with bit patterns, not with quantitative values; 0000 is not the same as 0). This restriction means that, at any step, the leftmost subtraction will be either 0 – 0 or 1 – 1, both of which equal 0. So, after subtraction, the leftmost bit of the remainder. Note that only the first bit of the remainder is dropped – if the second bit is also 0. It is retained, and the dividend/remainder for the next step will begin with 0. This process repeats units the entire dividend has been used.

The CRC Checker

A CRC checker functions exactly like the generator. After receiving the data appended with the CRC, it does the same modulo – 2 divisions. If the remainder is all 0s, the CRC is dropped and the data accepted; otherwise, the received stream of bits is discarded and data are resent. Figure shows the same process of division in the receiver. We assume that there is no error. The remainder is therefore all 0s and the data are accepted.

Figure 7.6: CRC Checker



Self Assessment

Fill in the blanks:

1. The data link layer receives a raw bit stream from the ……. layer that may not be error free.
2. Some of the examples of ……. check are audio storage and playback devices such as audio CD's.
3. CRC codes are also called as …….. codes.
4. …… consists of Even Parity and Odd Parity Method.

7.2.2 Error Correction Code

An error-correcting code (ecc) or forward error correction (fec) code is a system of adding redundant data, or parity data, to a message, such that it can be recovered by a receiver even when a number of errors (up to the capability of the code being used) were introduced, either during the process of transmission, or on storage. Since the receiver does not have to ask the

Notes

sender for retransmission of the data, a back-channel is not required in forward error correction, and it is therefore suitable for simplex communication such as broadcasting. Error-correcting codes are frequently used in lower-layer communication, as well as for reliable storage in media such as cds, dvds, hard disks, and ram.

Error-correcting codes are usually distinguished between convolution codes and block codes:

- Convolution codes are processed on a bit-by-bit basis. They are particularly suitable for implementation in hardware, and the viterbi decoder allows optimal decoding.
- Block codes are processed on a block-by-block basis. Early examples of block codes are repetition codes, hamming codes and multidimensional parity-check codes. They were followed by a number of efficient codes, reed-solomon codes being the most notable due to their current widespread use. Turbo codes and low-density parity-check codes (ldpc) are relatively new constructions that can provide almost optimal efficiency.

Shannon's theorem is an important theorem in forward error correction, and describes the maximum information rate at which reliable communication is possible over a channel that has a certain error probability or signal-to-noise ratio (snr). This strict upper limit is expressed in terms of the channel capacity. More specifically, the theorem says that there exist codes such that with increasing encoding length the probability of error on a discrete memory less channel can be made arbitrarily small, provided that the code rate is smaller than the channel capacity. The code rate is defined as the fraction k/n of k source symbols and n encoded symbols.

The actual maximum code rate allowed depends on the error-correcting code used, and may be lower. This is because Shannon's proof was only of existential nature, and did not show how to construct codes which are both optimal and have efficient encoding and decoding algorithms.

Self Assessment

State whether the following statements are true or false:

5. Shannon's theorem is an important theorem in forward error correction.
6. The actual maximum code rate allowed depends on the error-correcting code used.
7. The code rate is defined as the fraction k/n of k source symbols and n encoded symbols.
8. Block codes are processed on a bit-by-bit basis.
9. Early examples of block codes are repetition codes, hamming codes and multidimensional parity-check codes.
10. Turbo codes and low-density parity-check codes (ldpc) are relatively new constructions that can provide almost optimal efficiency.

7.3 Summary

- Data link layer describes the techniques to access a shared communication channel and reliable data transmission. Its main tasks are framing, checksums, error detection and correction, acknowledgement, flow control, encapsulating packets from network layer to frames, etc.
- The data link layer provides unacknowledged connectionless service, acknowledged connectionless service and acknowledged connection-oriented service.
- Parity check is the simplest form of error detection method as the receiver needs to count only the number of 1's in the received data stream with additional parity bit.

Notes

- Checksum is a simple type of redundancy check used to detect errors in data.
- Cyclic Redundancy Check is used widely in computer networks, is a technique of providing a data string added to packets of information that can be used to detect errors in the data packets.
- Stop and Wait protocol is easiest to implement and proves to be the most efficient on an error free communication channel. However, an error free communication channel is practically not possible.

7.4 Keywords

Acknowledged Connection-oriented Service: The data link layer provides this service to the network layer by establishing a connection between the source and destination hosts before any transfer of data takes place.

Acknowledged Connectionless Service: Refers to delivery of each frame sent between two hosts arrives correctly.

Checksum: Refers to an algorithm that calculates the binary values in a packet or other block of data and stores the results with the data to compare with a new checksum at the other end.

Cyclic Redundancy Check: Refers to a technique of providing a data string added to packets of information that can be used to detect errors in the data packets.

Error Control: Involves sequencing frames and sending control frames for acknowledgement.

Flow Control: Refers to control the rate of data transmission between two source and destination hosts.

Framing: Provides a reliable transfer of bit streams to the network layer the data link layer breaks the bit stream into frames.

Go Back N: The Go Back N protocol enables the source machine to have more than one outstanding frame at a time by using buffers.

High-level Data Link Control: Refers to receipt of data that is checked after multiple frames are sent for improved transmission efficiency. It also offers a form of advanced error control called CRC (Cyclic Redundancy Check).

Parity Checks: Consists of even parity and odd parity method. The operation of receiver is simple, as the receiver needs to count only the number of 1's in the received data stream with additional parity bit.

Unacknowledged Connectionless Service: Refers to the independent frames from source host to the destination host without any acknowledgment mechanism.

7.5 Review Questions

1. What is the data link protocol?
2. What advantages does Selective Repeat sliding window protocol offer over Go Back N protocol?
3. What is the purpose of flow control?
4. Describe how does finite state machine model carry out protocol verification?
5. What are different data link protocols available? Why does PPP have become popular?

Notes

Answers: Self Assessment

1.	physical	2.	parity
3.	Polynomial	4.	Parity check
5.	True	6.	True
7.	True	8.	False
9.	True	10.	True

7.6 Further Readings

Books

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall.

Behrouz A. Forouzan and Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies.

J. D. Spragins, *Telecommunications Protocols and Design*, Addison-Wesley.

Unit 8: Data Link Protocols

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Learn various concepts of elementary data link protocols with comprehensions of an unrestricted simplex protocol, a simplex stop-and-wait protocol and a simplex protocol for a noisy channel
- Comprehend sliding window protocols with various examples
- Know about protocol verifications and finite state machine model
- Discuss data link protocols such as high level data link control and the data link layer in the Internet

Notes

Introduction

The data link layer is layer 2 of the seven-layer osi model of computer networking. It corresponds to, or is part of the link layer of the tcp/ip reference model. The data link layer is the protocol layer that transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC and ADCCP for point-to-point (dual-node) connections.

8.1 Elementary Data Link Protocols

The basic objective of computer communication in a network environment is to send an infinite long message from source node to destination node. To explain how data link layer accomplishes data communication to the destination host at the data link layer, it is assumed here that the layer 3 or network layer has a long message to send to the destination host. The message available at network layer is broken into packets to pass to data link layer. The data link layer encapsulates each packet in a frame by adding header and trailer. Data link layer does not bother for the contents of packet.

8.1.1 Simplex Stop and Wait

An error free communication channel is assumed. The source node retrieves a packet from the network layer and encapsulates it into a frame to transmit. After transmission, the source node waits for an acknowledgement from the destination node. After receiving, the acknowledgement, the loop starts over again.

At the destination node, the machine waits for a frame from source destination. After receiving a frame, it passes the frame to the network layer and sends an acknowledgement for the frame to the source node. It then loops back to wait for next frame and the process continues till the End of File frame is reached.

Stop and wait protocol involves only one outstanding frame at a time so no sequence numbers are required. The acknowledgement the destination node sends back to the source machine is an empty frame. The Stop and Wait protocol is easy to implement and does not call for congestion because there is only one frame outstanding at any time. Also loss of frames is ruled out due to congestion. The destination host will also not be swamped by the sender. The disadvantage of this method is that an error free communication channel does not exist. Hence, it is easy that a frame or an acknowledgement mat get lost or damaged and a deadlock situation may occur where neither the source or destination nodes can advance.

8.1.2 Positive Acknowledgement with Retransmission Protocol (PAR)

It is an improvement on the Stop and Wait protocol. The source machine retrieves a packet from the network layer, encapsulates it into a frame with a sequence number to transmit to the destination node. After transmission, the source machine attempts to retrieve an acknowledgement from the physical layer. Once an acknowledgement arrives with the correct sequence number, next packet to send from network layer is retrieved and accordingly, the sequence number to send next packet is updated. In this manner, the loop starts over. If no frame is retrieved from the physical within specified time, the physical layer times out or an acknowledgement with an incorrect sequence number arrives. In this case, the last frame sent is retransmitted and thus the loop starts over.

Notes

At the destination node, the receiving machine waits for reception of the frame from the physical layer. Once, the frame is received, the sequence number is checked. If it is found correct, the packet is passed to the next layer i.e. network layer. The destination machine sends an acknowledgement for the frame to the source machine for the sequence number just received. If an incorrect or out of sequence frame arrives, the destination machines requests for retransmission to the source node.

PAR involves only one outstanding frame at a time, a sequence number must be used to determine if any frames are lost or damaged. This scheme requires only two sequence numbers because at a time there will be only one outstanding frame and sequence number will not change until a positive acknowledgement is received. This protocol simply uses '1' and '0' as sequence numbers. The *PAR* protocol is simple to implement. Sequence numbers and transmitting an acknowledgement for frame received in sequence keeps the source and destination hosts in synchronization.

The protocol is able to handle congestion, lost frames and damaged frames because frames are retransmitted until a positive acknowledgement is received. However, this characteristic makes the PAR protocol inefficient because the number of frames sent to transfer the entire message reliably becomes large frames on loss of acknowledgements.

8.2 Sliding Window Protocols

In data communications systems, it may be defined as the control of the rate at which data are transmitted from a terminal so that the data can be received by another terminal. By maintaining a compatible data transfer rate between sending and receiving ends, it prevents network congestion. A high-speed computer, for example, may generate traffic faster than the network can transfer it or faster than the destination device can receive and process it. In order to ensure effective transmission, source device requires an acknowledgment from the destination after a certain number of packets have been transmitted. This is a Windowing flow-control scheme. If the destination does not receive one or more of the packets for some reason, such as overflowing buffers, it does not receive enough packets to send an acknowledgment. The source then retransmits the packets at a reduced transmission rate.

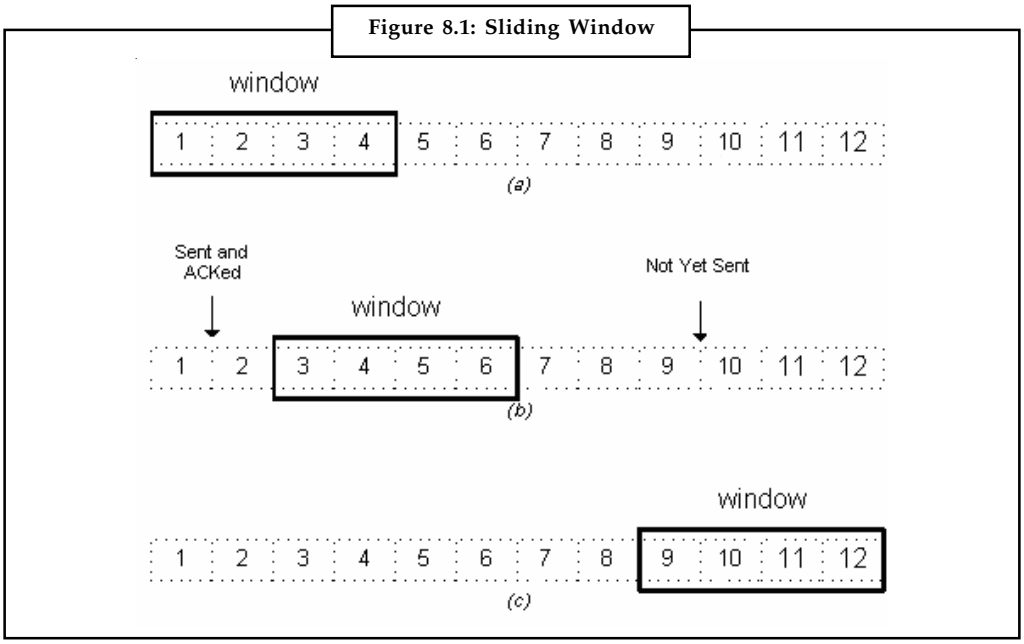
As we have seen in the foregoing topic that flow control is a technique whose primary purpose is to properly match the transmission rate of sender to that of the receiver and the network. However, it is not the same as congestion control. Congestion control is primarily concerned with a sustained overload of network intermediate devices such as IP routers.

In order to maintain a proper flow of data a window field is created to adjust the rate of flow of the byte stream between communicating devices. Figure 8.1 illustrates the concept of the sliding window.

In this simple example, there is a 4-byte sliding window. Moving from left to right, the window "slides" as bytes in the stream are sent and acknowledged. The size of the window and how fast to increase or decrease the window size is an area of great research.

Notes

Figure 8.1: Sliding Window



Sliding Window: Go Back N

The Go Back N protocol enables the source machine to have more than one outstanding frame at a time by using buffers. It thus overcomes the problem of PAR. The source machine keeps a buffer of a predetermined size that receives a packet, stores it in the correct empty slot in the buffer, creates a frame with the correct sequence number and transmits it. The corresponding logical timer is reset to 0 and the upper bound of the window is slid up by circularly incrementing for the next frame to transmit.

In case of no buffers are empty, the physical layer is checked to find out if an acknowledgement is there. If a good frame is received with the acknowledgement number within the current window, the number of buffers used is then decrement and the logical timer is reset to a negative value to indicate an unused slot. This enables to slide the Lower Bound of the window by circularly incrementing the acknowledgement number expected. This procedure creates a loop until expected acknowledgement equals received acknowledgement. This clears the received acknowledgement and the previous frames that have not been acknowledged so far.

Subsequent to this, logical timers are updated if a bad frame or out of window frame arrives. In case of a frame timed out, the same frame is retransmitted and the logical timer is reset to 0. Hence, the next frame will time out and will be re-sent on the next iteration of the loop. Thus the timed out frame and all the subsequent frames are retransmitted.

At the destination machine, the receiving machine waits until a good frame arrives. It checks the sequence number, if it is not the expected sequence number it re-sends an acknowledgement for the last correct sequence number received. If the sequence number is expected one, it passes the packet to the Network layer. Simultaneously, it updates the last correct sequence number received and circularly increments the expected next sequence number. An acknowledgement is thus created and transmitted. This creates loop back to the physical layer to retrieve the next frame.

Sliding Window: Selective Repeat

The Selective Repeat protocol intends to improve the problems of the Go Back N protocol. This is achieved by providing buffers at source and destination hosts to enable the source node to

Notes

have more than one outstanding frame at a time and destination node to accept out of order frames and store them in its window.

In Selective Repeat scheme, time-outs, loop iterations and retransmissions are all the same as Go Back N except that the source node retransmits the corresponding frame identified by the not acknowledgement but not all subsequent frames. Hence, the destination node that keeps a window of frames, it requires only to retransmit the timed out frame but not the whole series.

At the receiving end, the destination node waits until a frame arrives. In case of damaged frame, timeout frames or an out of sequence frame arriving, a not acknowledgement is sent for the expected sequence number. If there is empty slot in the buffer of a destination machine, a packet is stored in the correct slot and the slot is flagged as used. If all slots are full the packet is passed to the network layer with a flag set to transmit an acknowledgement and the buffer slot is reset to empty. This increases the upper bound of the window and the lower bound for expected frame is circularly incremented. Subsequent to this, it loops back to find out the buffer slot for expected sequence number. The loop continues until the expected slot is empty. Thus, all packets available in buffer are passed to the network layer in order.

Notes The Selective Repeat protocol is more difficult to implement than other types of protocols as given above.

In this case, the sequence numbers are kept greater than the window size to avoid overlap in the window. This enables source and destination machine to be in synchronization even when frames and acknowledgements are lost at a very high rate. Thus, enhanced buffering and acknowledgements allow this protocol to easily handle congestion, damaged frames and lost frames. It also calls for a much higher timeout value as compared to Go Back N in order to reduce the number of frames sent. If a lower timeout value is kept, it will call for too many frames for retransmission unnecessarily.

8.3 Protocol Verification

Protocols are a set of rules, which govern the exchange of messages between two nodes or processes to provide a particular set of services to its local protocol layers above and to furnish a set of logical rules or protocols to its remote peer machines. Protocols are verified either during the design phase before implementation of the system or during the testing and simulation phase after implementation of the system. The design verification is considered to reduce the cost of protocol development and testing. Design verification divides the work into two tasks. They are service-specification verification and protocol specification verification. The protocol specification verification attempts to detect the existence of logic errors in the protocol design.

Interaction and concurrency are two major components of any multi-process local or distributed systems. Interaction is coordination or synchronization among processes. Concurrency is parallelism between different processes. In other words, concurrency is the execution of processes in a multi process local or distributed system simultaneous and independent from any other processes in the same system.

Finite State Machine Models

In the Finite State Machine (FSM) model, each process has a communicating finite state machine or a directed labeled graph. The directed labeled graph has nodes and edges to represent states and transitions respectively. A message transmission transition is indicated by a "-" (minus

Notes

sign) and a message reception transition is indicated by a "+" (plus sign). A full duplex, error-free, FIFO channel connects each pair of processes.

Figure 8.2: A Correctly Designed Protocol

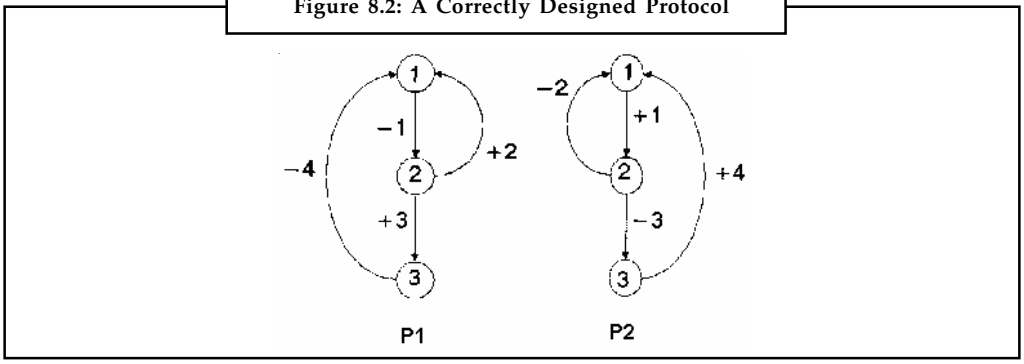


Figure 8.2 shows a correctly designed protocol involving two processes P1 and P2. Initially, both processes are in their state 1. P1 transmits message 1 to P2 and enters state 2. P2 receives the message 1 and enters state 2. At this time, P2 either transmits message 2 and returns to the initial state or transmits message 3 and enters a new state 3. Similarly, P1 returns to its initial state or goes to a new state 3 depending on the message received. When both the processes are in state 3, the only possible transition is the transmitting and receiving of message 4 by P1 and P2 respectively.

Petri Net Models

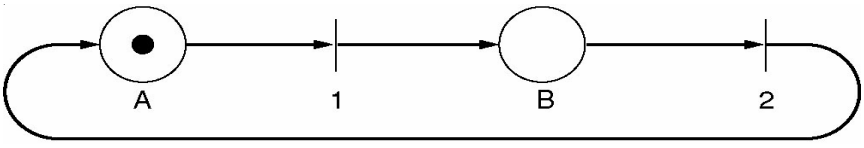
Petri net model also uses a graph to indicate states and transitions and consist of four parts:

Places: It is denoted by a circle and represents the state of the system. Figure 8.3 has two places A and B.

Transitions: It is denoted by horizontal or vertical bar.

Arrows: Each transition has zero or more input arrows coming from its input places and zero or more input arrows going to its output places.

Figure 8.3: A Petri Net with Two States



Tokens: It is denoted by heavy dot and tells the current state of the system. Figure 8.3 indicates that the system is in State A.

- A transition is enabled if each of its input places has at least one input token.
- Any enabled transition is fired and the tokens at each input places are removed to store in each of the output places.
- After firing, the number of tokens may vary depending upon the number of input and output places.
- One transition can fire at a time; however the choice of a transition to fire is indeterminate.

Petri net of Figure 8.3 can be used to model any two phase process and therefore deterministic.

Notes

Petri nets are used to detect protocol failures similar to the use of finite state machine. For example, if some firing sequence included transition Tn twice without transition Tn+1 intervening, the protocol would be incorrect.

Self Assessment

Fill in the blanks:

1. ..... describes the techniques to access a shared communication channel and reliable transmission of data frame in computer communication environment.
2. ..... does not include any connection setup or release and does not deal with frame recovery due to channel noise.
3. ..... refers to a reliable transfer of bit streams to the network layer for which the data link layer breaks the bit stream into frames.
4. ..... controls mismatch between the source and destination hosts data sending and receiving speed and therefore dropping of packets at the receiver end.
5. In stop and wait protocol, the acknowledgement frame has ..... bits that the destination node sends back to the source machine.
6. Positive Acknowledgement with Retransmission Protocol (PAR) uses ..... to determine if any frames is lost or damaged.
7. The Go Back N protocol overcomes the problem of PAR by enabling the source machine to have more than ..... at a time by using buffers.

8.4 Example Data Link Protocols

Data link protocols regulate communication flow between various computers. A wide variety of computers and communication technologies are used to carry out useful tasks. These include mainframe computers, local area networks, workstations, personal computers, and proprietary and standards based networking platforms. All of these products are not interoperable and it is not easy to exchange data across different systems and applications. Therefore, standards were developed to ensure the interrelationship of many different standards adopted by various vendors. To establish a meaningful session, a certain sets of rules need to be adopted by vendors of networking device.

Some of the examples of data link protocol are High Level Data Link Control (HDLC) protocol and Point-to-Point Protocol (PPP). The discussion here of the simpler HDLC and PPP protocols will explore many of the most important features of data link protocols.

8.4.1 High-level Data Link Control (HDLC)

HDLC procedure is standardized by ISO. This is suitable for high-speed transmission of large amounts of data, something the basic control procedure cannot provide. HDLC procedure has been standardized based on the SDLC. In addition to characters, bit strings of a desired length can also be transmitted through this procedure. The unit of data transmission is called a frame. With the basic control procedure, receipt of data is checked after multiple frames are sent for improved transmission efficiency. It also offers a form of advanced error control called CRC (Cyclic Redundancy Check).

The advantage of this procedure is that the sending equipment can send multiple blocks of data at one time for improved transmission efficiency. As the receiving equipment must inform the

Notes

sending equipment how much data has been received, therefore, it is necessary to attach a sequence number to each piece of data.

The unit of data transmission is called a frame. The frame format of HDLC is depicted in Figure 8.4. Each frame has a 01111110 bit pattern, called a flag, at its beginning and end. That is, HDLC procedure uses a flag synchronous system.

(1) Bit order of transmission (Information Frame)

(2) Bit order of Transmission (Supervisory Frame)

Figure 8.4: HDLC Frame Format

(1) Bit order of transmission (Information Frame)

Flag	Address	Control	Information	FCS	Flag
F 0111110	A 8 Bits	C 8 Bits	I N Bits	FCS 16 Bits	F 01111110

(2) Bit order of Transmission (Supervisory Frame)

Flag	Address	Control	FCS	Flag
F 0111110	A 8 Bits	C 8 Bits	FCS 16 Bits	F 01111110

In addition to these two flags, a frame consists of the following fields:

1. ***Address field:*** This indicates the destination or source address of a frame.
2. ***Control fields:*** This indicates the command or response addressed to remote equipment. The sequence number mentioned earlier is also included.
3. ***Information field:*** This contains message.
4. ***FCS (Frame Check Sequence):*** This is 16 bit sequence for error control.

The frame format given in (2) of Figure 8.4 is for response only and does not include any information field. As the control field holding control information and the information field holding information are clearly separated, any types of codes can be sent through the HDLC procedure. Also data sequence numbers are included in the control field, consecutive data blocks (frame) can be sent without checking receipt of each data block.

8.5 Point-to-Point Protocol (PPP)

PPP is for a dialup link from residential hosts. Hence, it is one of the most widely deployed data link protocols. The Point-to-Point Protocol is a data link layer protocol and operates over a point-to-point link that connects two communicating link-level peers at each end of the link This link may be a serial dialup telephone line, a SONET/SDH link, an X.25 connection, an ISDN circuit, etc.

The Point-to-Point Protocol (PPP) is used to transmit datagrams across a serial connection as an encapsulation protocol to transport IP traffic over point-to-point links. The PPP supports the assignment and management of IP addresses, asynchronous and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, etc by providing an extensible Link Control Protocol (LCP) along with Network Control Protocols (NCPs). The advantages of PPP are that it is capable of carrying a large number of protocols and thus operates beyond the

Notes

IP protocol, providing error detection on the link itself, allowing the hosts to negotiate options like IP address, maximum datagram size at start-up time, host authorization, etc.

8.5.1 PPP Components

The point-to-point protocol has the following components for transmitting datagrams over serial point-to-point links:

Encapsulating Datagrams: PPP uses the High-Level Data Link Control (HDLC) protocol as a mechanism for encapsulating datagrams over point-to-point links. The HDLC protocol defines the boundaries around the individual PPP frames and provides a 16-bit checksum. A PPP frame adds a protocol field to the basic HDLC frame to identify the type of packet carried by the frame so that it could enable to hold packets from protocols other than IP, such as Novell's IPX or Appletalk.

Implementing LCP: An extensible link control LCP is used to set up, configure and test the data-link connection. The LCP is implemented on top of HDLC to negotiate options pertaining to the data link.

Implementing NCP: A family of network control protocols (NCPs) are used for setting up and configuring different network-layer protocols like IP and AppleTalk, which are routed across the data link. They are configured dynamically using a corresponding NCP. Before transmitting IP datagrams across the link, both the hosts running PPP are required to negotiate the IP address being used by each of them. The control protocol used for such negotiation is known as the Internet protocol control protocol (IPCP).

In order to communicate over a point-to-point link, the PPP transmits LCP frames to configure the data-link so that a connection over a point-to-point link is set up. When the link is set up, the optional facilities are also negotiated which are essential for the LCP. Thereafter, the originating PPP transmits NCP frames to select and configure one or more network layer protocols. This leads to the transmission of packets from each network-layer protocol over the link. The link remains configured unless a LCP or NCP frames requests to close the link. Sometimes some external event also closes the link. In brief, communication over a point-to-point link is given as below:

- LCP frames from originating PPP first configure and test the data link for establishing a connection.
- Once the link is established, the originating PPP sends NCP frames for negotiating optional facilities and configuring one or more network layer protocols according to LCP.
- When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link will remain configured for communications until explicit LCP or NCP frames close the link, or until some external event occurs.

Caution PPP is capable of operating across any DTE/DCE interface like RS-232-C, RS-422, etc. However, the PPP requires duplex circuit for operation. They may be either dedicated or switched in asynchronous or synchronous mode.

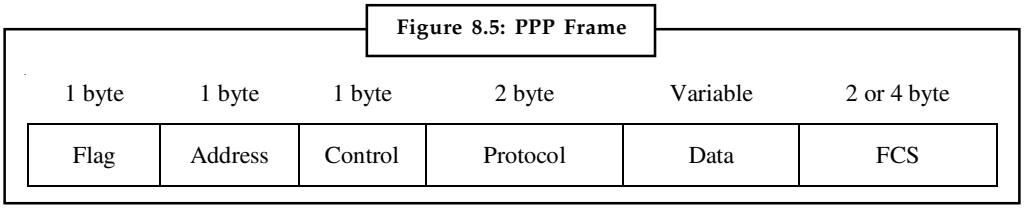
8.5.2 PPP Frame

There are six fields making up the PPP frame. These are given below and also diagrammatically represented in Figure 8.5.

Notes

- ***Flag:*** It is consisted of a single byte that indicates the beginning or end of a frame.
- ***Address:*** Address comprises of a single byte that contains the binary sequence. PPP does not assign individual station addresses.
- ***Control:*** It makes up of a single byte that contains the binary sequence, which calls for transmission of user data. It is a connectionless link service similar to that of Logical Link Control (LLC).
- ***Protocol:*** It is consisted of two bytes that identify the protocol encapsulated in the information field of the frame.
- ***Data:*** Data may range from zero or more bytes containing the datagram for the protocol specified in the protocol field. The default maximum length of the information field is 1,500 bytes. Closing flag sequence indicates the end of the information field with 2 bytes for the Frame Check Sequence (FCS) field.
- ***Frame Check Sequence (FCS):*** It has 2 bytes. In some case, it may also use 4-byte FCS for improved error detection but with prior agreement.

Figure 8.5: PPP Frame



PPP Link-Control Protocol (PPP LCP)

The protocols that differentiate PPP from HDLC are the Link Control Protocol (LCP) and the Network Control Protocol (NCP). LCP establishes, configures, maintains, and terminates point-to-point links. As we know by now that PPP LCPLCP provides a method of establishing, configuring, maintaining, and terminating the point-to-point connection for which it uses four steps. These are link establishment and configuration negotiation. A configuration-acknowledgment frame completes this step. Thereafter the quality of link is tested as to whether the link quality is sufficient to bring up network layer protocols. This phase is optional. After testing the link quality, network layer protocols can be configured separately by the appropriate NCP and can be brought up and taken down at any time. If LCP closes the link, it informs the network layer protocols so that they can take appropriate action. Finally, link termination takes place and LCP can terminate the link at any time. This usually is done at the request of a user but can happen because of a physical event, such as the loss of carrier or the expiration of an idle-period timer.

Did u know? Three classes of LCP frames exist. Link-establishment frames are used to establish and configure a link. Link-termination frames are used to terminate a link, and link-maintenance frames are used to manage and debug a link.

Point-to-Point Protocol Network Control Protocols (PPP NCP)

The Network Control Protocol (NCP) phase in the PPP link connection process is used for establishing and configuring different network-layer protocols such as IP, IPX or AppleTalk.

Once NCP has reached, PPP will carry the corresponding network-layer protocol packets. During this phase, link traffic consists of any possible combination of LCP, NCP, and network-layer

Notes

protocol packets. The IP-specific NCP protocol is the IP Control Protocol (IPCP). Aside from dealing with the calling peer's IP address, this protocol can also negotiate whether or not to use header compression, providing a significant speed improvement for low-speed links. If the calling peer has an IP address, it tells the called peer what it is; if the calling peer doesn't have an IP address, the called peer can assign the caller one from a pool of addresses.

8.6 Multiple Access Protocols

Traditional networks were point-to-point channels based on the dedicated channels for a pair of users. These channels due to their simplicity were not only economical but also used to provide transmission between a pair of nodes has no effect on the transmission between another pair of nodes even if they have a common node. The disadvantages of such channels were that they used to require fixed topology and enormous number of dedicated connections between a pair of channels thus imposing a challenge to design maintenance and cost effectiveness. Instead, broadcast channels began to use in which more than a single receiver can receive every transmitted message. The broadcast channels were good when a message is destined to a large number of destinations than a single or a very small number of destinations because it incurred wasteful processing results in all switches in which the message is not intended. The transmissions over a broadcast channel were also prone to interfere with another transmission. Thus, the transmission between a pair of nodes was no longer independent of other transmissions. To avoid such interference, a transmission control mechanism is required. Such transmission control mechanism known as multiple access protocol determines the access to shared channels in which allocation of shared resources are critical for desirable performance characteristics and proper operation of the network. These multiple access protocols are channel allocation schemes and they reside mostly in a special layer called the Medium Access Control (MAC) layer within the data link layer of the OSI model.

8.6.1 Multiple Access Protocols Classification

There are numerous multiple access protocols. One of them is non-centralized multiple access protocols in which all hosts perform based on the same rules and no single host is allowed to coordinate the activities of the others. This also does not include polling type access protocols. Broadly, they are classified as conflict free and contention protocols.

Conflict Free Protocols: They ensure successful transmission each time without interfering with another transmission. This further divided into static or dynamic conflict free protocols in which hosts communicate with channel allocation statically or dynamically.

Static Channel Allocation: The channel resources in static conflict free schemes depend on time, frequency or mixed time-frequency. The channels are divided based on the frequency range (bandwidth) to a single host for a fraction of the time as in time division multiple access (TDMA) or giving a fraction of the frequency range to every host all of the time as in frequency division multiple access (FDMA) or providing every host a portion of the bandwidth for a fraction of the time as in code division multiple access (CDMA).

Dynamic Channel Allocation: The dynamic channel allocation considers channel allocations based on demand so that optimum uses of channel may be ensured. The hosts who demand only little use of channel but keep the channel idle for most of the time within their allocated share in static allocation may leave the channel resources for more active hosts. It may further be classified into reservation and token passing scheme.

Reservation Scheme: The hosts first announce their intent to transmit in the dynamic channel allocation by various reservation schemes and reserve their right to transmit before new hosts obtain a chance to announce their intent to transmit.

Notes

Token Passing Scheme: A single token either in logical or physical form is circulated among the hosts for allowing the host to transmit who possesses the token so that interferences between transmissions of other hosts could b avoided.

Contention Schemes: Unlike the conflict free schemes, a transmitting host is not guaranteed to be successful in contention schemes. The protocol must be embedded with some resolution processes to resolve conflicts when they happen so all hosts could transmit successfully. The different resolution protocols build up the contention schemes. In contention schemes, idle hosts do not transmit and thus do not consume the channel resources.

Static Resolution: It refers to the right of the first host to transmit when a conflict happens. It is also based on probability in which the transmission schedule for the interfering hosts is chosen from a fixed distribution that is independent of the actual number of interfering hosts. Examples are Aloha type protocols and the various versions of Carrier Sense Multiple Access (CSMA) protocols.

Dynamic Resolution: It determines the highest priority or lowest priority to a packet based on the time of arrival in the system. The resolution can also be probabilistic. Some of the protocols based on this scheme are the multiplicity of the interfering packets and the exponential back-off scheme of the Ethernet.

8.6.2 Aloha and Slotted Aloha

Development of Aloha protocols in itself was a pioneer effort towards computer networking. It is also known as pure Aloha. It was developed by University of Hawaii in 1970 under the able expertise of Norman Abramson and Franklin Kuo for project sponsored by DARPA. It laid the foundation for the basis for the evolution of the Ethernet. Aloha network as developed with the aim of enabling people in different locations to access the main computer systems. Unlike ARPANET, Aloha network had used packet radio. Aloha network also initiated the concept of a shared medium for transmission. Aloha used same frequency for each node and therefore needs contention management. Aloha used to send data via a teletype in which the data rate usually did not go beyond 80 characters per second. In fact, Aloha network was a true network in which all of the computers were connected to Alohanet and they could send data at any time without operator intervention. It did not raise any limitation on number of computers to have been involved. It was possible as the medium used was a radio, which did not entail any fixed costs.

Aloha Protocols

The Aloha protocol works on OSI layer 2 for establishing LAN networks with broadcast domain. The first version of the protocol was basic:

- Whenever a user has a frame to send, it simply transmits the frame.
- If collision occurs, it waits for a random period of time and re-sends it again

Pure Aloha had about a 18.4% max throughput. This means that 81.6% of the total available bandwidth is basically being wasted due to stations trying to talk at the same time. In the Slotted Aloha protocol the throughput could be increased up to 36.8% with the provision that a station could not send anytime. It could send just at the beginning of a timeslot, and thus collisions are reduced. You should know that Slotted Aloha is not out of use today and it finds its usage on low bandwidth tactical satellite communications networks by the US Military. In order to mitigate the problem of contention, a number of ways were proposed. These are given below:

Frequency Multiplexing: In this case, each node are required to use a different radio frequency. However this would require each node added to able to be tuned in by all of the other machines.

Notes

Soon there would be hundreds of such frequencies, and radios capable of listening to this number of frequencies at the same time are very expensive.

Time Division Multiplexing: In this case, each node is given time slots for sending message. Unlike frequency multiplexing each node continue to have a single radio frequency. The disadvantage of this method lies in wastage of time when a node has nothing to send in its particular slot. This makes a node to wait long for sending data when there are several nodes.

Carrier Sense Multiple Access: In order to overcome the problem of empty time slots, Aloha devised carrier sense multiple access techniques which has now become the de facto standard. As you have already studies that this system has no fixed multiplexing at all. Instead each node listens to see if anyone else is using the channel, and if they don't hear anyone, they start talking. However, this techniques saved the time but was not foolproof as if first node started using the radio, then it might have it as long as it wanted and therefore left other nodes to wait indefinitely. This gave the birth of breaking down of the messages into small packets, and interlaced them in between the time slots of one node to other. This allowed other nodes to send out their packets in between, so everyone could share the medium at the same time. In order to avoid the collision problem when two nodes attempted to start their broadcast at the same time, Aloha protocol devised the technique of acknowledgement when sender could always find out if its frame was destroyed by listening to channel. For a LAN, feedback is immediate; while for a satellite there is a long delay of 270 ms before sender knows. In this case, after sending any packet the nodes listened to see if their own message was sent back to them by a central hub. If they got their message back, they could move on to their next packet. If not, it meant that some collision with another node's packet had prevented it to reach to the intended destination. This prompted them to send again after waiting for a random time. This collision avoidance system allowed any node to use the entire network's capability if no one else is using it.

Slotted Aloha

It uses small clock tick packets to allow intended nodes to send their packets immediately after receiving a clock tick. This protocol does improve the overall channel utilisation, by reducing the probability of collisions by a half. But this was not sufficient advantage and therefore further work on the same for wired networks by Bob Metcalfe improved collision avoidance on busy networks and established standards for Ethernet which is popularly known as CSMA/CD, carrier sense, multiple access, collision detection. In the previous unit this has been explained in quite detail.

Performance of Aloha or Slotted Aloha is determined with the help of throughput and average delay. Throughput is average number of frames successfully transmitted per unit time. A high value indicates a good performance. Poisson distribution can model frame transmission rate with mean arrival rate l frames/s. We can assume average frame length tf second then Normalized channel traffic or average number of old and new frames submitted per frame time is

$G = \lambda\tau_f$ Erlang

The throughput is then given by $S = G\lambda\tau_f$ (no collision)

Probability that a frame does not have a collision is given by

$P_0 = e^{-2G}$ for Aloha

$P_0 = e^{-G}$ for Slotted Aloha

The throughput/frame time is then given by

$S = G \times e^{-2G}$ for Aloha

Notes

$S = G \times e^{-G}$ for Slotted Aloha

Maximum throughput

$dS/dG = e^{-2G} - 2G \times e^{-2G} = 0$ then

$G_{Max} = ½$ and $S = ½ e^{-1} = 0.1839$ for Aloha

$dS/dG = e^{-G} - G \times e^{-G} = 0$ then

$G_{Max} = 1$ and $S = e^{-1} = 0.3679$ for Slotted Aloha

Managing Access to Networks

You may think if all the stations at a time begin to access network, there would be some sort of chaos. Therefore, there are many methods of managing access to a network. If all network stations tried to send data at once, the messages would become unintelligible, and no communication could occur. It necessitates to device mechanism to avoid such deadlocks. Some of important methods are listed below and discussed elsewhere in this study material:

- Carrier-Sense Multiple Access with Collision Detection (CSMA/CD)
- Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Token Passing
- Polling

Carrier Sense Multiple Access: In this case when a user wishes to transmit, he first listens to the medium to ensure whether another transmission is in progress or not. It is known as carrier sense. If the channel is in use, he must wait. If the medium is idle, he may transmit. If channel is busy, he has to wait for a random period of time before trying to listen. This has been explained in detail in other part of the tutorial.

CSMA with Collision Detection: If a user desires to transmit, he first listens to ensure whether the channel is free or not. If the channel is idle, he transmits. If the channel is busy, he keeps on listening until the channel is free, then transmits immediately. During the transmission, he continues listening to detect collision. If a collision is detected, he stops transmitting immediately, and waits a random period of time before goes back to step transmit again. Basically CSMA/CD has three states. These are transmission period, contention period and idle period. This also explained in other parts of this tutorial in detail.

Demand Priority: It uses services of intelligent hubs for controlling data transmission. A demand signal is issued to the hub indicating that it wants to transmit. Depending on circumstances, the hub responds with an acknowledgement that will allow the node to transmit. Likewise other nodes are allowed to transmit in turn.

Token Passing: As name signifies, it uses a token or series of bits to allow a node to transmit. The device after capturing token can transmit data into the network. When that particular node completes sending its data, the node passes the token along to the next node in the topology. Protocol specifications signifies how long a device may keep the token, how long it can transmit for and how to generate a new token if there is not one circulating.

Polling: This method uses a central controller to ensure the demands of nodes in polling order. Of so the central controller will allow them to transmit for a limited time, then the next device is polled.

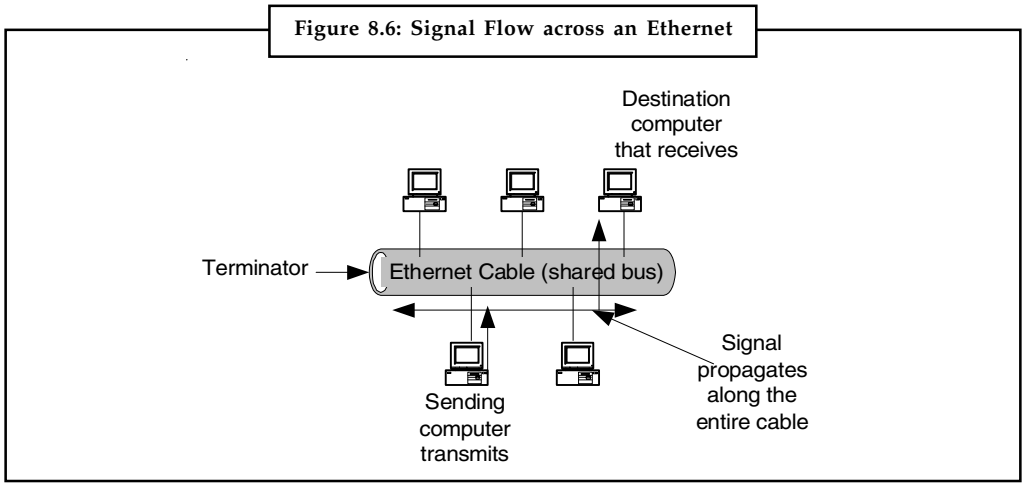
8.7 Ethernet Technologies

Notes

Among LAN standards, IEEE 802.3 Ethernet has become one of the most used LAN media. Its ample use and wide availability has made it one of the cheapest LAN media. Moreover, it can carry high-speed transmission. The evolution of Ethernet to such a widely accepted media may be traced back to late 1970s when the first Ethernet standard was created by Xerox. Around 1984, DIX (a consortium of Digital, Intel, and Xerox) and IEEE created standards for Ethernet which are popularly known as the IEEE 802.1. Subsequently, these groups segregated their work and worked as the Logical Link Control (LLC) Group focussing on end-to-end connectivity and came to be called the IEEE 802.2 Committee. Another group, called the Data Link and Medium Access Control (DLMAC) took the responsibility for developing medium access protocols. This group later formed committees for Ethernet (802.3), Token Bus (802.4), and Token Ring (802.5).

Ethernet is the least expensive high-speed LAN alternative. It transmits and receives data at a speed of 10 million bits per second. Data is transferred between wiring closets using either a heavy coaxial cable (thick net) or fibre optic cable. Thick net coaxial is still used for medium-long distances where medium levels of reliability are needed. Fibre goes a further distance and has greater reliability but a higher cost. To connect a number of workstations within the same room, a light duty coaxial cable called thin net is commonly used. These other media reflect an older view of workstation computers in a laboratory environment. Figure 8.6 shows the scheme of Ethernet where a sender transmits a modulated carrier wave that propagates from the sender toward both ends of the cable.

Figure 8.6: Signal Flow across an Ethernet



Ethernet was first designed and installed by Xerox Corporation at its Palo Atto Research Center (PARC) in the mid 1970. In 1980 DEC Intel and Xerox came out with a joint specification, which has become the de facto standard. Ethernet from this period is often called DIX after its corporate sponsors Digital, Intel, and Xerox.

Ethernet, which uses number devices such as hubs, switches and repeaters, has already been explained earlier. Ethernet IEEE 802.3. Here we will study implementation of LAN along with some associated key issues.

Collision and Broadcast Domains

Media access mechanism is a very important part of Ethernet technology and we will now understand collision and broadcast domains. Collision is nothing but the crashing of data when all devices or nodes on a single segment send data on the same physical wire. In case of a hub, all

Notes

the nodes connected to the hub are in the same collision domain. We may recall that hub is basically a repeater that re-sends any signal it receives out of each one of its ports and this signal is accessible to all nodes connected to the same hub. This explains why any message or signal sent by any node is treated as broadcast signal and therefore all nodes on the same hub are in same broadcast domain.

8.7.1 Ethernet Frame

This has also been explained in Section I in detail; however, a cursory look of the same is being presented here. There are three basic elements, which makes an Ethernet. These are physical medium, a set of medium access control rules, and the Ethernet frame. Ethernet takes packets from upper-layer protocols, and places header and footer information around the data before it traverses the network. This process is called data encapsulation or framing. Ethernet frames travel at the Data Link layer of the OSI model and must be a minimum of 64 bytes and a maximum of 1518 bytes. Figure 8.7 shows an Ethernet IEEE 802.3 frame and an Ethernet frame.

Figure 8.7 Ethernet IEEE 802.3 frame

7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46-1500 Bytes	4 Bytes
Preamble (P) 1010…10	SFD 10101011	SA	DA	Length Field		FCS

Below is a brief description of each field in an Ethernet IEEE 802.3 frame:

- ***Preamble (P):*** It is beginning of the frame and used to establish bit synchronization with the help of an alternating pattern of ones and zeros that is used by the receiver.
- ***SFD (Start Frame Delimiter):*** It lets the receiver know the beginning of the frame and contains one byte length.
- ***Destination Address (DA) and Source Address (SA):*** These are each six bytes long and are contained in hardware on the Ethernet interface card.
- ***Type Field:*** In Ethernet frames, this is the two-byte field after the source address. After Ethernet processing, the type field specifies the upper-layer protocol to receive the data.
- ***Length Field:*** It is a two-byte field following the source address. The length field indicates the number of bytes of data that follow this field and precede the frame check sequence field.
- ***Data Field:*** It is the place where the information to be transmitted is contained in the frame. It follows the type and length fields. After Physical-layer and Link-layer processes are complete, this data is sent to an upper-layer protocol. With Ethernet, the upper-layer protocol is identified in the type field. With IEEE 802.3, the upper-layer protocol must be defined within the data portion of the frame. If the data of the frame is not large enough to fill the frame to its minimum size of 64 bytes, padding bytes are inserted to ensure at least a 64-byte frame.
- ***FCS (Frame Check Sequence) or CRC (Cyclic Redundancy Check) fields*:** These are at the end of the frame. The frame check sequence recalculates the number of frames to make sure that none are missing or damaged. The CRC applies to all fields except the first, second, and last.

Notes

8.7.2 Fast Ethernet

100BaseT (Fast Ethernet)

100BaseT is a high-speed LAN standard and is considered a variation of 10BaseT. This is standardized as IEEE 802.3u. This operates with an access mechanism as CSMA/CD and provides a transmission speed of 100 Mbps through an Ethernet switching hub. Multiple 10 Mbps connections are supported through multiple ports on the switch. Cat 3, 4, or 5 UTP can be used in 4-pair configuration. Cat 5 UTP is generally used for a maximum LAN diameter of 500 meters. Three pairs are used for transmission, with the fourth pair used for signaling and control (CSMA/CD) in half-duplex mode. Connections to nodes, servers and other switching hubs are provided at 100 Mbps, supporting ten 10-Mbps channels. The 100 Mbps media include fiber (up to 30 miles or 50 Km without repeaters) and Cat 5 UTP at 100 meters.

Type of 100Base-T

The 100BaseT can be divided into 100BaseTX, 100BaseT4 and 100BaseFX, depending on the type of transmission media used as explained above. Two pair category 5 UTP, four pair category 3 UTP and optical fiber cable are used for 100BaseTX, 100BaseT4 and 100BaseFX respectively. This standard has been defined in IEEE802.3u.

Figure 8.8: Hardware Configuration of 100BaseTx

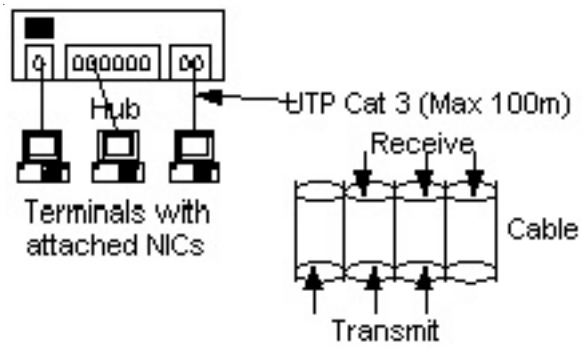


Figure 8.8 shows the hardware configuration of 100BaseTx. As with 100Baset, terminals are connected to the hub with 100BaseTx. Cat5 UTPs are used for connection. 100BaseTx has been developed based on 10BaseT to enable a higher transmission speed, vendors can readily develop peripheral equipment for 100BaseTx. Virtually all hubs and NICs for 100BaseTx can also be used for 10BaseT.

Figure 8.9 shows the hardware configuration of 100BaseT4. It is same as that for 100BaseTx. Cat3 UTPs are used for connection. Although originally intended for use as transmission lines at 10Mbps, cables of this type now offer a transmission speed of 100Mbps as a result of special arrangements., including improved signal processing and simultaneous use of three out of four pairs for transmission or reception. This enables the trouble free introduction of a 100Mbps LAN without the need to replace 10BaseT cables. However, these cables must be four pair cables.

Notes

Figure 8.9: Hardware Configuration of 100BaseT4

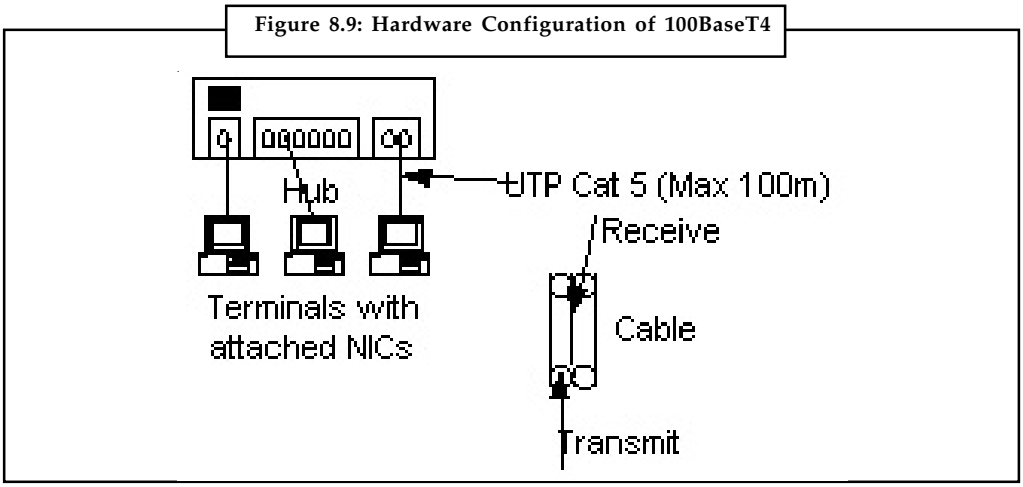
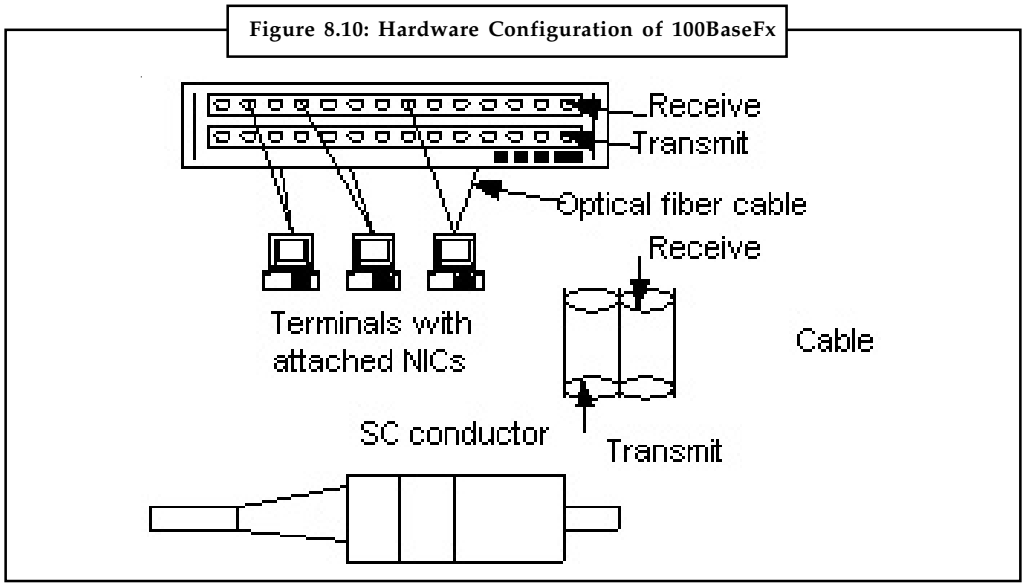


Figure 8.10 shows the hardware configuration of 100BaseFx. The SC connector that is a push-lock-type is recommended for use as an interface connector. However, some other connectors including the ST connector are also defined as options. Two fiber cables one for transmission and the other for reception are required for each connection.

Figure 8.10: Hardware Configuration of 100BaseFx

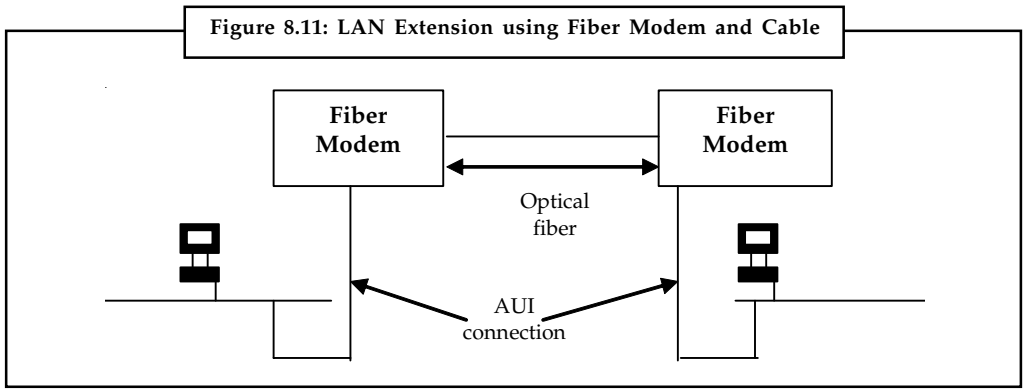


Fiber Optic Extensions

Fiber is a very flexible in nature and provides less attenuation and good immunity to noise. Optical fiber with fiber modem is used to extend a LAN beyond its limit. Figure 8.11 illustrates the concept of fiber modem to extend an Ethernet connection. A fiber modem is inserted between AUI and fiber optic cable at both the segments of Ethernet. This AUI connection may come directly from computer or transceiver depending upon the type of wiring being used. Fiber modems perform the conversion AUI signal to digital representation and light pulses, which can be sent along the fiber optic cable and vice versa. This mechanism can operate effectively for several kilometers. They are used widely to connect computers located in different buildings.

Notes

Figure 8.11: LAN Extension using Fiber Modem and Cable



Self Assessment

State whether the following statements are true or false:

8. Preamble is ending of the frame and used to establish bit synchronization with the help of an alternating pattern of ones and zeros that is used by the receiver.
9. Ethernet was first designed and installed by Xerox Corporation.
10. Performance of Aloha or Slotted Aloha is determined with the help of throughput and average delay.
11. Five classes of LCP frames exist.

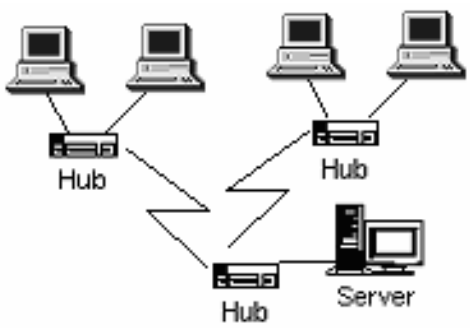
8.8 Wireless LAN

Wireless networks provide connectivity by using radio signal frequency to communicate among computers and other network devices and connection to the Internet anywhere in home or office. The wireless networks are known as WiFi network or WLAN. Wireless LAN (WLAN) enables hosts to communicate over short distances with the help of radio or infrared signal in place of traditional network cabling. A WLAN helps in extending an existing wired LAN like Ethernet by implementing access point to the edge of the wired network. The hosts connect to the Internet through access point using a wireless network adapter like Ethernet adapter. The wireless LAN adaptors also referred to as wireless NICs or wireless network cards are used in each device that wishes to connect on a wireless network. Generally, the wireless networks are built on wireless routers that act as base stations to provide a communication path through them and enabling nearby computers to connect to the Internet or to each other. Wireless routers perform like routers for wired networks. However, most wireless networks use a wireless router. To reduce the cost of the wireless networks, the wireless networks may be built without using routers. It is observed that no wireless hardware other than adapters is required to build a small wireless LAN (WLAN). However, wireless access points and/or wireless routers are used to increase the performance of a WLAN, accommodate more computers and increase the network's range. Access points that are provided as edge devices in wireless networks are alternative to routers and help in extending a wireless networks by joining it to an existing wired network. A single access point or router is considered to have sufficient range to span most homes but office buildings require multiple access points. Along with the routers or access points a wireless antenna is used to significantly increase the communication range of the wireless radio signal. The wireless network with wireless adapter encodes the binary data to radio frequency and wireless router transmits it. The reverse process takes place at the host computer. The wireless network set is comprised of a computer fitted with a low power radio

Notes

antenna, which is wirelessly connected to other hub antennas, computers, servers, peripherals and hosts via cabled connections. They also connect multiple hub antennas for transmission between rooms, floors and buildings. In order to serve multiple hosts, spread-spectrum radio technology is used to make effective use of limited bandwidth. Spread spectrum involves scattering of packets of a data stream across a range of frequencies, rather than using a single transmission frequency. A side benefit of spread-spectrum is of increased security, as the signal is virtually impossible to intercept. Some wireless LANs also use direct sequence transmission which means that a signal is sent simultaneously over several frequencies and therefore increasing its chances of getting through to the access hub. Figure 8.12 shows an example of wireless network block diagram.

Figure 8.12: Wireless LAN Configurations



The wireless network is becoming popular due to easy to setup feature and no cabling is involved. The computers can be connected anywhere in the home and office without the need for wires. Some of the features of wireless networks are given below:

- Wireless LANs are a relatively immature technology but becoming popular very fast.
- Acquisition costs are not particularly low when compared to wired LANs, although reconfiguration costs are virtually nonexistent.
- WLAN is mostly a mix of wire and wireless media having an access point or wireless router that is connected to a wired network via a coaxial cable, universal serial bus (USB) or Ethernet connection.
- Frequency range lies in 900 MHz, 2 GHz and 5 GHz bands.
- A hub antenna is located at a central point from where line-of-sight can be established with the various terminal antennae.
- Bandwidth of a wireless radio LAN is approximately 4 Mbps.
- The effective throughput is more in the range of 1 to 2 Mbps per hub.
- The infrared transmission technique can also be used. PDA (Personal Digital Assistant) make widespread use of infrared to establish links with hosts and other PDA for data transfer. Enhanced infrared technology recently has been demonstrated at speeds of 1.5, 4, and even 155 Mbps.
- Error performance and security are issues of some significance.
- IEEE 802.11a and IEEE 802.11b are wireless network standards with a data rate of only 2 Mbps and 11 Mbps respectively. They have a distance limitation up to 100 feet from the access point router. This uses 2.4 GHz band.
- IEEE 802.11g allows speeds up to 54 Mbps and continues to use the 2.4 GHz band.

Notes

The common devices that are used in wireless networks are:

Wireless Network Adaptor: A wireless network adapter is used to interface a computer to a network. The wireless adaptors are available as hardware devices like PCI Ethernet cards, PCMCIA devices, USB devices, etc. Some wireless network adapter devices for laptop computers are integrated circuit chips pre-installed inside the computer. A software device called device driver is used to communicate the network devices with the application software in different operating system environments. Virtual adaptors as simply software program are widely used in virtual private network (VPN).

Wireless Routers: The wireless routers are used to configure computers with wireless network adapters. They may also possess a network switch to enable some computers to be connected with Ethernet cables and share cable modem and DSL Internet connections. Some of the wireless routers also have built in firewalls to protect the network from intruders. They are available based on the wireless network protocols they support. The network protocols are 802.11g, 802.11a, 802.11b or a combination.

Wireless Access Points: They are configured nodes on wireless local area networks (WLANs) to act as a central transmitter and receiver of WLAN radio signals and to support WiFi wireless communication standards. The wireless access points (WAP) that are used in home or small business networks are generally small, dedicated hardware devices possessing features of a built-in network adapter, antenna and radio transmitter. However, small WLANs can function without access points. They find use in ad hoc or peer-to-peer mode, access points support infrastructure mode. The ad hoc infrastructures is used to bridge a WLAN with a wired Ethernet LAN so that it may be scaled up to support more hosts.

Wireless Range Extender: *A wireless range extender* is deployed to increases the distance over which a WLAN signal can spread. It thus improves the potential of signal to overcome obstacles and enhances overall wireless network signal quality. The wireless range expander is also known as range expanders or signal boosters and performs as a relay or network repeater by picking up and reflecting WiFi signals from a network's base router or access point.

Wireless Fidelity (WiFi)

WLAN are popularly known as the WiFi and operates on a family of 802.11 standards defined by IEEE. The 802.11b is considered the first standard in 802.11 to enjoy widespread popularity. However, the standards like 802.11a, 802.11b, 802.11g and 802.11n are available for WiFi. The WiFi Alliance examines the specifications of 802.11 products and certifies them to ensure compatibility with other products.

802.11: Refers to the generic name of a family of standards for wireless networking from the IEEE. They define rules for communication on wireless local area networks (WLANs) in terms of standards including 802.11a, 802.11b and 802.11g. The 802.11 that was developed around 1997, define WLANs to operate at 1-2 Mbps. It is not in use today.

802.11a: It is a WLAN communication standard that supports a maximum bandwidth of 54 Mbps with a radio signals in the frequency range above 5 GHz and provides improved performance and reduced interference over 802.11b standard but at the cost of significantly enhanced cost of access points and adapters. The 5 GHz frequency band of 802.11a limits the access point transmitter to send signal over a one fourth area of 802.11b access point transmitter. The frequency spectrum of 802.11a is regulated and dedicated to 802.11a devices only. Due to high frequency, walls and other obstructions also significantly reduced the performance of 802.11a wireless networks comparable 802.11b networks.

802.11b: It utilizes frequencies in the unregulated 2.4 GHz ranges, which may be allocated to other radio devices and therefore encounters much more radio interference from them. However,

Notes

the low cost of 802.11b devices have made them popular for smaller establishments like home, small offices, etc. They support a maximum data rate of 11 Mbps and are considered superior than dial-up. Compared to the performance of 802.11b and other standards of the same family, their performances are considered inferior.

802.11g: It came around 2003 to extend and improve the 802.11b standard. It is considered as the latest in the series of IEEE 802.11 standards for wireless LAN (WLAN) communications. The 802.11g compatible devices provide a maximum bandwidth of 54 Mbps and uses the same communication frequency range of 2.4 Ghz as 802.11b so that the 802.11b compatible devices may be used along with 802.11g devices.

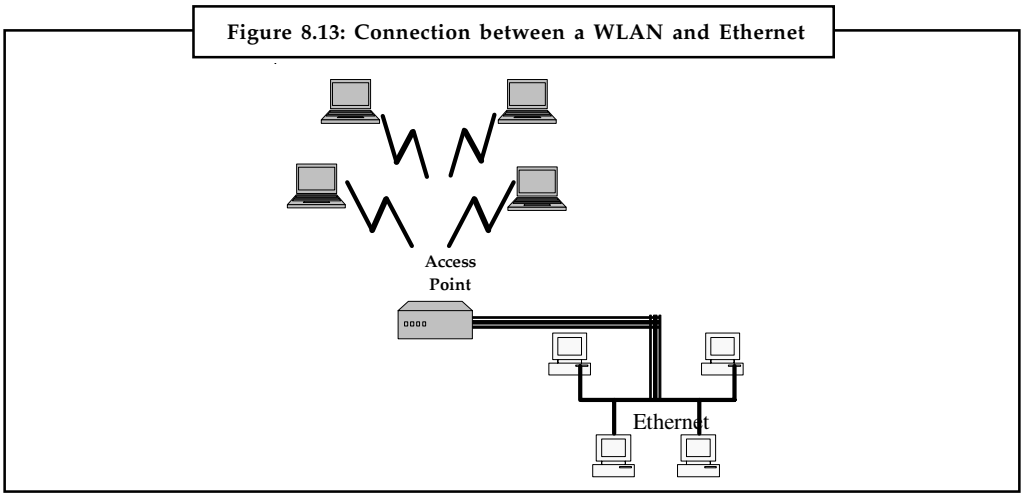
802.11n: It is an upcoming industry standard being developed for high-speed WiFi networking to replace the 802.11a, 802.11b and 802.11g WiFi standards with backward compatibility for local area networking. 802.11n intends to provide Multiple Input Multiple Output (MIMO) so that multiple simultaneous radio signals can be transmitted and received using multiple wireless antennas in tandem. This will lead to increase the range and throughput of a wireless network. The 802.11n standard is expected to support bandwidth greater than 100 Mbps.

Implementing WLAN

The WLANs, as of today, operate at much higher speeds ranging from 1 Mbps to 20 Mbps due to sharing of the spectrum by a much smaller number of hosts in a much smaller area up to a maximum radius of about a hundred meters. These factors lead to higher throughputs because smaller area and hosts cause less interference, distortion from the environment, reduced amount of error to the radio signal of WLAN. The higher throughput of WLAN makes it compatible with the existing network operating systems and applications like file and printer sharing, database access, etc.

The different topologies for implementing WLANs are spread spectrum including direct sequence and frequency hopping, low-power narrowband approach, HiperLAN and infrared LANs. The maximum reliable propagation range of the radio signals determines the physical size of a wireless network. The wireless networks are mostly used for temporary situations such as meetings, conferences, etc and therefore are of ad hoc nature and therefore referred to as ad-hoc networks, which connect, to an existing wired LAN. It is the access point at the edge of wireless network to bridge WLAN traffic onto wired LAN. Sometimes, this functionality is provided by software in a server computer that collocates both a WLAN card and a wired LAN card. However, in general, dedicated hardware as an access point device is used for this function. Figure 8.13 shows a bridging between WLAN and wired Ethernet.

Figure 8.13: Connection between a WLAN and Ethernet



Notes

Spread Spectrum: It is popular in WLAN and provides operation in a number of radio bands including 900 MHz, 2.4 GHz and 5 GHz. The wireless nodes are restricted to 1 watt of power for transmissions, which appear as noise to all except intended receivers because the nature of spread spectrum.

Low-Power Narrowband: It enables to transmit narrowband signals at low-power levels and is considered an alternative to spread spectrum technique that operates at high data rate. This approach operates at 10 Mbps in the 5 GHz band with 50 mw of peak transmission power with a reduced transmission range of 30 meters (100 feet) in a home or office environment.

HiperLAN: It stands for Higher Performance Radio LAN. It is a wireless technology standard developed by the European Telecommunications Standards Institute. It provides a data rate of about 24 Mbps using five channels each of them with a channel width of 23.5 MHz in 5 GHz band. Such throughput is capable of supporting multimedia applications.

Infrared LANs: It is considered an alternative approach to radio based WLANs. Infrared networking works on electromagnetic radiation with wavelengths of 820 to 890 nanometers equivalent to a frequency of about 350,000 GHz. The advantages of IR are that it does not require licenses and safety issues. Additionally, it provides huge potential capacity and good control of interference. The drawback of this technology is that it does not penetrate walls; so infrared WLANs are confined in a room only. They can also not perform well in outdoor areas in sunlight. The Infrared Data Association which is a consortium of manufacturers of IRDA devices is intending to provide low-cost IR communications characterized by directional point-to-point communications of up to one meter, 115-Kbps and 4-Mbps connectivity and walk up ad hoc connectivity for LAN access, printer access and portable computer to portable computer communications. Laptops are provided with IRDA ports.

Task List the various devices used in wireless networking along with their functionality.

8.9 Bluetooth

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions in the ISM band from 2400-2480 MHz) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Created by telecoms vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization.

Bluetooth is managed by the Bluetooth Special Interest Group, which has more than 14,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. The SIG oversees the development of the specification, manages the qualification program, and protects the trademarks. To be marketed as a Bluetooth device, it must be qualified to standards defined by the SIG. A network of patents are required to implement the technology and are only licensed to those qualifying devices; thus the protocol, whilst open, may be regarded as proprietary.

Bluetooth Implementation

Bluetooth uses a radio technology called frequency-hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 bands (1 MHz each; centered from 2402 to 2480 MHz) in the range 2,400-2,483.5 MHz (allowing for guard bands). This range is in the globally unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency band.

Notes

Originally Gaussian frequency-shift keying (GFSK) modulation was the only modulation scheme available; subsequently, since the introduction of Bluetooth 2.0+EDR, /4-DQPSK and 8DPSK modulation may also be used between compatible devices. Devices functioning with GFSK are said to be operating in basic rate (BR) mode where an instantaneous data rate of 1 Mbit/s is possible. The term Enhanced Data Rate (EDR) is used to describe /4-DPSK and 8DPSK schemes, each giving 2 and 3 Mbit/s respectively. The combination of these (BR and EDR) modes in Bluetooth radio technology is classified as a "BR/EDR radio".

Bluetooth is a packet-based protocol with a master-slave structure. One master may communicate with up to 7 slaves in a piconet; all devices share the master's clock. Packet exchange is based on the basic clock, defined by the master, which ticks at 312.5 µs intervals. Two clock ticks make up a slot of 625 µs; two slots make up a slot pair of 1250 µs. In the simple case of single-slot packets the master transmits in even slots and receives in odd slots; the slave, conversely, receives in even slots and transmits in odd slots. Packets may be 1, 3 or 5 slots long but in all cases the master transmit will begin in even slots and the slave transmit in odd slots.

Bluetooth provides a secure way to connect and exchange information between devices such as faxes, mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles.

Uses

Bluetooth is a standard wire-replacement communications protocol primarily designed for low power consumption, with a short range (power-class-dependent, but effective ranges vary in practice; see table below) based on low-cost transceiver microchips in each device. Because the devices use a radio (broadcast) communications system, they do not have to be in visual line of sight of each other, however a quasi optical wireless path must be viable.

Class (m)	Maximum permitted power (mW)	Range (dBm)
Class 1	100	20~100
Class 2	2.5	4~10
Class 3	1	0~5

The effective range varies due to propagation conditions, material coverage, production sample variations, antenna configurations and battery conditions. In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver, compared to a pure class 2 network. This is accomplished by the higher sensitivity and transmission power of class 1 devices.

While the Bluetooth Core Specification does mandate minimums for range, the range of the technology is application specific and is not limited. Manufacturers may tune their implementations to the range needed to support individual use cases.

8.10 Summary

- Stop and Wait protocol is easiest to implement and proves to be the most efficient on an error free communication channel. However, an error free communication channel is practically not possible.
- PAR is also reliable and easy to implement but at the cost of the loss in bandwidth.
- Go Back N protocol needs buffer maintenance and therefore, is complicated to keep source and destination machines in synchronization. It is also considered the most inefficient because it retransmits all subsequent frames on the loss of a frame and thus incurs huge wastage of bandwidth.

Notes

- Selective Repeat is an improvement on Go Back N protocol and tries for more efficient use of bandwidth by reducing the number of retransmissions because it retransmits only one frame instead of the entire series. Thus, Selective Repeat is considered a better choice.
- Finite State Machine model is a technique to verify the correctness of the protocol. PPP and HDLC are widely used data link protocols.
- Wireless technology has helped to simplify networking by enabling multiple computer users to simultaneously share resources in a home or business without additional or intrusive wiring. These resources might include a broadband Internet connection, network printers, data files, and even streaming audio and video. This kind of resource sharing has become more prevalent as computer users have changed their habits from using single, stand-alone computers to working on networks with multiple computers, each with potentially different operating systems and varying peripheral hardware.
- Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions in the ISM band from 2400-2480 MHz) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security.

8.11 Keywords

Bluetooth: Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions in the ISM band from 2400-2480 MHz) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security

Point-to-Point Protocol (PPP): It is a data link layer protocol and operates over a point-to-point link that connects two communicating link-level peers at each end of the link.

Positive Acknowledgement with Retransmission Protocol (PAR): The protocol is able to handle congestion, lost frames and damaged frames because frames are retransmitted until a positive acknowledgement is received.

Protocol Verification: Protocols are verified either during the design phase before implementation of the system or during the testing and simulation phase after implementation of the system.

Selective Repeat: Provides buffers at source and destination hosts to enable the source node to have more than one outstanding frame at a time and destination node to accept out of order frames and store them in its window.

Simplex Stop and Wait: After transmission, the source node waits for an acknowledgement from the destination node. After receiving, the acknowledgement, the loop starts over again.

8.12 Review Questions

1. What is the data link protocol?
2. What advantages does Selective Repeat sliding window protocol offer over Go Back N protocol?
3. What is the purpose of flow control?
4. Describe how does finite state machine model carry out protocol verification.
5. What are different data link protocols available? Why does PPP have become popular?
6. How does the data link layer accomplish the transmission of data from the source network layer to the destination network layer?

Notes

7. How are frames created and checksums applied on them?
8. How does the data link layer handle errors and lost frames due to some hardware problem?
9. Why is Hamming code considered important among various error detection and recovery techniques?
10. What procedure is used to prevent a stream of binary data from being misinterpreted as a HDLC flag?
11. Explain any three techniques by which frame boundaries may be encoded within a transmitted bit stream. Describe character stuffing and state which technique it is associated with and why it is needed.
12. How does pipelining improve data link layer protocol throughput?
13. The IEEE has split the data link layer in LANs such as Ethernet and Token ring into two sub layers. Which of these layers deals with error detection?
14. How does PPP transmit datagrams over serial point-to-point links?
15. How does PPP establish link for authenticated transfer of file?
16. What are different methods of authentication adopted in PPP technique?
17. How can a collision be avoided in CSMA/CD network?
18. Compare and contrast CSMA/CD and token passing access methods.
19. Is Slotted Aloha always better than Aloha? Explain your answer with justification.
20. What are the basic components, which constitutes an Ethernet?
21. On what basis is Ethernet versions defined? List them.
22. What are the different frequencies and data rates available for wireless LAN?
23. What are the technologies available for Wireless LAN?

Answers: Self Assessment

1. Data link layer
2. Unacknowledged connectionless service
3. Framing
4. Rate of data transmission
5. nil
6. a sequence number
7. one outstanding frame
8. False
9. True
10. True
11. False

8.13 Further Readings

Books

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall.

Behrouz A. Forouzan and Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies.

J. D. Spragins, *Telecommunications Protocols and Design*, Addison-Wesley.

Unit 9: Network Layer

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss Network layer design issues along with connection oriented and connectionless services
- Describe various concepts of routing algorithm with comprehensions of adoptive and non-adoptive algorithms
- Understand the routing protocols for internal and external networks

Introduction

The network layer deals with forwarding packets from the source node to the destination node using different routes. Hence, the network layer transports traffic between devices that are not locally attached. In doing so, it controls the operation of the subnet, which involves routing of the packets from the source to destination. Routes are based on static or dynamic routing tables. The destination IP address is checked for packet received on a router interface. If the packet is not addressed for the router where it is received, the router will look up the destination network address in the routing table so that it may be routed accordingly. Therefore, the network layer must know about the topology of the communication subnet and choose appropriate paths through it. The routes are chosen in such a manner so that the network layer avoids overloading some of the communication lines while leaving others idle. The routing algorithm is part of the network layer. The routing algorithm enables the network layer to decide to which output line an incoming packet should be forwarded. Routing algorithms provides correctness, simplicity, robustness, stability, fairness and optimality. All these functions of network layer differ from the data link layer whose objective is to transmit the bits from one end of a wire to the other end. The Network layer is the lowest layer that deals with end-to-end transmission.

Notes

9.1 Network Layer Design Issues

The network layer design issues include the service provided to the transport layer, routing of packets through the subnet, congestion control, and connection of multiple networks together, etc. The design issues of network layer are given as below:

- It is the purpose of network layer to provide seamless services to different users connected to different networks, therefore, the services provided should be independent of the underlying technology. In other words, users availing the service need not to bother of the physical implementation of the network for transmitting their messages. It should be able to provide interoperability among variety of networks in operation and provided by different vendors. Hence, the design of the layer should not restrict the uses from connecting to networks of different technologies.
- The transport layer at the host machine should not need to know as to how the communication link with destination machine is established. Hence, it should be shielded from the number, type and different topologies of the subnets that it uses.
- There should be some uniform addressing scheme for network addresses.

There are two different types of communication links. They are connection oriented and connectionless.

Connection Oriented Services: In connection-oriented service, each packet is associated with a source/destination connection. These packets are routed along the same path, known as a virtual circuit. Thus, it provides end-to-end connection to the user for reliable data transfer. It delivers data in order without duplication or missing data and therefore, does not congest the communication channel and the buffer of the receiving machine. The host machine requests a connection to communicate and closes the connection after transmission of the data. A telephone communication is an example of a connection-oriented service. In the connection-oriented service, the user engages the bandwidth and other resources of the network for duration of the connection and therefore bound to pay more. This service also keeps network resources engaged even when there is no communication during the connection. It is found to be efficient to send a constant stream of data down the line. If user wishes to send only a packet or two of data, then the cost of setting up the connection is enormously high and most of the time the line will remain idle and wasting bandwidth and resources of the network. Apparently, connection-oriented services are useful when the user has a constant stream of data to transmit.

Connectionless Service: In connectionless service, a router treats each packet individually. The packets are routed through different paths through the network according to the decisions made by routers. In connectionless service, the network or communication channel does not guarantee delivery of data from host machine to destination machine. The data to be transmitted is broken into packets. These independent packets are called datagrams in analogy with telegrams. The packets contain the address of the destination machine. A connectionless service is equivalent to the postal system. In postal system, a letter is put in an envelope that contains the address of the destination. It is then put in a letterbox. The letter finally delivers at the destination through postal network. However, it does not guarantee to arrive at the addressee's letterbox. Similarly, in connectionless service packets of data containing address are transmitted with a hope that it will finally reach to the destination after bouncing forth and back in the communication network. The connectionless service as compared to connection-oriented services appears to offer a drawback in terms of unreliable delivery of data but the probability of loss of packet is quite low. Many applications have their own error detection, flow and congestion control mechanism at a higher level of layers in the protocol stack i.e. transport layer at either host or destination machine or at both ends.

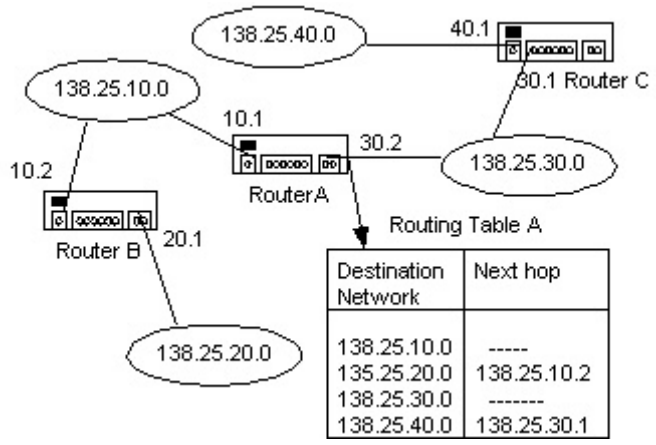
Notes

Task Differentiate between connection oriented and connectionless service.

9.2 Routing

The routing algorithm that runs on the network layer decides which output line an incoming packet should be transmitted on. A routing table that is built in every router tells which outgoing line should be used for each possible destination router. A router looks up the outgoing communication line to use in the routing table after receiving a datagram that contains the destination address. Thereafter, it sends the packet on its way to the destination. Thus, the major role of the network layer is to routing the packets from source to destination machine. The algorithms that enable to choose the possible routes and the data structures that they use are a major area of routing algorithm. The desirable properties of the routing algorithms are correctness, simplicity, robustness, stability, fairness and optimality.

Figure 9.1: Routing Table



Hence, the routing algorithm is defined as the part of the network layer software deciding which output line an incoming packet should be transmitted on. It all depends upon if the subnet uses datagrams internally, this decision is made a new for every arriving data packet since the best route may have changed since last time. If the subnet using virtual circuits such decision is made ones per session.

Figure 9.1 shows the routing table for router A (address 138.25.10.1). This table lists destination addresses for each local network, and not for each destination host. This table also includes as the next hop (the address of next router) to which the packet must be transferred. If no hops are included, this means that the destination network is directly connected to the router.

When router A receives a packet, it tracks this table to perform routing. For example, if the packets addressed to the host of network 138.25.40.0, then router A sends the packet to router C (138.25.30.1). Router C has a similar routing table so that it can perform routing.

Routing plays a major role in the forwarding function.

Next hop routing: A router is used to determine the route of datagrams based on its internal routing table. The table contains entries indicating to which router datagrams should be transmitted to reach a particular network. The router receives datagrams from different sources. The role of the router to check the IP address of the destination and determine what the next hop would be much

Notes

closer to its final destination to which the datagram should be sent. To determine the next hop, the routers maintain a set of information to enable mapping between different networks IDs and the other routers to which it is connected. This information is contained in a data structure known as routing table. The entries in the routing table facilitate details of subnetwork or host. Thus, when a router receives a datagram, it examines the destination IP address of datagram against the routing entries in its table to determine where to send the datagram, and then sends it on its next hop. The next hop is a technique to enable router to take fast decision what to do with datagrams due to the fewer the entries in this table. The classless inter domain routing (CIDR) aggregates routes into supernets to reduce router table size. In brief the next hop routing is the technique to simply reduce the contents of a routing table, which holds information that leads to the next hop instead of holding information about the complete route.

Network specific routing: The network specific routing is also a technique to reduce the routing table and simplify the searching process. As the name implies, this technique allows one entry only to define the address of the network itself to which many hosts are connected. Thus, the network specific routing does not involve an entry for each and every host connected to the same physical network and treat all hosts connected to same network as one single entity. For example, if there are 500 hosts attached to the same network, only one entry exists in the routing table instead of 500 entries.

Host specific routing: It is considered inverse of network-specific routing in which each destination host addresses are given in the routing table. Thus it is not as fast as next hop and network specific routing, however network administrator has greater control over routing.

Default routing: It is another technique to simplify routing in which a host is connected to two routers in a network. One router is used to route the packets to the host connected to another network and for the rest of the Internet another router is used.

Routing are grouped into two classes. They are non-adaptive and adaptive algorithms.

Non-adaptive algorithms or static routing are independent of the volume of the current traffic and topology. They decide the route to which a datagram is to sent off-line. The route is computed in advance and downloaded to the routers when the network is booted. Thus, routing information is manually specified. It provides fixed route information to each router. If there is no change in route, it is made manually. This procedure is also called static routing.

Adaptive algorithms or dynamic routing are capable of changing their routing decisions to reflect changes in the topology and the traffic. Routers automatically update routing information when changes are made to the network configuration. It is convenient, as it does not involve human intervention in case of changes to the network configuration. Its disadvantage, however, is that the overhead required to send configuration change information can be a heavy burden. They are also known as dynamic routing. To update information in the routing table, it uses one of the dynamic routing protocol such as OSPF or BGP or etc.

9.2.1 Routing Table

Each router on the network maintains a routing table in memory that may be simple or complex. In the simplest form the table is consisted pairs of IP addresses. When the originating station concludes that the intended destination is, itself, directly reachable, the frame is sent directly to the destination IP address in the frame. However, it may not be necessary to send it to a router if the sender finds that it is on the same subnetwork as the destination. When the masked destination address is compared against the available entries in the table and it is found that the routing table does not possess any matching lookup value. In such a situation, a special address appears in the routing table called the Default Gateway Address. The routing decisions are based on the following points:

Notes

1. The destination IP address and router IP are masked to determine if the incoming packet is to be forwarded to another network or not. If the results are the same, it indicates that a packet is for the same subnet as the destination. The frame is then forwarded directly to the data link address of the destination.
2. When the result is not same, it indicates that the destination is not on the same subnet. The routing table is checked to find out if the exact, complete, 32-bit destination address is specified which is referred to as a host specific routing. If host specific route is specified, the frame is transmitted to the IP destination indicated in the table that implies that this destination is the next router in line on the way to the destination.
3. When host specific route is not found in the routing table then the masked address is used to lookup key in the routing table to examine whether the network/subnetwork is specified in the table. If it is specified, the frame is sent to the IP address specified in the table that implies that this is the IP address of the next router in line.
4. When both the conditions 2 and 3 given above fail, the frame is forwarded to the address specified as the target for the Default Gateway.
5. In a situation when no default gateway is specified, it is assumed that all unspecified destinations are directly reachable. The physical address of the destination IP station is resolved and the frame is forwarded directly to the destination. This is sometimes called as activating Proxy ARP.

It is evident from the above that routing table requires at least four entries like mask, destination address, next hop address and interface.

Self Assessment

State whether the following statements are true or false:

1. The routing algorithm enables the network layer to decide to which output line an incoming packet should be forwarded.
2. There are three different types of communication links.
3. Connection-oriented services are useful when the user has a constant stream of data to transmit.
4. A connection-oriented service is equivalent to the postal system.
5. In connection-oriented service, the packets are routed along the same path, known as a virtual circuit.

9.3 Routing Protocols

Routers are used to connect different networks, determine which path it should take and forward IP traffic. These informations are obtained at routers by performing per-packet processing in which IP header of the packet is checked to make routing decisions based on destination IP address and the current state of the network connectivity. The network connectivity and routing information is constantly maintained by the router to accurately forward the packets. The packet is eventually passed though many routers before reaching to the destination. The routing table at each router in the way of a packet reaching to its indented destination specifies the optimum path for the packet. The optimality principle defines that if router A is on the optimal path from router B to router C, then the optimal path from A to C also falls along the same route. Consequently, the set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such tree is called a sink tree. The routing table may be either static or

Notes

dynamic. The static table does not alter frequently while dynamic table is updated frequently whenever some change in the Internet is advertised like failure of some route or addition of a better route. Routing protocols are used for dynamic routing tables. They are based on combination of rules and procedures that enable routers to inform each other about the changes in the Internet and share the information about the Internet or their neighborhood.

Unicast Routing

The majority of IP addresses are unicast addresses that are meant for a single recipient. Unicast connections are one-to-one connections. A connectionless and connection oriented protocol can use unicast addresses irrespective of whether connection exists between a specific pair of hosts. In unicast routing the router forwards the incoming packet through one of its port as defined in the routing table. A router that is attached to several networks has to determine the optimal path for a packet so that a router chooses the route with the shortest metric. Metric is defined as the cost assigned for passing through a network. The total metric for a particular route is the sum of the metrics of the network that build up the route. The metric assigned to each network depends upon the protocol used. The unit of metric cost is hop count and protocol like routing information protocol assigns equal metric to each networks. If it assigns a metric of 1 hop to each network then a packet traversing 15 networks will have metric value as 15 hop count. The assignment of metric varies from protocols to protocols based on the services required from the network.

Interior and Exterior Routing

An Internet is divided into autonomous systems so that routing protocols may handle Internet effectively and efficiently. An autonomous system (AS) is a group of networks under the administration of a single authority and therefore routing inside an AS is called as interior routing while routing among autonomous systems is called exterior routing. There exist many standard and proprietary interior gateway protocols. Some of them are Routing Information Protocol (RIP) and Open Shortest Path Fist (OSPF). The exterior protocol is Border Gateway Protocol (BGP).

Hierarchical Routing

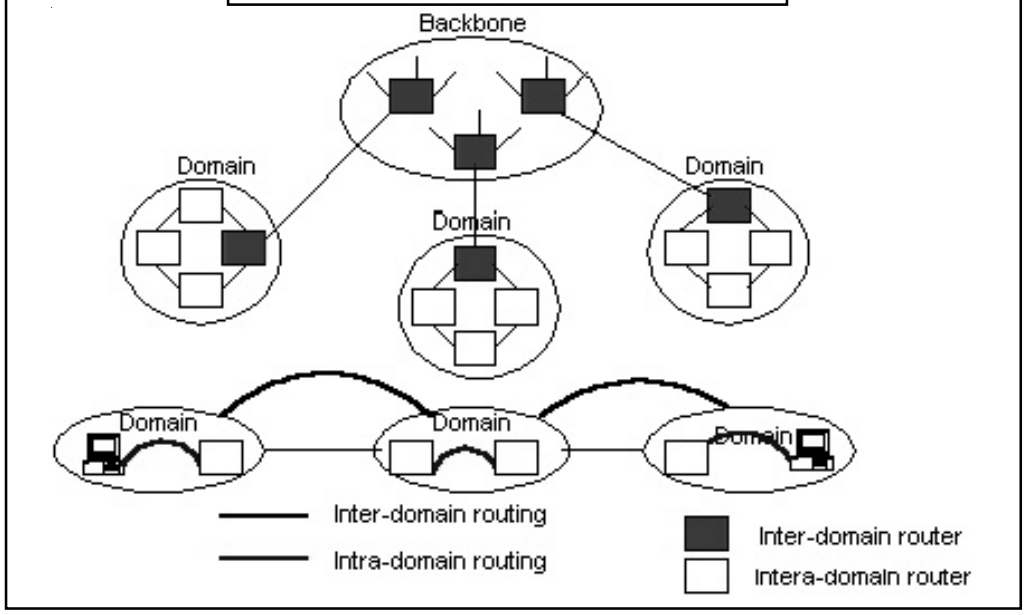
Because of the global nature of Internet system and ever growing networks in size, it becomes more difficult to centralize the system management and operation. For this reason, the system must be hierarchical such that it is organized into multiple levels, with several group loops connected with one another at each level. The routers are divided into regions with each router knowing all the details about how to route packets within its own region but knowing nothing about the internal structure of other regions. Therefore, hierarchical routing is commonly used for such a system as shown in the Figure 9.2.

- A set of networks interconnected by routers within a specific area using the same routing protocol is called domain.
- Two or more domains may be further combined to form a higher-order domain.
- A router within a specific domain is called intra-domain router. A router connecting domains is called inter-domain router.
- A network composed of inter-domain routers is called backbone.

Each domain, which is also called operation domain, is a point where the system operation is divided into plural organizations in charge of operation. Domains are determined according to the territory occupied by each organization.

Notes

Figure 9.2: Hierarchical Routing



Routing protocol in such an Internet system can be broadly divided into two types:

- Intra-domain routing
- Inter-domain routing.

Notes Each of these protocols is hierarchically organized. For communication within a domain, only the former routing is used. However, both of them are used for communication between two or more domains.

Two algorithms, Distance-Vector Protocol and Link-State Protocol, are available to update contents of routing tables.

RIP

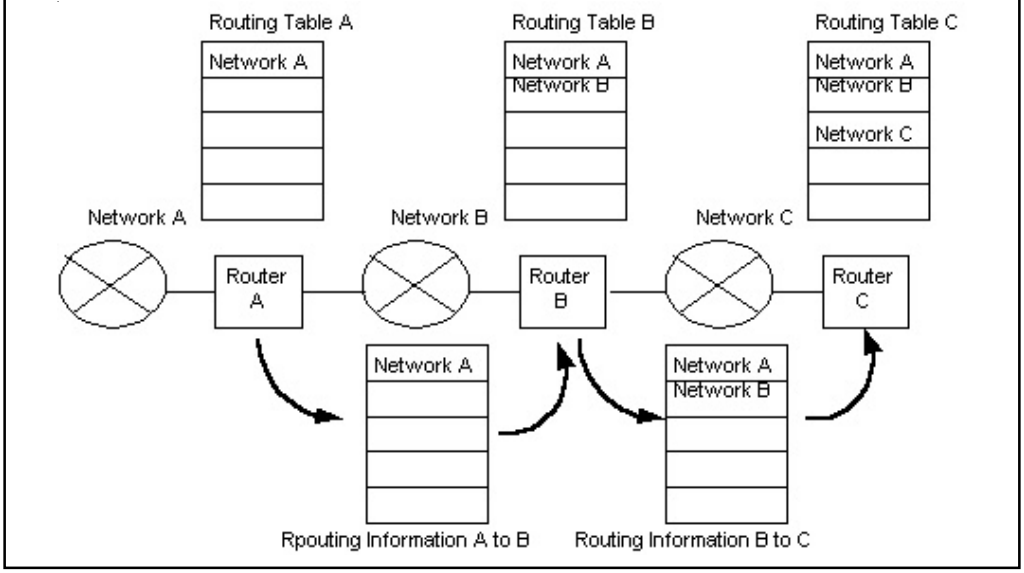
It is a simple protocol based on the distance vector routing which uses the Bellman Ford algorithm for calculating the routing tables.

Distance Vector Routing

Distance Vector Routing comes under the category of dynamic routing. Modern computer networks believe in dynamic routing algorithms as compared to static routing algorithms. This routing algorithm along with link state routing is the popular. Distance vector protocols are RIP, Interior Gateway Routing Protocol (IGPR). In distance vector algorithm each router maintains a routing table and exchanges its routing table with each of its neighbors so that their routing tables get updated. Each router will then merge the received routing tables with its own table, and then transmit the merged table to its neighbors. This is shown in Figure 9.3. This occurs dynamically after a fixed time interval by default, thus requiring significant link overhead.

Notes

Figure 9.3: Routing Method-Distance - Vector Type



There are problems, however, such as:

(1) If exchanging data among routers every 90 seconds, for example, it takes 90 × 10 seconds that a router detects a problem in a router 10 routers ahead and the route cannot be changed during this period.

(2) Traffic increases since routing information is continually exchanged.

(3) There is a limit to the maximum amount of routing information (15 for RIP), and routing is not possible on networks where the number of hops exceeds this maximum.

(4) Metric cost data is only the number of hops, and so selecting the best path is difficult.

However, routing processing is simple, and it is used in small-scale networks in which the points mentioned above are not a problem. Distance vector routing was used in the ARPANET routing algorithm and was also used in the Internet under the name RIP. It also found its uses in early versions of DECnet and Novell's IPX. AppleTalk and CISCO routers use improved version of distance vector protocols. In the improved version, each router has a routing table indexed by and containing one entry for each router in the subnet. This entry has two parts. They are the preferred outgoing line to use for destination and an estimate of the time or distance to destination. The metric used is number of hops, time delay in milliseconds and total number of packets queued along the path or something similar.

Link State Routing

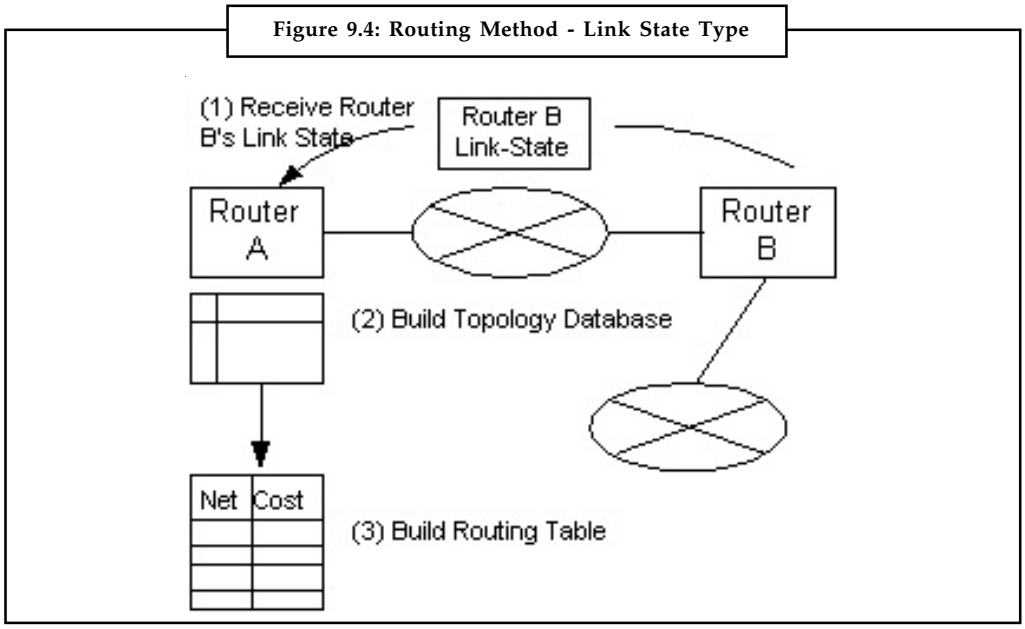
The link state routing is simple. Link state routing algorithm in which each router in the network learns the network topology then creates a routing table based on this topology. Each router will send information of its links (Link-State) to its neighbor who will in turn propagate the information to its neighbors, etc. This occurs until all routers have built a topology of the network. Each router will then prune the topology, with itself as the root, choosing the least-cost-path to each router. Thereafter, they build a routing table based on the pruned topology as shown in Figure 9.4.

The entire topology and delays are measured and distributed to every router. Then Dijkstra's algorithm is used to find the shortest path to every other router.

Notes

Did u know? In link-state protocols, there are no restrictions in number of hops as in distance-vector protocols, and these are aimed at relatively large networks such as Internet backbones. The load on routers will be large however, since processing is complex.

Figure 9.4: Routing Method - Link State Type



Dijkstra Algorithm: It calculates the shortest path between two points on network. The Dijkstra graph is consisted of nodes and arches and nodes. It first selects a node tentatively. The algorithm checks the tentative node against certain criteria to declare it as permanent node. The algorithm starts with the roots of the tree, which is the local router and termed as local node. This node is declared as permanent node and assigned a cost of 0. Thereafter, each neighbor node of this node is examined to declare it last permanent node. And this node is assigned a cumulative cost .

Briefly, the link state routing deals with:

- discovering its neighbor and learn their network addresses,
- measuring the delay or cost to each of its neighbors,
- constructing a packet indicating all it has just learned,
- sending this packet to all other routers for their learning and
- computing the shortest path to every other router.

Self Assessment

Fill in the blanks:

6. Distance Vector Routing comes under the category of …… routing.
7. Dijkstra's algorithm is used to find the …….. path to every other router.
8. …….. a simple protocol based on the distance vector routing which uses the Bellman Ford algorithm.
9. Routing protocol in such an Internet system can be broadly divided into ……. types.
10. Routing inside an AS is called as …… routing.

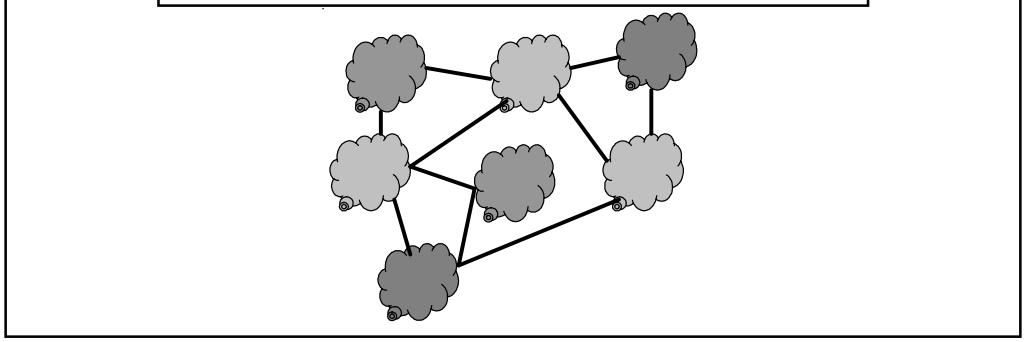
Notes

9.4 Internetworking

The availability of different operating systems, hardware platforms and the geographical dispersion of computing resources necessitated the need of networking in such a manner that computers of all sizes could communicate with each other, regardless of the vendor, the operating system, the hardware platform, or geographical proximity. Therefore, we may say that internetworking is a scheme for interconnecting multiple networks of dissimilar technologies. Some of the factors that make networks differ are frame, packet, and message size, checksum algorithms, maximum packet lifetimes, connection-oriented vs. connectionless protocols, timer values, etc. When all routers in a network have same protocols then the network is called homogeneous. When these homogeneous networks are interconnected, it results in an internetwork. There may be instances, when the routers of different networks use different protocols such as Internet Protocol (IP), Systems Network Architecture (SNA), Asynchronous Transfer Mode (ATM), Novel NCP/IPX and AppleTalk are some. Wireless ad-hoc and mobile networks using e.g. Bluetooth are others. Hence, to interconnect multiple networks of dissimilar technologies use of both additional hardware and software is needed. This additional hardware is positioned between networks and software on each attached computer. This system of interconnected networks is called an internetwork or an Internet.

An Example Internetwork

Figure 9.5: Internetworking of Different Homogeneous Networks



* Shades represents homogeneous networks of different types

To develop standards for internetworking, Defense Advanced Research Projects Agency (DARPA) funded research projects. ARPAnet, a project of DARPA, introduced the world of networking with protocol suite concepts such as layering, well before ISO's initiative in this direction. DARPA continued its research for an internetworking protocol suite. This may be seen in the early NCP (Network Control Program) host-to-host protocol to the TCP/IP protocol suite, which took its current form around 1978. DARPA was well known for its pioneering of packet switching over radio networks and satellite channels and ARPAnet was declared an operational network with responsibility of administering it to Defense Communications Agency (DCA) in 1975. TCP/IP had not yet been developed.

ARPAnet was basically a network based on leased lines connected by special switching nodes, known as Internet Message Processors (IMP). Many researchers were involved in TCP/IP research by 1979. This motivated DARPA to form an informal committee to coordinate and guide the design of the communication protocols and architecture. The committee was called the Internet Control and Configuration Board (ICCB).

The first real implementation of the Internet was when DARPA converted the machines of its research network ARPAnet to use the new TCP/IP protocols. After this transition, which started in 1980 and finished in 1983, DARPA demanded that all computers willing to connect to its

Notes

ARPAnet must use TCP/IP. The US military adopted TCP/IP as standard protocol in 1983 and recommended that all networks connected to the ARPAnet conform to the new standards.

The success of ARPAnet was more than the expectations of its own founders and TCP/IP internetworking became widespread. As a result, new wide area networks (WAN) were created in the USA and connected to ARPAnet using TCP/IP protocol. In turn, other networks in the rest of the world, not necessarily based on the TCP/IP protocols, were added to the set of interconnected networks. Computing facilities all over North America, Europe, Japan, and other parts of the world are currently connected to the Internet via their own sub-networks, constituting the world's largest network. In 1990, ARPAnet was eliminated, and the Internet was declared as the formal global network.

DARPA also funded a project to develop TCP/IP protocols for Berkeley UNIX on the VAX and to distribute the developed codes free of charge with their UNIX operating system. The first release of the Berkeley Software Distribution (BSD) to include the TCP/IP protocol set was made available in 1983 (4.2BSD). This led to the spread of TCP/IP among universities and research centers and has become the standard communications subsystem for all UNIX connectivity. There are many updated versions of BSD code available. These are 4.3BSD (1986), 4.3BSD Tahoe (1988), 4.3BSD Reno (1990) and 4.4BSD (1993).

9.5 Summary

- The main role of the network layer is to accept packets from a source and deliver them to a destination machine. The network layer provides services that should be independent of the router technology. It shields the transport layer from the router network details and facilitates, network addressing to be consistent across networks.
- Services of the network layer are available in connection oriented and connectionless modes. Connection-oriented services are useful only when the user wants to send a constant stream of data down the line.
- The routing algorithms that require selecting a path or route from many possible routes in the network are part of the router software. They are of two basic types namely non-adaptive or static and dynamic or adaptive. Selection of routing algorithms depends on the minimum mean delay for the packets and number of hop before reaching to the destination machine.
- Link State Routing attempts to discover its neighbor and learn their network addresses and enable the router to choose a shortest path. The hierarchal routing uses multiple groups to route the packets. Broadcast and multicast routings are used to forward a single packet to several recipients depending on whether they belong to broadcast or multicast group.
- The shortest path to each destination within the network is found by traversing the tree and the most common shortest path first algorithm is the Dijkstra algorithm.
- The distance vector algorithms is used to determine which path is the best path to each destination based on the advertised details about the path and distance for each destination which is maintained in a local database.

9.6 Keywords

Adaptive Algorithms: They are capable of changing their routing decisions to reflect changes in the topology and the traffic and automatically update routing information when changes are made to the network configuration.

Notes

Distance Vector Routing: It maintains a routing table and exchanges its routing table with each of its neighbors so that their routing tables get updated.

Flow-based Routing: It takes into account the topology as well as the load.

Hierarchical Routing: It uses intra-domain routing and inter-domain routing.

Link State Routing: It enables each router in the network learns the network topology to creates a routing table based on this topology.

Multicast: It is used for one or more network interfaces located on various subnets. It allows one-to-many communication.

Multicast Routing: Refers to sending information to well-defined groups that have large members but small compared to the network as a whole.

Non-adaptive Algorithms: They are independent of the volume of the current traffic and topology and decide the route to which a datagram is to send off-line.

Optimality Principle: This defines the optimal path.

Routing Algorithms: They are software part of the router and decide which output line an incoming packet should be transmitted on.

9.7 Review Questions

1. Discuss the role of network layer in the OSI model.
2. What are the main issues of concerns for the design of network layer?
3. Describe briefly how hierarchal algorithm works.
4. What is the main purpose of using router in a network?
5. Differentiate between:
   (a) Connectionless and connection-oriented service
   (b) Interior and Exterior Routing
   (c) Link state and distance vector routing

Answers: Self Assessment

1.	True	2.	False
3.	True	4.	False
5.	True	6.	Dynamic
7.	Shortest	8.	RIP
9.	Two	10.	Interior

9.8 Further Readings


Books

Achyut S Godbole and Atul Kahate, *Web Technologies,* Tata McGraw Hill.

Andrew S. Tanenbaum, *Computer Networks,* Prentice Hall.

Notes

Behrouz A. Forouzan, Sophia Chung Fegan, *Data Communications and Networking,* McGraw-Hill Companies.

Douglas Comer, *Computer Networks and Internets with Internet Applications,* 4th Edition, Prentice Hall.

Ferguson P., Huston G., John Wiley & Sons, Inc., 1998. *Quality of Service: Delivering QoS on the Internet and in Corporate Networks*.

J. D. Spragins, *Telecommunications Protocols and Design*, Addison Wesley.

McDysan, David E. and Darren L. Spohn, *ATM Theory and Applications*, McGraw-Hill Osborne Media, 1998.

Nassar, Daniel J., *Ethernet and Token Ring Optimization*, iUniverse.com, 2000.

Spurgeon, Charles E. Ethernet, *The Definitive Guide.* O'Reilly & Associates, 2000.

William A Shay, *Understanding Communication and Networks,* 3rd Edition, Thomson Press.

Notes

Unit 10: Network Layer in the Internet

CONTENTS

Objectives

After studying this unit, you will be able to:

- Describe the concept of IP protocol and IP addresses
- Discuss general Principles of congestion control
- Understand Congestion control and related algorithm
- Learn about various approaches of quality of service

Introduction

The Internet is considered as the interconnection of subnets or autonomous systems. They operate at network layer. To facilitate these subnets to virtually connect with one another for transferring a packet from source machine to destination machine, several backbones of high bandwidth and fast routers exist.. There are also several mid-level networks attached to the high speed backbones. Attached to this mid-level networks are the LANs of universities, companies, internet service providers, etc.

The glue that binds the Internet together is the IP (Internet Protocol) of the network layer. It provides a best-efforts way to transport datagrams from source machine to destination machine

Notes

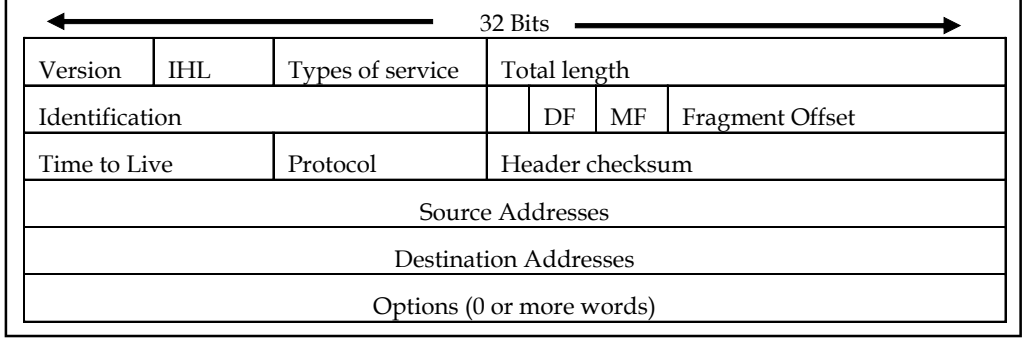
without considering as to whether or not these machines are on the same network or not. The steps involved in communication in the Internet are given below:

- The transport layer immediately above the network layer breaks data streams into datagrams. The size of the datagram size can be up to 64 KB but practically, it is around 1500 bytes so that they can fit into an Ethernet frame. Each datagram or fragment is a packet.
- Each datagram is transmitted through the Internet. Large datagrams are non-transparently fragmented, when required, into smaller units.
- When all the pieces reach to the destination machine, they are reassembled by the network layer into the original datagram.
- The reassembled datagram is handed over to the transport layer, which inserts it into the receiving process' input data stream.
- IP is an unreliable connectionless protocol.

10.1 IP Protocol

In contrast to TCP, it is a connectionless type service and operates at third layer of OSI reference model. That is, prior to transmission of data, no logical connection is needed. This type of protocol is suitable for the sporadic transmission of data to a number of destinations. It does not have such functions as sequence control, error recovery and control, flow control but it identifies the connection with port number. The IP datagram has a header of 20-byte fixed size and a text of variable length optional parts. The header format of IP datagram is depicted in Figure 10.1. The header format is transmitted from left to right, with the high order bit of Version field is transmitted first.

Figure 10.1: The IP (Internet Protocol) Header



Data encapsulation adds the IP header to the data. The IP header consists of five or six 32-bit words; the sixth word is attributed to the IP options field. The different fields of the IP header are given as below:

- Version refers to the version of the IP protocol in use and keeps track of the version of the protocol to which the datagram belongs to. The current version of IP is 4.
- Internet Header Length (IHL) indicates the length of the header field in 32-bit words. The minimum value of the header field is 5 that apply when no option is present. The maximum value of this 4 bit filed is 15 that restricts the header to 60 bytes and thus Option field to 40 byte.
- Type of service enables the host to indicate the subnet what kind of service (e.g., reliability and speed) it wants. It refers to any of the type of services that IP supports. Desired service

Notes

type is normally specified by user level applications. Examples of service type include minimum and maximum throughput, requested by applications such as the File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP).

- Total length has everything in the datagram (max. 64 KB). If it is subtracted from the IHL field, it indicates to IP the actual length of the data field.
- Identification enables the destination host to determine which datagram a newly arrived fragment belongs to:
  - DF means Do not Fragment.
  - MF is for More Fragments.
- Fragment offset indicates the source location of the current datagram. The elementary fragment unit size is 8 bytes.
- Time to live that counts hops is expressed in seconds. A zero count indicates that the packet is discarded. TTL is employed by IP to prevent a lost datagram from endlessly looping around the network. IP achieves this objective by initializing the TTL field to the maximum number of routers that the packet can traverse on the network. Every time the datagram traverses a router, IP decrements the TTL field by 1.
- Protocol indicates the destination which transports process to give the datagram to (TCP, UDP, or others).
- Header checksum verifies the header only. The algorithm is to add up all the 16-bit half-words as they arrive, using one's complement arithmetic.
- Source/Destination address tells the network number and host number.
- Options provides an escape to allow subsequent versions of the protocol to have information not present in the original design, to allow experimenters to try out new ideas, and to avoid allocating header bits to information that is rarely needed. On its presence, it includes optional control information. An example of optional information includes the route record, which includes a record of every router that the datagram traversed during its trip around the network.

10.1.1 IP Addresses

Using Internet has become common. We will now understand how Internet interprets the Internet address. The Internet addresses are written as www.hotmail.com, for the instance we write one more address as server.institution.domain. The address www.hotmail.com is not actual address; it is a text version of the Internet address, which is basically a binary representation. Now we compare www.hotmail.com, and server.institution.domain. WWW is the name of the server owned by the institution (in this case, it is hotmail) and this server is connected to the Internet to a domain server namely (com in this case) which maintains a database of the addresses of different servers using the same domain com. The domain name has no geographical relevance and two sites with same domain name may exist at two end of this world.

The above case is the simplest case. In another instance an organization may be large enough and have several other servers for different purposes such as web server, email server, print server, etc. Suppose we now take an example www.sun.planet.universe.in. This address has five parts separated by three dots. If we try to understand this address, this address will indicate that a group Planets (planet) comes under an Universe sub domain which is a part of India domain

Notes

and maintaining one server sun out of many servers, which is linked to Internet through its web server. Likewise any organization with several departments may create addresses for its sub domain with different servers being maintained there.

Internet is the collection of several independent networks, which are interconnected with one another. Now each independent network may have several hosts. Keeping this in mind, you can now think of address of your house. Your house has a unique house number, which is not assigned, to any other house in your locality. In this case, your house can be considered as a host. Your locality can be considered as network and your city as domain. You can write your address in Internet addressing notation as houseno.locality.city. If suppose you want to tell your address to a foreigner, then you will have to add your country name in your address. In this case it will become houseno.locality.city.country. Now if anybody desires to send you a letter or visit your house, he will first has to come to your country and then to your city. After that he will reach to your locality and then your house by your house number. The same analogy applies in case of Internet addressing.

We have already noted that a host on Internet has two parts. These are identification of the network and identification of the host on the network. In this manner, the address of a host is therefore comprised of two parts namely network address and host address. These two parts together make 32 bit long IP address for a particular host on the Internet. The IP address, which will see in the subsequent discussion, is written in four octets each separated by a dot. It may have a form like 197.23.207.10.

Notes Presently, we are using IP address version 4 (IPv4). However, IP address version 6 (IPv6) is gradually under implementation stage.

10.1.2 IPv4 Addressing

IPv4 addresses are uniquely used as identifiers, which work at network layer to identify the source or destination of IP packets. Presently, the version of IP, which is in use, is called as IPv4. In this version, every node on Internet may have one or more interfaces, and we are required to identify each of these devices with a unique address assigned to each of them. It means that each node is assigned one or more IP addresses to invoke TCP/IP. These are logical addresses and have 32 bits.

Technically, IP addresses are expressed using binary notation with 32 bit long string. In order to make these strings to remember easily, dotted decimal notations are used, in which periods or dots separate four decimal numbers from 0 to 255 representing 32 bits. As there are 32 bits therefore each decimal number contains 8 bits and called octet.

For example, the IPv4 address 11000000101010000000101000011001 is expressed as 192.168.10.25 in dotted decimal notation. Below are the steps to convert an IPv4 address from binary notation to dotted decimal notation:

- Break 32 bit long address into segments of 8-bit blocks: 11000000 10101000 00001010 00011001
- Write decimal equivalent of each segment: 192 168 10 25
- Separate the blocks with periods: 192.168.10.25

Figure 10.2 shows the IP address structure.

Notes

Figure 10.2: IP Address in Dotted Decimal Notation

11000000	10101000	00001010	00011001
192	168	10	25

Dotted Decimal Notation

We have seen that IPv4 address is expressed as a 32-bit number in dotted decimal notation. IP addresses may have fixed part and variable part depending upon the allocation of total addresses to you or your organization. Fixed part of the address may be from one octet to three octets and remaining octets will then be available for variable part. An IPv4 address is assigned using these parts. All bits in the fixed octet(s) are set to 1 while variable octet(s) are set to 0 bits. Thereafter, convert the result into dotted decimal notation. For example, you may take an IP address as 192.168.10.25. Now set all fixed bits to 1 and set all variable bits to 0. This gives 11111111 11111111 00000000 00000000. On converting it in dotted decimal notation, the result is 255.255.0.0. This dotted decimal notation with fixed and variable parts is used as address prefix to 192.168.10.25 and is expressed as 192.168.10.25, 255.255.0.0. This way of expressing the prefix length as a dotted decimal number is known as network mask or subnet mask notation.

Classification of IPv4 Addresses

Internet standards allow the following addresses:

1. ***Unicast:*** It is assigned to a single network interface located on a specific subnet ad facilitates one-to-one communication. This is unique address globally for the identification of a device on the network. It may be understood as the house number on a particular locality. It includes a subnet prefix and a host ID portion.

   (a) *Subnet prefix:* The subnet prefix is basically network identifier or network address portion of an IP unicast address. It should be noted that all nodes on the same physical or logical subnet must use the same subnet prefix, which eventually becomes unique within the entire TCP/IP network.

   (b) *Host ID:* The host ID, which is a host address portion of an IP unicast address, identifies a network node to which some devices are interfaced. It is also unique within the network segment.

2. ***Multicast:*** It is used for one or more network interfaces located on various subnets. It allows one-to-many communication. It delivers single packets from one source to many destinations. These addresses are part of Class D addressing scheme.

3. ***Broadcast:*** It is allocated to all network interfaces located on a subnet and is used for one-to-everyone on a subnet communication. It delivers packets from one source to all interfaces on the subnet. Broadcast addresses may be further classified as network broadcast, subnet broadcast, all subnets directed broadcast and limited broadcast.

Internet Addresses are further classified into different classes. It is based on the number bits are used for the address prefix of a single subnet and the number of bits are used for the host ID. It therefore allocates the number of networks and the number of hosts per network. There are five address classes as given below:

- ***Class A:*** It uses an 8 bit network number whose first bit is always zero as shown in Table 10.1. It is reserved for IP unicast addresses. If the number of hosts is very large on a

Notes

network, this class is used. It uses the only one octet to define prefix length. The numbers of network, which can be accommodated, are 2^8 or 128. However, out of these 128 addresses, 2 are used for administrative purposes and thus 126 addresses are available as prefix length. The remaining 3 octets are used for identifying up to 2^{24} or 16,777,214 host IDs.

- ***Class B:*** It uses 16 bits for both the network address and host address. In this case the first two bits are always 10. It is reserved for IP unicast addresses. It uses 2 octets for a particular network while remaining two octets for host IDs. They are particularly used for medium to large-sized networks. The Class B addresses can be provided to 16,384 networks with up to 65,536 hosts per network.
- ***Class C:*** It is reserved for IP unicast addresses. They are meant for small networks. The first 3 octets specify a particular network and the last one octet specify host IDs. The Class C addresses may be used up to 2,097,152 networks with up to 254 hosts per network. Its first three bits are always set to 110.
- ***Class D:*** It defines IP multicast addresses.
- ***Class E:*** These addresses were reserved for experimental uses.

The Table represents IPv4 addresses classifications.

Table 10.1: Classifications of IPv4 Addresses

32 bit address					Number of possible networks	Maximum number of host or nodes
Classification	**Octet 1**	**Octet 2**	**Octet 3**	**Octet 4**		
Class A	0bbbbbbb	xxxxxxxx	xxxxxxxx	xxxxxxxx	$2^7 = 128$	$2^{24} = 16,777,216$
Class B	10bbbbbb	bbbbbbbb	xxxxxxxx	xxxxxxxx	$2^{14} = 16,384$	$2^{16} = 65,536$
Class C	110bbbbb	bbbbbbbb	bbbbbbbb	xxxxxxxx	$2^{21} = 2,097,152$	$2^8 = 256$
Class D	1110bbbb followed by a 28 bit multicast address					
Class E	1111; reserved					

Allocation of the IPv4 address based on the above schemes sometimes proves to be wastage of addresses. Any organization with Class A address may have 16,777,214 hosts. Probably, no organization may have more than 100,000 hosts. In this case a huge IPv4 addresses are just wasted. Earlier, Classless Inter-Domain Routing (CIDR) method is used to allocate IPv4 addresses based on the organization's needs. The agency namely Internet Corporation for Assigned Names and Numbers (ICANN) or an Internet Service Provider (ISP) are responsible to determine the need of an organization for allocating IPv4 addresses under required Class.

In case of individual address, public address is used. Private addresses are also allocated based on proxied or translated connectivity to the Internet. It is observed that a user who is either a part of any organization or belong to an ISP did not require direct connectivity to the Internet. Therefore such organizations or ISPs require only a few public addresses for their nodes such as proxy servers, routers, firewalls, and translators etc. to connect directly with the Internet. Therefore, some the addresses are reserved for private use distinctly from public addresses.

Address is an identifier that is assigned to a device attached to a node in the Internet. It tells about the source or destination of IP packets. Addresses are classified based on their purposes as unicast, multicast and broadcast. The number of network segments and hosts on the network is determined based on Class A, B and C addresses for unicast communication.

Notes

10.1.3 Subnetting for IP Addresses

Over the past several years, the Internet has scaled enormous volume in terms of hosts connected to it and therefore IPv4 addresses yet available are becoming scare. You may have confusion here that 32 bits give 2^{32} unique addresses which comes around 4.3 billion different addresses. But this not the condition because of the different classes of the IPv4 addresses. Suppose a medium sized organization gets Class B address based on its current user population of say 1000. It uses 1000 different addresses. But the organization management has the ability to assign 2^{16} = 65,536 different identifiers. It means that there is 65,536 addresses wastage. Since they all belong to the same class B network number, they cannot be reclaimed by any other organization. A network administrator may suggest using Class C network address, which may require at least four class C networks. Later on, suppose, the number of users increase and the organization applies for another class C network, it might not get the same or if it gets, it has to pass through a hell of paper works and delays. In addition there is another angle of this problem with regard to additional routing. With many Class C networks, you need to have more network number for routers to track. Consequently performance of the network deteriorates. The solution of these problems lie either in increasing the number of bits in IP address or Classless Inter Domain Routing (CIDR).

We may also use a technique called subnetting to efficiently divide the address space allocated to an organization to the different users divided among different subnets of an organization network. Therefore subnetting is a process through which the address space of a unicast address prefix is efficiently divided for allocation among the subnets of an organization network. As we know that a unicast address have fixed and variable portions. The fixed portion of a unicast address prefix has a defined value. The variable portion of a unicast address prefix has the bits beyond the prefix length, which needs to set to 0. Subnetting uses the variable portion of a unicast address prefix for assignment to the subnets of an organization network.

In order to implement subnetting, you need to follow the some guidelines:

- Assess the number of subnets requirement.
- Assess the number of host IDs for each subnet.

After this, a set of subnetted address prefixes with a range of valid IP addresses may be defined. Following steps are followed for subnetting:

1. Estimate the number host bits for the subnetting.
2. Determine the new subnetted address prefixes.
3. Determine the range of IP addresses for each new subnetted address prefix.

We may now learn as to how the subnet prefix of an IP address is determined. Following steps give you a way to determine the same without the use of binary numbers:

1. Write the number n (the prefix length) as the sum of 4 numbers by successively subtracting 8 from n. For example, 22 is 8 + 8 + 6 + 0.
2. In a table with four columns and three rows, place the decimal octets of the IP address in the first row. The second row will then contain the four digits of the sum as has been determined in step 1.
3. The columns having 8 in the second row, write the corresponding octet from the first row to the third row. In case of 0 in a column in the second row, place 0 in the third row.
4. The column in the second row having a number between 0 and 8, convert the decimal number in the first row to binary. Now select the high-order bits for the number of bits

Notes

indicated in the second row and put zero for the remaining bit and then convert back to decimal number. This will be the entry in that column. For our example the entry in third column of first row is 10. Therefore, the binary equivalent is 00001010. Again the third column of second row is having 6. It means we have to take 6 bits as such from high bi side and converting the remaining two bits as 00. This will give us a binary number as 00001000 which is decimal equivalent to 8. Therefore, the entry 8 will go in that column.

192	168	10	25
8	8	6	0
192	168	8	0

This gives the subnet prefix for the IPv4 address configuration 192.168.10.25/22 as 192.168.204.0/22.

Now, we have to extract the subnet prefix from an arbitrary IPv4 address using an arbitrary subnet mask. For this purpose a mathematical operation logical AND is used. A logical comparison between the 32-bit IP address and the 32-bit subnet mask is performed. It gives the subnet prefix. For example, we may consider the following possible addresses for Class C.

Class C Network	Bit Representation	Address Range
210.195.8.0	11010010-11000011-00001000-xxxxxxxx	210.195.8.0-211.195.8.255
210.195.9.0	11010010-11000011-00001001-xxxxxxxx	210.195.9.0-211.195.9.255
210.195.10.0	11010010-11000011-00001010-xxxxxxxx	210.195.10.0-211.195.10.255
210.195.11.0	11010010-11000011-00001011-xxxxxxxx	210.195.11.0-211.195.11.255

These Class C networks define the contiguous set of addresses from 210.195.8.0 to 210.195.11.255. On examining these addresses, it is observed that the first 22 bits are same for each address. It means that any of these Class C networks has 22 bit network number followed by a 10 bit local identifier for hosts. A router then can extract the network number using a logical AND operation between a 22-bit subnet mask and an IP address. For this example, we can say that a router can represent the four networks using the single entry 210.195.8.0/22, where /22 indicates the network number is 22 bits long. Likewise, 210.195.8.0/20 address would first 20 bits and so on. This indicates that we are grouping different smaller networks together and they are being treated same for the routing purposes.

Let us know take an example. Our IPv4 address is 210.195.8.0 and a 22 bit subnet mask is 255.255.252.0.

11010010 – 11000011 – 000010xx – xxxxxxxx (IP Address)

and

$$\frac{11111111 - 11111111 - 11111100 - 00000000}{11010010 - 11010011 - 00001000 - 00000000} \quad \frac{\text{(22 bit subnet mask)}}{\text{(network number)}}$$

(210) (195) (8) (0)

The result of the bit-wise logical AND of the 32 bits of the IPv4 address and the subnet mask is the subnet prefix 210.195.8.0. It may therefore be noted that the bits in the fixed portion of the address (in which the bits in the subnet mask are set to 1), the subnet prefix bits are copied from the IPv4 address, essentially extracting the subnet prefix of the IPv4 address. On the other side, the bits in the variable portion of the address where these are set to zero, the subnet prefix bits are also set to 0 and thus discarding the host ID portion of the IPv4 address.

Notes

Task Differentiate between Class A, B, C, D and E type of IP addresses.

Self Assessment

Fill in the blanks:

1. …… is the collection of several independent networks, which are interconnected with one another.
2. The …….. is basically network identifier or network address portion of an IP unicast address.
3. …… is reserved for IP unicast addresses.
4. CIDR stands for ……..
5. Technically, IP addresses are expressed using binary notation with …… bit long string.

10.2 Congestion Control

Congestion causes chocking of the communication channel. When too many packets are present in a part of the subnet, the performance of the subnet degrades. Hence, a communication channel of a network is called *congested* if packets traversing the path experience delays largely in excess of the paths propagation delay. It is called heavily congested when the packets never reach the destination indicating that the delay approaches infinity. The reasons for congestion are not one but many. When the input traffic rate exceeds the capacity of the output lines, the input part of the subnet gets chocked and creates congestion. Congestion is also happened when the routers are too slow to perform queuing buffers, updating tables, etc. Lack of capacity of the routers' buffer is also one of many factors for congestion. However, enhancing memory of the router may be helpful up to a certain point. Beyond a certain point of time, congestion gets worse because of timeout retransmission will create more traffic load. Briefly, the apparent causes of congestion are jamming by several input lines, slow processors, low bandwidth, finite number of buffers, etc.

Did u know? Congestion control and flow control are two different phenomenons. Congestion is a global phenomenon involving all hosts, all routers, the store-and-forward processing within the routers, etc., whereas, flow control is concerned with point-to-point traffic between a given source host and a given destination host. The example of congestion control is a situation when a store-and-forward network with 1-Mbps lines and 1000 large minicomputers, half of which were trying to transfer files at 100 kbps to the other half. An example of flow control is when a fiber optic network with a capacity of 1000 gigabits/sec on which a supercomputer was trying to transfer a file to a personal computer at 1Gbps.

10.2.1 General Principles of Congestion Control

According to control theory, the computer network, which is also a system, is divided into two groups. They are open loop and closed loop solutions.

The open loop solutions: provide good design to ensure that the problem does not occur in the first place. The designing tools include decision for accepting new traffic, discarding packets and scheduling of the packets at various points in the network. The open loop solution's decisions are independent of the current state of the network.

Notes

Closed loop solutions: make decision based on the concept of a feedback loop. The feedback loop enables the closed loop system to monitor the system to detect when and where congestion occurs. Thereafter, it passes the information to the places where actions can be taken. This enables to adjust system operation to correct the problem.

Monitoring of the system is dependent upon the percentage of all packets discarded for lack of buffer space, the average queue lengths, the number of packets that time out and are retransmitted, the average packet delay and the standard deviation of packet delay. The monitored congestion information is provided to all places of actions when the router detects the congestion; it sends a separate warning packet to the traffic source immediately. This done by reserving a bit or field in each packet which is filled in each outgoing packet in case of a congested state encountered by a router to caution the neighbors. Secondly, hosts or routers send packets periodically to explicitly know about congestion so that the traffic around congested areas may be routed to alternate destination paths.

The congestion may be controlled as given below:

1. Increase the bandwidth in the network. Increasing an additional line temporarily increases the bandwidth between certain points.
2. Split traffic to follow multiple routes.
3. Increase the resources. For example, use spare routers.
4. Decrease the load by denying service to some users or degrading service to some or all users.
5. Estimate users schedule and demands in a more predictable way.

10.2.2 Traffic Management

The traffic management facility allows maximizing available network resources and ensures efficient use of resources that have not been explicitly allocated. Traffic management will be mainly dependent on transmit priority and bandwidth availability. In the transmit priority, delay-sensitive traffic is assigned a higher transmit priority. Support for bandwidth availability deals bandwidth allocation for each VCC, connection admission control (CAC) preventing network users from allocating more bandwidth than the network can provide, traffic policing to ensure that a VCC, once established, does not attempt to use more bandwidth than the network currently has available and selective cell discard dealing with momentary over subscription of the buffer capacity of an output port.

Average Packet Delay

Suppose

Average arrival rate of packets at a router for processing = λ packets per second

Average processing rate of packets one at a time at the router = μ packets per second

Utilization of the channel = $\rho = \lambda / \mu$

From Queueing theory, the average delay a packet experiences at a router before being forwarded is given by:

$T = \lambda / \mu (1/1- \rho)$

From the above, it is clear that average delay approaches infinity as utilization approaches unity.

Notes

10.2.3 Congestion Prevention Policies

Open loop systems are designed to minimize the congestion at the place of its origin. Applying congestion prevention policies at different layers solves the problem in case of open loop systems. The policies at data link, network and transport layers that affects congestion is given below:

Data link layer: The issues such as retransmission of packets, out of order caching, acknowledgement of the received packets from destination machine and flow control affect congestion at this layer.

Network layer: Setting up of virtual channel and datagram inside the subnet, packet queueing and forwarding at router, dropping of packets at router, routing algorithms, packet lifetime management, etc are the factors affecting congestion at this layer.

Transport layer: Retransmission of packets, out of order caching, acknowledgement of the received packets from destination machine, flow control mechanism, time out packets, etc. affect congestion at this layer.

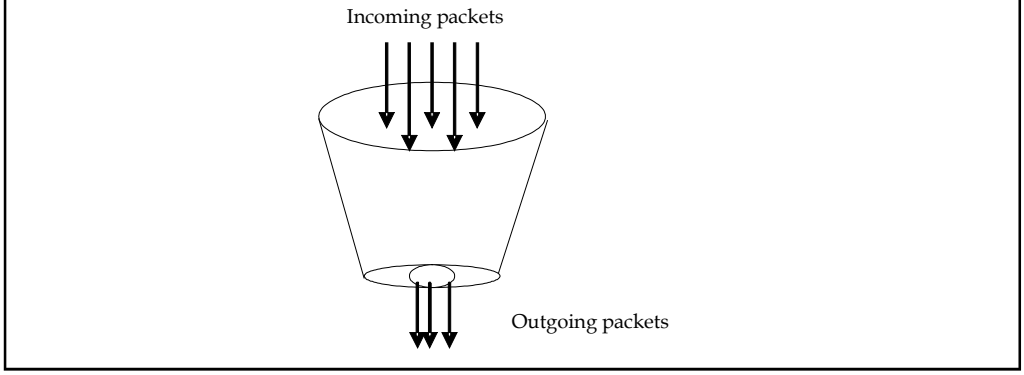
Traffic Shaping

One of the main reasons for congestion is the bursty traffic. Another cause is the transmission of packets at an unpredictable rate. Hence, the traffic shaping approach includes transmission of packets at uniform rate and in more predictable rate in case of open loop method. Thus, the traffic shaping attempts to regularize the average rate of data transmission. For example, the ATM networks exploit this method to a greater extent. To reduce congestion, the user and the subnet agree on a certain traffic pattern in a virtual circuit. Such agreements are of great importance for transfer of real time audio and video connections, which do not tolerate congestion. Monitoring traffic pattern is called traffic policing.

Leaky Bucket

The leaky bucket algorithm finds its use in the context of network traffic shaping or rate limiting. The algorithm enables to control the rate at which data is injected into a network and thus handling burstiness in the data rate. A leaky bucket implementation and a token bucket implementation are predominantly used for traffic shaping algorithms. The leaky-bucket algorithm is used to control the rate at which traffic is sent to the network and shape the bursty traffic to a steady stream of traffic. Figure 10.3 shows the leaky bucket algorithm.

Figure 10.3: Leaky Bucket Algorithm



Notes

In the leaky bucket algorithm, a bucket with a volume of, say, b bytes and with a hole in the bottom is taken into consideration. If the bucket is empty, it means b bytes are available as storage. A packet with a size lesser than b bytes arrives at bucket, it will be forwarded. If size of the packet increases more than b bytes, it will either be discarded or queued. It is also assumed that the bucket leaks through the hole in its bottom at a constant rate of *r* bytes per second. The outflow is considered at a constant rate when there is any packet in the bucket, and zero when the bucket is empty. This explains that if data flows into the bucket faster than data flows out through the hole, the bucket overflows. This results further incoming data to be discarded until enough volume again exists in the bucket to accept new data.

The disadvantages associated with the leaky-bucket algorithm are inefficient use of available network resources. The leak rate is a fixed parameter. In case of the traffic volume is very low, the large portions of network resources like bandwidth are not being used efficiently. The leaky-bucket algorithm does not enable individual flows to burst up to port speed to effectively consume network resources at times when there would not be resource contention in the network.

The leaky bucket algorithm uses average rate and burst rate parameters to control traffic flow. Average rate is defined as the average number of packets per second that leak from the hole in the bottom of the bucket and enter the network. The burst rate is the rate of accumulation of packets in the bucket and expressed in packets per second. For example, if the average burst rate is 10 packets per second, a burst of 10 seconds allows 100 packets to accumulate in the bucket.

Notes The leaky bucket algorithm also uses two state variables namely current time and the virtual time. The current time is current time of the computer's watch while virtual time measures how much data has accumulated in the bucket and is expressed in seconds.

For example, if the average rate is 10 packets per second and 100 packets have accumulated in the bucket, then the virtual time is 10 seconds ahead of the current time.

The Token Bucket Algorithm

The leaky bucket algorithm has rigid output pattern at the average rate independent of the bursty traffic. In many applications, when large bursts arrive, the output is allowed to speed up. This calls for more flexible algorithm preferably that never loses data. Hence, a token bucket algorithm finds its uses in the context of network traffic shaping or rate limiting. The token bucket is a control algorithm that dictates when traffic should be transmitted. This order comes based on the presence of tokens in the bucket. The bucket contains tokens. Each of the token represents a packet of predetermined size. Tokens in the bucket are removed for the ability to send a packet. When tokens are present, A flow to transmit traffic occurs in the presence of tokens. No token means no flow transmits its packets. Hence, a flow transmits traffic up to its peak burst rate in the presence of adequate tokens in the bucket.

Thus, the token bucket algorithm adds token to the bucket every 1 / *r* seconds. The capacity of the bucket is b tokens. When a token arrives and the bucket is full, the token is discarded. If a packet of n bytes arrives and n tokens are removed from the bucket, the packet is forwarded to the network. When a packet of n bytes arrives but fewer than n tokens are available. In such case no tokens are removed from the bucket and the packet is considered to be non-conformant. The non-conformant packets may either be dropped or queued for subsequent transmission when sufficient tokens have accumulated in the bucket. They may also be transmitted but marked as being non-conformant. Possibility is that they may be dropped subsequently if the network is overloaded.

Notes

The advantage of this algorithm is to save up to the maximum size of the bucket. This means that bursts of up to number of packets can be sent at the maximum speed for a certain period of time.

Task What are some preventive measures for congestion control?

10.3 Quality of Service

Quality of Service (QoS) determines the capability of a network to provide predictable service over various technologies including frame relay, Asynchronous Transfer Mode (ATM), Ethernet, SONET and IP-routed networks. The networks may use any or all of these technologies. The QoS also ensure that while providing priority for one or more flow does not make other flows fail. A flow may be a combination of source and destination addresses, source and destination socket numbers, and the session identifier or any packet from a certain application or from an incoming interface. The QoS is primarily used to control over resources like bandwidth, equipment, wide-area facilities and so on, make more efficient use of network resources, provide tailored services, provide coexistence of mission-critical applications, etc.

The traffic to computer networks often receives equal priority and the computer networks usually do not differentiate between non-critical browser traffic and critical business applications. The quality of service (QoS) of computer networks is evaluated with respect to the traffic priority to understand why QoS is desirable in an intranet and the Internet. The bandwidth is considered an important subject for Internet and intranet services. The amount of data that is being transmitted through the Internet has been increasing exponential and new applications like real audio and video; VoIP, videoconferencing, etc. keep on demanding increased bandwidth. The conventional Internet applications like WWW, FTP, telnet; etc. cannot tolerate packet loss but are less sensitive to variable delays. However, most real-time applications can compensate for a reasonable amount of packet loss but are usually very critical towards high variable delays. Therefore, bandwidth plays an important role in providing a good quality of service. A QoS is defined as a policy framework that describes the quality of a specific stream of data in terms of bandwidth, buffer usage, priority, CPU usage, etc. However, the IP protocol stack provides only one QoS in term of best effort in which the packets are transmitted from point to point without any guarantee for a special bandwidth or minimum time delay. The best effort traffic model handles all Internet requests with equal priority and serves them with the first come first serve strategy.

10.3.1 Basic QoS Architecture

QoS enables better service to certain flows in a network by either raising the priority of a flow or limiting the priority of another flow. The queue management tool, policing and shaping, Link efficiency tools, etc. are used for controlling the flows and congestion. Thus, QoS tools intend to alleviate most congestion problems. The basic QoS architecture involves three fundamental pieces for QoS implementation. They are QoS identification and marking techniques for coordinating QoS from end to end between network elements, QoS within a single network element, for example, queuing, scheduling, and traffic-shaping tools and QoS policy management and accounting functions to control and administer end-to-end traffic across a network. QoS Identification and Marking is carried out through classification and reservation. Classification refers to the identifying and providing preferential service to a type of traffic. In classification, the packet may or may not be marked. If the packet is identified but not marked, it is said to be on a per-hop basis. If packets are marked, IP precedence byte is set. Common methods of identifying flows are Access Control Lists (ACLs), Policy-based Routing, Committed Access Rate (CAR), Network-based Application Recognition (NBAR), etc.

10.3.2 QoS Concepts

Notes

Congestion Management: The bursty nature of data traffic, sometimes bounds to increase the amount of traffic more than the speed of a link. In such a situation, QoS enables a router to put packets into different queues and service certain queues more often based on priority rather than buffer traffic in a single queue and let the first packet in be the first packet out. Such issues are incorporated in congestion-management tools to handle. Thus, the congestion management tool may include priority queuing, custom queuing, weighted fair queuing, etc.

Queue Management: The queues in a buffer may fill and overflow. A packet will be dropped if a queue is full and router cannot prevent this packet from being dropped even if it is a high-priority packet. This is referred as tail drop. It could be prevented either by ensuring that the queue does not fill and provide room for high-priority packets or allow some rule for dropping packets with lower priority before dropping higher-priority packets. A mechanism called weighted early random detect perform both of these functions.

Link Efficiency: Sometimes, the low-speed links are bottlenecks for smaller packets. The serialization delay caused by the large packets force the smaller packets to wait longer. The serialization delay is the time taken to put a packet on the link. The serialization delay (For example, the serialization delay for a 2400-byte packet on a 56-kbps link will be 343 milliseconds) will make a voice packet, which is behind it in queue to delay enormously before the packet left the router, a situation, which is not desirable for voice packets. The link fragmentation and interleave process segment large packet into smaller packets interleaving the voice packet.

Elimination of overhead bits: The efficiency could also be improved by eliminating too many overhead bits. For example, RTP headers have a 40-byte header and a payload of as little as 20 bytes. In such a case, the overhead is twice that of the payload. Some compression technique may be applied to reduce the header to a more manageable size.

Traffic shaping and policing: Shaping is used to prevent the overflow problem in buffers by limiting the full bandwidth potential of the packets of applications. Sometimes, in many network topologies that has a high-bandwidth link connected with a low-bandwidth link in remote sites may overflow low bandwidth link. Hence, shaping is used to provide the traffic flow from high bandwidth link closer to the low bandwidth link to avoid the overflow of the low bandwidth link. Policing is used to discard the traffic that exceeds the configured rate but in case of shaping it is buffered.

End-to-end QoS Levels

It refers to the capability of a network to deliver service needed by specific network traffic from end to end or edge to edge under network constraints like bandwidth, delay, jitter, loss characteristics, etc. These factors describe how tightly the end-to-end service performs. The QoS involves a policy framework or set of rules that designate an action. The policy framework provides a particular service to particular client, application and schedule. Three basic levels of end-to-end QoS can be provided across a heterogeneous network. They are integrated service, differentiated service and inbound admission service types.

Performance Limits: The performance limits also considers the token bucket limits and bandwidth limits together to guarantee packet delivery in outbound bandwidth policies for the integrated and differentiated service.

Token Bucket Size: When an application is sending information faster than the server sends the data out of the network, the buffer will fill up. To avoid such situations, the token bucket size is applied to determine the amount of information a server can process at any given time. A packet

Notes

exceeding this limit is not considered. However, in integrated service, any packet overruling the packet size is not limited but discarded and will not be allowed for a RSVP connection request. The maximum token bucket size is considered as 1 GB.

Token Rate Limit: The rate limit is the number of bits per second that can be allowed into a network. The requested bandwidth for an application is compared with the token rate limit. When the requested bandwidth is more than the rate limit, the request is denied. The token rate limit is only used for admission control within integrated service. This value can range from 10 Kbps to 1 Gbps.

Self Assessment

State whether the following statements are true or False:

6. The quality of service (QoS) of computer networks is evaluated with respect to the traffic priority.
7. Bandwidth has no role to plays in providing a good quality of service.
8. The best effort traffic model handles all Internet requests with equal priority and serves them with the first come first serve strategy.
9. The congestion management tool may include priority queuing, custom queuing, weighted fair queuing, etc.
10. The link fragmentation and interleave process segment small packet into large packets interleaving the voice packet.
11. Shaping is used to prevent the overflow problem in buffers by limiting the full bandwidth potential of the packets of applications.

10.4 Summary

- IPv4 addresses are uniquely used as identifiers, which work at network layer to identify the source or destination of IP packets. Presently, the version of IP, which is in use, is called as IPv4. In this version, every node on Internet may have one or more interfaces, and we are required to identify each of these devices with a unique address assigned to each of them. It means that each node is assigned one or more IP addresses to invoke TCP/IP. These are logical addresses and have 32 bits.
- The designers of the internet protocol defined an ip address as a 32-bit number and this system, known as internet protocol version 4 (ipv4), is still in use today. However, due to the enormous growth of the internet and the predicted depletion of available addresses, a new addressing system (ipv6), using 128 bits for the address.
- When too many packets are present in a part of the subnet, the performance of the subnet degrades. Hence, a communication channel of a network is called *congested* if packets traversing the path experience delays largely in excess of the paths propagation delay. It is called heavily congested when the packets never reach the destination indicating that the delay approaches infinity.
- Congestion control and flow control are two different phenomenon. Congestion is a global phenomenon involving all hosts, all routers, the store-and-forward processing within the routers, etc., whereas, flow control is concerned with point-to-point traffic between a given source host and a given destination host.
- According to control theory, the computer network, which is also a system, is divided into two groups. They are open loop and closed loop solutions.

Notes

- The traffic management facility allows maximizing available network resources and ensures efficient use of resources that have not been explicitly allocated. Traffic management will be mainly dependent on transmit priority and bandwidth availability. In the transmit priority, delay-sensitive traffic is assigned a higher transmit priority.
- The leaky bucket algorithm finds its use in the context of network traffic shaping or rate limiting. The algorithm enables to control the rate at which data is injected into a network and thus handling burstiness in the data rate.

10.5 Keywords

Congestion: A communication channel of a network is called *congested* if packets traversing the path experience delays largely in excess of the paths propagation delay.

IP Address: An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

IP Protocol: The Internet Protocol (IP) is the principal communications protocol used for relaying datagrams (packets) across an internetwork using the Internet Protocol Suite.

Traffic Shaping: Attempts to regularize the average rate of data transmission.

10.6 Review Questions

1. Describe IP Protocol. How does it differ from TCP protocol.
2. What are IP addresses? Describe the format of an IP address.
3. Discuss IPV4 addressing along with its classification.
4. Describe the concept of subnetting.
5. Explain the general principles of congestion.
6. What do you understand by QoS? Describe the basic QoS structure.
7. Discuss the following two algorithms:
   (a) Leaky Bucket
   (b) Token Bucket
8. What are two types of congestion control? Where is congestion control implemented in each case?

Answers: Self Assessment

1. Internet
2. subnet prefix
3. Class C
4. Classless Inter Domain Routing
5. 32
6. True
7. False
8. True
9. True
10. False
11. True

Notes

10.7 Further Readings

Books

Achyut S Godbole and Atul Kahate, *Web Technologies,* Tata McGraw Hill.

Andrew S. Tanenbaum, *Computer Networks,* Prentice Hall.

Behrouz A. Forouzan, Sophia Chung Fegan, *Data Communications and Networking,* McGraw-Hill Companies.

Douglas Comer, *Computer Networks and Internets with Internet Applications,* 4th Edition, Prentice Hall.

Ferguson P., Huston G., John Wiley & Sons, Inc., 1998. *Quality of Service: Delivering QoS on the Internet and in Corporate Networks.*

J. D. Spragins, *Telecommunications Protocols and Design*, Addison Wesley.

McDysan, David E. and Darren L. Spohn, *ATM Theory and Applications*, McGraw-Hill Osborne Media, 1998.

Nassar, Daniel J., *Ethernet and Token Ring Optimization*, iUniverse.com, 2000.

Spurgeon, Charles E. Ethernet, *The Definitive Guide.* O'Reilly & Associates, 2000.

William A Shay, *Understanding Communication and Networks,* 3rd Edition, Thomson Press.

Unit 11: Transport Layer

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Describe the concepts behind the transport layer services like multiplexing/demultiplexing, reliable data transfer, flow control, congestion control
- Analyze the transport services and issues involved for efficient exchange of data from transport entity to transport entity.
- Understand the transport layer primitives and examples for implementing transport protocol.
- Discuss various transport layer protocols in the Internet including UDP and TCP

Introduction

The transport layer makes the upper layers from any concern with providing reliable and cost effective data transfer. It facilitates end-to-end control and information exchange with the quality of service required by the application program. Thus, layer four of the OSI reference model is the transport layer that provides transparent transfers of data between the source and destination machines using the services of the network layer such as IP. It enables reliable internetworking data transport services that are transparent to upper layers. The transport layer protocol

Notes

administers end-to-end control and error checking to ensure complete data transfer. The functions provided at this layer are transport address to network address mapping, makes multiplexing and splitting of transport connections, flow control, virtual circuit management and error checking and recovery. The transport layer's job also includes breaking the messages from the session layer into segments. The transport-layer protocols including Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Name Binding Protocol and OSI transport protocols provide either connection-oriented or connectionless transmission. Quality of service is also one of the functions of the transport layer.

11.1 Transport Service

The basic function of the transport layer is to respond to service requests from the session layer and issue service requests to the network layer. To accomplish this task, it accepts data from the session layer, splits it up into smaller units if required, pass these smaller units to the network layer and ensure that the packets of data reassemble correctly at the destination machine. The transport layer indents to perform all these function efficiently and keep the session layer isolated from the necessary changes in the hardware technology. The transport layer provides the following services:

11.1.1 Services Provided to the Upper Layers

Transport layer in conjunction with network layer intends to provide efficient, reliable and cot effective services to its users through processes in application layer. The software and hardware that are used in the transport layer is called transport entity. The transport entity is located either in the kernel of the operating system or network interface card or remote user process or the library package meant for network applications.

Did u know? Like, network layer, the transport also provides connection oriented and connectionless services. Under normal conditions, in both cases, connection is established to transfer data and after successful transfer of data the connection is released.

The transport layer establishes a distinct network connection for a transport connection required by the session layer. When the transport connection needs a high throughput, the transport layer establishes multiple network connections where it divides the data among the multiple network connections to improve throughput. It also manages the bandwidth and thus reduces the cost of establishing a connection. It does so by multiplexing several transport connections onto the same network connection. The multiplexing always remains transparent to the session layer. Thus transparent layer isolates the upper layers from the technology, design and imperfections of the subnet.

11.1.2 Quality of Service

Transport layer bridges the gap of the services provided by the network and therefore enhances the quality of service provided to the users. The possible parameters for the quality of service as offered by the transport layer are connection establishment delay, connection establishment failure probability, throughput, transit delay, residual error ratio, protection priority, resilience, etc.

Connection establishment delay: It is the amount of time when an acknowledgement is received from the destination machine to which a connection is requested. Obviously, lesser is the delay, better is the service.

Notes

Connection establishment failure probability: Due to congestion in the network, lack of availability of space in table, some internal problem, etc., causes the connection not to set within the establishment delay.

***Throughput*:** It defines the number of bytes of user data transferred per second in a defined time interval. For each communication link it is measured separately.

Transit delay: It is the time gap between a transmitted data from source machine to the reception of the same data by the destination machine. Like, throughput, for each communication link it is measured separately.

Residual error ratio: It is the fraction of the lost data with respect to the total data sent over the network by source machine.

Protection priority: It is defined as the capability of the transport layer to provide Protection against third parties who try to interfere with the data. It specifies the priority of the important connections so that high priority connections are served before the low priority connections in the event of congestion.

Resilience: It is the capability of the transport layer to terminate a connection itself spontaneously in the case of congestion.

Transport layer can not always fulfill all of the parameters as mentioned above. It tries to implement a trade off among the parameters of quality of service. This process is called option negotiation.

11.1.3 Transport Service Primitives

They are used to access transport services by the application layer or the users. Each transport service is defined with a unique transport primitive. The network layer provides an unreliable service whereas the transport layer attempts to provide a reliable service on top of the unreliable service. Some of the transport primitives are LISTEN, CONNECT, SEND, RECEIVE and DISCONNECT.

Transport Protocol Data Unit (TPDU) is a term used for exchanging data from transport entity to transport entity. The TPDUs are contained in the packets exchanged by the network layer. The packets are then contained in the frames exchanged by the data link layer. At the destination machine, when a frame arrives the data link layer processes the frame header and passes contents of the frame payload field up to the network entity. Similar process takes place at the network layer.

The above situation may be understood from an example, when a remote machine, say, client machine requests another machine, say, server for connection. The client machine issues a TPDU CONNECT to the server. The server has already transmitted a TPDU LISTEN to the network to block the connection until a client machine turns up. On receiving the TPDU CONNECT, it unblocks the server machine and a CONNECTION ACCEPTED TPDU is sent back to the client machine and thus connection is established by unblocking the client machine too. After this, the SEND and RECEIVE primitives enable exchange of data.

Following are the steps implemented by client machine to establish the connection:

- Create a socket
- Connect the socket to the address of the server machine
- Send/Receive data
- Close the socket

Notes

Following are the steps implemented by the server machine to establish the connection:

- Create a socket
- Bind the socket to the port number known to all clients
- Listen for the connection request
- Accept connection request
- Send/Receive data

Task Give a brief description of the exchange of data between a client and server machine using transport primitives.

11.2 Elements of Transport Protocol

To establish a reliable service between two machines on a network, transport protocols are implemented which some how resembles to the data link protocols implemented at layer 2. The major difference lies in the fact that data link layer uses a physical channel between two routers while the transport layer uses subnet. Following are the issues for implementing transport protocols:

- ***Types of Service:*** The transport layer also determines the type of service provided to the users from the session layer. An error-free point-to-point communication to deliver messages in the order in which they were transmitted is one of the key functions of the transport layer. However, the service may be reliable or may be reliable within certain limits or may be unreliable entirely. The order of the received message may or may not be the same in which it was transmitted. When the connection is created between two processes, transport layer determines the type of service to be provided to session layer at that time.
- ***Error Control:*** Error detection and error recovery are the integral part of a reliable service and therefore they are necessary to perform error control mechanism on end-to-end basis. To control errors from lost or duplicate segments the transport layer enables unique segment sequence numbers to the different packets of message, creating virtual circuits, allowing only one virtual circuit per session. Timeouts mechanism is also used to remove the packets from the network segments that have been misrouted and have remained on the network beyond a specified time. End-to-end error control using checksums are also used to handle any corruption in data.
- ***Flow Control:*** The underlying rule of flow control is to maintain a synergy between a fast process and a slow process. Transport layer enables a fast process to keep pace with a slow one. Acknowledgements are sent back to manage end-to-end flow control. Go back N algorithms is used to request retransmission of packets starting with packet number N. Selective Repeat is used to request specific packets to be retransmitted.
- ***Connection Establishment/Release:*** The transport layer creates and releases the connection across the network. This includes naming mechanism so that a process on one machine can indicate with whom it wishes to communicate. The transport layer enables to establish and delete connections across the network to multiplexing several message streams onto one communication channel.
- ***Multiplexing/Demultiplexing:*** The transport layer establishes separate network connection for each transport connection required by the session layer. To improve throughput, the transport layer establishes multiple network connections. When the issue of throughput

Notes

is not important, it multiplexes several transport connections onto the same network connection, thus reducing the cost for establishing and maintaining the network connections. When several connections are multiplexed, they call for demultiplexing at the receiving end. In case of transport layer, the communication takes place only between two processes and not between two machines. Hence, the communication at transport layer is also known as peer-to-peer or process-to-process communication.

- ***Fragmentation and re-assembly:*** When transport layer receives large message from session layer, it breaks the message into smaller units depending upon the requirement. This process is called fragmentation. Thereafter, it is passed to the network layer. Conversely, when transport layer acts as receiving process, it reorders the pieces of message before reassembling them into a message.
- ***Addressing:*** Transport Layer deals with addressing or labeling a frame. It also differentiates between a connection and a transaction. Connection identifiers are ports or sockets that label each frame so the receiving device knows which process it has been sent from. This helps in keeping track of multiple-message conversations. Ports or sockets address multiple conservations in the same location. For example, the first line of a postal address is analogous of port and distinguishes among several occupants of the same house. Computer applications listen for information on their own ports and therefore more than one network-based application may be used at the same time. The transaction identifiers deal with the request or response frames. They are one-time events.

Self Assessment

Give one word for the following statements:

1. It is the amount of time when an acknowledgement is received from the destination machine to which a connection is requested. Obviously, lesser is the delay, better is the service.
2. Due to congestion in the network, lack of availability of space in table, some internal problem etc, causes the connection not to set within the establishment delay.
3. The transport layer for creating and releasing the connections across the network includes naming mechanism so that a process on one machine can indicate with whom it wishes to communicate.
4. When transport layer receives large message from session layer, it breaks the message into smaller units depending upon the requirement.
5. IETF working group had proposed the integrated services (IS) model based on outbound bandwidth policies for predictable resources in the network.
6. A policy framework that describes the quality of a specific stream of data in terms of bandwidth, buffer usage, priority, CPU usage, etc.
7. It is the capability of the transport layer to terminate a connection itself spontaneously in the case of congestion.

11.3 A Simple Transport Protocol

Some of the examples are:

- The Example Service Primitives
- The Example Transport Entity
- The Example as a Finite State Machine

Notes

11.3.1 The Example Service Primitives

The abstract service primitives also called as system calls are connection-oriented such as LISTEN, CONNECT, SEND, RECEIVE and DISCONNECT. They are listed below along with their functions:

LISTEN: Broadcast willingness to accept connections and provide queue size.

ACCEPT: Block the caller unless a communication attempt arrives.

CONNECT: Actively try to establish a connection.

SEND: Send data over the connection.

RECIEVE: Receive data from the connection.

CLOSE: Release the connection.

In the client server architecture, a machine (client) requests to another machine (server) to create a connection for providing some service. The services running on the server run on ports. The ports are application identifiers. The client machine should know the address of the server machine for getting the desired services from this port and to connect to the server machine. However, the server machine should not know the address or the port of the client machine at the time of connection initiation. The first packet transmitted by the client machine as a request to the server machine contains details about the client which are further used by the server to send any information. Client machine acts as the active device which makes the first move to establish the connection whereas the server machine passively waits for such requests from some client.

11.3.2 The Example Transport Entity

The transport layer uses the network layer primitives to send and receive TPDUs. The transport entity resides in:

- the host operating system kernel,
- a separate user process,
- a package of library routines running within the user's address space, or
- a co-processor chip or network board plugged into the host's backplane.

The interface to the network layer is given as below:

to_net(int cid, int q, int m, pkt_type pt, unsigned char *p, int bytes);

from_net(int *cid, int *q, int *m, pkt_type *pt, unsigned char *p, int *bytes);

The network layer packets that are used are given below:

CALL REQUEST: Sent to establish a connection

CALL ACCEPTED: Response to CALL REQUEST

CLEAR REQUEST: Sent to release a connection

CLEAR CONFIRMATION: Response to CLEAR REQUEST

DATA: Used to transport data

CREDIT: Control packet for managing the window

When information is passed as procedure parameters rather than the actual outgoing or incoming packet itself, the transport layer is shielded from the details of the network layer protocol. The

Notes

transport entity suspends transparently within *to_net* until there is room in the window. Apart from this transparent suspension mechanism, some explicit procedures called by the transport entity to block/unblock itself are given above:

- *sleep()* – This procedure is called when the transport entity logically needs to wait for an external event to happen. After calling the *sleep* procedure, the (main stream of the) transport entity is blocked.
- *wakeup()* – This procedure is called by the event handling procedure (i.e., *packet_arrival()*) – To unblock the sleeping (main stream of the) transport entity.

User programs call most of procedures in the transport entity directly. However, there are two procedures that are effectively (software) interrupt routines and are called only when the main stream of the transport entity is sleeping. They are given as below:

- *packet_arrival()* – This is triggered by the packet arrival event. The underlying network layer creates this procedure.
- *clock()* – The clock ticking event triggers this procedure.

A flow control mechanism based on credit is used in the example transport entity:

- When an application calls RECEIVE, a special credit message is sent to the transport entity on the source machine and is recorded in the conn array.
- When SEND is called, the transport entity checks to see if a credit has received on the specified connection.
  - If so, the message is transmitted in multiple packets, if needed, and the credit decremented;
  - If not, the transport entity changes itself to sleep until a credit receives.

In the transport entity, each connection is expresses in one of the following seven states:

Idle – Connection not established yet.

Waiting – CONNECT has been executed, CALL REQUEST sent.

Queued – A CALL REQUEST has arrived; no LISTEN yet.

Established – The connection has been established.

Sending – The user is waiting for permission to send a packet.

Receiving – A RECEIVE has been done.

Disconnecting – A Disconnect has been done locally.

11.3.3 The Example as a Finite State Machine

Figure 11.1 shows an example of finite state machine. In the finite state machine, each entry has an optional predicate, an optional action and the new state.

Task What is the difference between flow control and congestion control?

The key protocols of the Transport Layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP enables reliable data delivery service with end-to-end error detection and correction. UDP facilitates low-overhead, connectionless datagram delivery service. Both protocols are responsible for delivering data between the session layer and the network layer.

Notes

Figure 11.1: Example Finite State Model

		State						
		Idle	Waiting	Queued	Established	Sending	Receiving	Dis-connecting
Primitives	LISTEN	P1: –/Idle P2: A1/Estab P2: A2/Idle		–/Estab				
	CONNECT	P1: –/Idle P1: A3/Wait						
	DISCONNECT				P4: A5/Idle P4: A6/Disc			
	SEND				P5: A7/Estab P5: A8/Send			
	RECEIVE				A9/Receiving			
Incoming packets	Call_req	P3: A1/Estab P3: A4/Queu'd						
	Call_acc		–/Estab					
	Clear_req		–/Idle		A10/Estab	A10/Estab	A10/Estab	–/Idle
	Clear_conf							–/Idle
	DataPkt						A12/Estab	
	Credit				A11/Estab	A7/Estab		
Clock	Timeout			–/Idle				

Predicates
P1: Connection table full
P2: Call_req pending
P3: LISTEN pending
P4: Clear_req pending
P5: Credit available

Actions
A1: Send Call_acc
A2: Wait for Call_req
A3: Send Call_req
A4: Start timer
A5: Send Clear_conf
A6: Send Clear_req
A7: Send message
A8: Wait for credit
A9: Send credit
A10: Set Clr_req_received flag
A11: Record credit
A12: Accept message

11.3.4 User Datagram Protocol (UDP)

The User Datagram Protocol enables application programs to have direct access to a datagram delivery service like the delivery service that IP provides. This enables applications to exchange messages over the network with a minimum of protocol overhead. UDP is connectionless unreliable datagram protocol in which the sending terminal does not check whether data has been received by receiving terminal. The unreliable service indicates that there is no guarantee that the data reaches at the receiving end of the network correctly. It can be understood more clearly by Figure 11.2.

However, this protocol makes it possible to omit a variety of processes thus reducing the load on the CPU. UDP has 16-bit *Source Port* and *Destination Port* numbers. Figure 11.3 shows the data structure of the UDP header. The simplicity of the UDP header stems from the unsophisticated nature of the services it provides.

Figure 11.2: Comparison between TCP and UDP

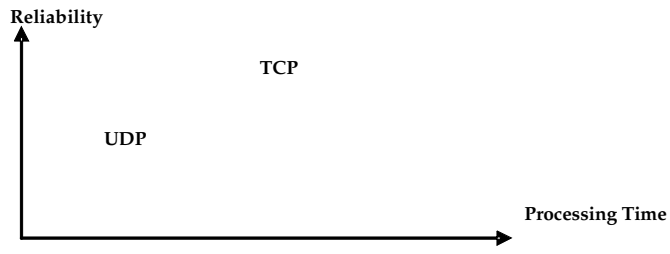
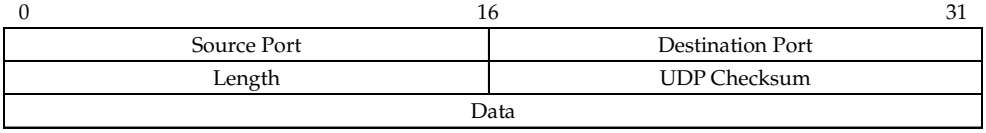
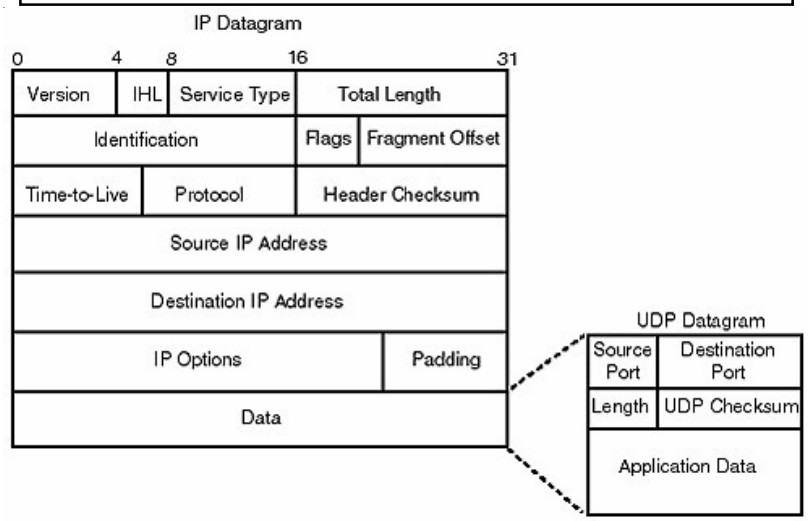


Figure 11.3: Format of the UDP Datagram



Notes

Figure 11.4: The Correspondence between the UDP and IP Datagrams



Following is a brief description of each field:

Source Port: Source port specifies port number of the application relating to the user data.

Destination Port: As it name indicates, this pertains to the destination application.

Length: It describes the total length of the UDP datagram, including both data and header information.

UDP Checksum: It gives an option of integrity checking.

At this point, it is important to understand the layering concept along with the need for headers. The relationship between the IP and UDP has been depicted in Figure 11.4.

Notes There are a number of good reasons for choosing UDP as a data transport service. When the amount of data being transmitted is small, UDP is considered the most efficient choice for a transport layer protocol because of the overhead for establishing connections and ensuring reliable delivery may be greater than the work of re-transmitting the entire data. Applications for a query-response model also work excellent for using UDP. The response is used as a positive acknowledgment to the query. When a response is not received within a certain time period, the application initiates another query.

Some examples of the usage of UDP are Remote file server (NFS), name translation (DNS), intra-domain routing (RIP), network management (SNMP), multimedia applications and telephony.

11.3.5 Transmission Control Protocol

Transmission Control Protocol (TCP) was designed to provide a reliable end-to-end data transfers over an unreliable internetwork in which TCP adapts properties of the internetwork dynamically. The internetwork may have different topologies, bandwidths, throughputs, delays, packet sizes, etc for different networks building up the internetwork. Each machine supporting TCP has a TCP entity that accepts user data streams from local processes and breaks them up into pieces not exceeding 64k bytes to transmit each piece as a separate IP datagram.

Notes

The TCP Service Model

TCP service model is consisting of sockets, which are used to create end points for TCP service at the host machines. It specifies the addressing format, the type of service and the protocol. Each socket possesses a socket number consisting of the IP address of the host and a 16-bit number local to that host which is referred as a port. Some of the well-known ports are 21 for FTP, 23 for telnet, 25for SMTP, 79 for finger, 80 for HTTP, etc. TCP provides a connection type service with full duplex point-to-point connection. That is, a logical connection must be established prior to communication. The TCP connection is byte stream instead of message stream. The TCP segment size is determined by the network's Maximum Transfer Unit (MTU), which is generally consisting of 1500 bytes. Because of this a continuous transmission of large amount of data is possible. It ensures a highly reliable data transmission for upper layers using IP protocol. This is possible because TCP uses positive acknowledgement to confirm the sender about the proper reception of data as shown in Figure 11.5. The sender keeps on send data at constant intervals until it receives a positive acknowledgement. A negative acknowledgment implies that the failed data segment needs to be retransmitted.

What happens when a packet is lost on the network and fails to reach its ultimate destination? When host A sends data, it starts a time down counter. If the timer expires without receiving an acknowledgment, host A assumes that the data segment was lost. Consequently, the sending computer retransmits a duplicate of the failing segment. The TCP protocol uses the sliding window protocol. Its other functions include sequence control, error recovery and control, flow control and identification of port number. The TCP has functionality to handle urgent or priority data. When some urgent data is received, the process ongoing at receiving machine is interrupted and instructed to read data stream to find the urgent data. The end of urgent data is always marked, so the process knows that it is over.

Figure 11.5: TCP Service Model

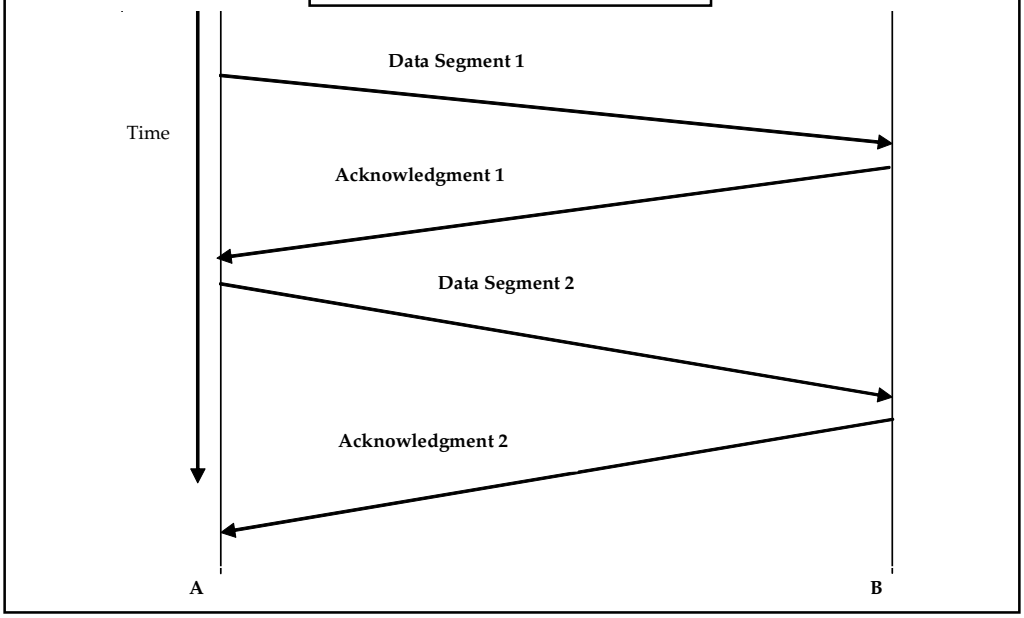


Figure 11.6 shows the format of the TCP data segment. The TCP header includes both source and destination port fields for identifying the applications for which the connection is established. The sequence and acknowledgment number fields underlie the positive acknowledgment and retransmission technique. Integrity checks are accommodated using the checksum field. TCP, therefore, unlike to UDP, TCP is a reliable connection-oriented byte-stream protocol.

TCP Protocol

Notes

Each byte on a TCP connection is comprised of its own 32-bit sequence number. The sending and receiving TCP entities transfer data in segments, which is determined by the TCP software. The TCP segment has a fixed 20-byte header followed by zero or more data bytes. The TCP functionalities support aggregation of data from several writes into one segment or split data from one write over multiple segments. The TCP segment should be such that it should fit into the MTU of each network. When a TCP segment is transmitted, a timer is also set. If the TCP segment timer goes off before the acknowledgement is received, the sender transmits the segment again. Therefore it is said that TCP is a reliable end-to-end delivery.

Reliable: TCP provides reliable delivery of data using *Positive Acknowledgment with Re-transmission* (PAR) mechanism. PAR is a mechanism where the data is transmitted again and again until it hears from the remote system that the data arrived correctly. The unit of data exchanged between source and destination host is called a *segment* as shown in the Figure 11.6. It is clear from the Figure 11.6 that each segment has a checksum to verify that the data arrives at the destination end undamaged. When the data segment is received undamaged, the receiver sends a *positive acknowledgment* back to the source end. When the data segment is damaged, the destination machine discards it. When the source machine does not receive any positive acknowledgement with in a specified time out period, it re-transmits the data segment.

Connection-oriented: TCP creates a logical end-to-end connection between the source and destination hosts. H*andshake* that is control information is exchanged between the source and destination hosts to set a dialogue before data is sent. TCP indicates the control function in a segment by setting the flag in a Flags field in the *segment header*. TCP uses a *three-way handshake* that indicates that three segments are exchanged. Figure 11.7 depicts the simplest form of the three-way handshake. Host *A* initiates the connection by transmitting host *B* a segment with the "Synchronize sequence numbers" (SYN) bit set. This segment indicates to host *B* that host *A* requests to create a connection. The segment also indicates to host *B* the sequence number host *A* will use as a starting number for its segments so that data can be put in the proper order. Host *B* replies to host *A* with a segment that has the "Acknowledgment" (ACK) and SYN bits set. Host *B's* segment acknowledges the receipt of *A's* segment and tells host *A* the Sequence Number host *B* will begin with. Finally, host *A* transmits a segment that acknowledges receipt of host *B*'s segment. Thus, host A transfers the first actual data.

This exchange of data also indicates to the TCP of host *A* has indication that the remote TCP is active and ready to receive data. When the connection is created, data can be exchanged. As soon as the source and destination machines have completed the data exchange, they initiate a three-way handshake with segments containing the "No more data from sender" bit (called the *FIN* bit) to release the connection. Thus, end-to-end exchange of data using the logical connection between the source and host machines is accomplished.

TCP Segment Header

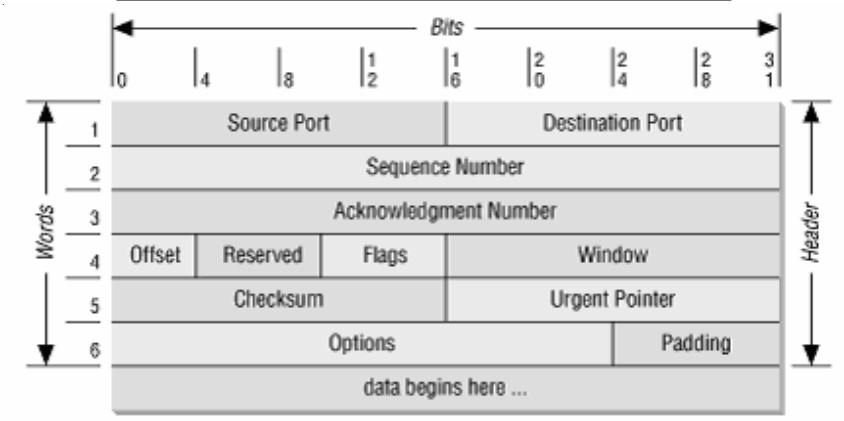
Figure 11.6 shows the layout of a TCP segment:

- ***Source and Destination Port (Socket) numbers:*** They together identify the connection between two hosts.
- ***Sequence and Acknowledgement number:*** These fields perform their functions and are 32 bits long because every byte of data is numbered in a TCP stream.
- ***TCP header length:*** It indicates how many 32-bits words are contained in the TCP header.
- ***Option Field:*** It is of variable length and includes the TCP header length.

Notes

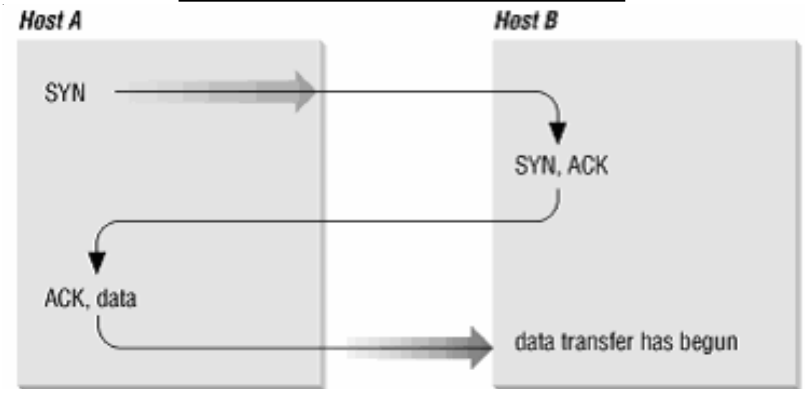
The segment header also includes a six 1 bit flags. Each bit indicates URG, ACK PSH, RST, SYN and FIN. URG field of the flag is set to 1 if the Urgent Pointer is in use, which indicates a byte, offset from the current sequence number at which urgent data are to be found. The ACK bit is set to 1 to indicate that the Acknowledgement number is valid. When ACK is 0, it indicates that the segment does not contain an acknowledgement so the Acknowledgement number field is ignored. The PSH indicates to push the data to a process upon arrival and not buffer it until a full buffer has been received. The RST bit is used to deny access to an invalid segment or refuse an attempt to open a connection. Sometimes because of a hot crash or some other reasons, the connection request is not clear. The SYN bit establishes a connection, if set to 1. The FIN bit indicates release of a connection after completion of transmission of data. The SYN and FIN segments have sequence numbers and are therefore processed in the correct order.

Figure 11.6: Data Segment Format of the TCP Protocol



Continuous Stream of Bytes: TCP considers the data it transmits as a continuous stream of bytes, not as independent packets. This necessitates TCP to take care to maintain the sequence in which bytes are sent and received. The sequence number and acknowledgment number fields in the TCP segment header keep track of the bytes. In order to keep track of the data stream correctly, each end of the processes are required to know the other end's initial number. The source and destination ends of the processes synchronize byte-numbering systems by exchanging SYN segments during the handshake. The sequence number field in the SYN segment has the Initial Sequence Number (ISN). This is considered the starting point for the byte-numbering system. Thereafter, each byte of data is numbered sequentially from the ISN to start with ISN+1 for the first real byte of data to be transmitted.

Figure 11.7: Threeway Handshake



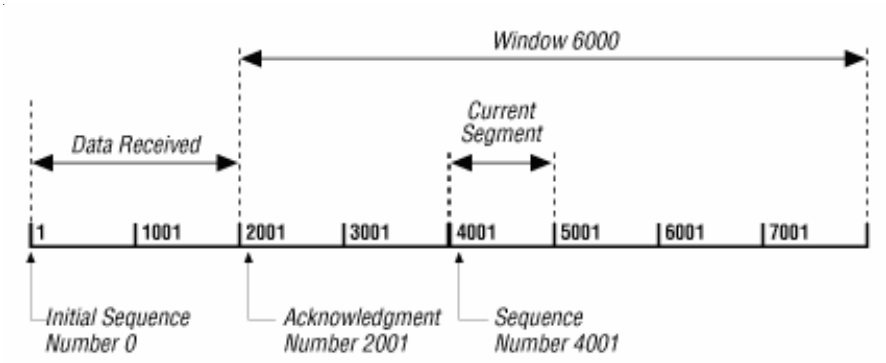
Notes

Flow control in TCP is handled by using a variable size sliding window protocol. The window fields indicate how many bytes may be sent starting art the byte acknowledgment. The acknowledgment segment (ACK) has positive acknowledgment and flow control functions. The acknowledgment indicates to the sender the amount of data received and the data, which can be received further. The acknowledgment number is the sequence number of the next byte the receiver is about to receive.

Figure 11.8 illustrates a TCP data stream that begins with an ISN of 0. The destination machine has received and acknowledged 2000 bytes. Therefore, the current acknowledgment number is 2001. The destination machine has enough buffer space for another 6000 bytes. The source machine is currently transmitting a segment of 1000 bytes starting with sequence number 4001. The source machine has received no acknowledgment for the bytes from 2001 onwards, but continues transmitting data as long as it is within the window. When the source machine fills the window and receives no acknowledgment of the data previously sent, it will, after time-out, transmit the data again beginning from the first unacknowledged byte. In Figure 11.8 re-transmission begins from byte 2001 when no further acknowledgments are received. This makes source machine to believe that data is reliably received at the remote locations of the network.

TCP also ensures for delivering data received from IP to the correct application. 16-bit port number identifies the application. The source machine and destination machine ports are included in the first word of the segment header. Thus, transport layer passes data to and from the application layer correctly.

Figure 11.8: TCP Data Stream



TCP Connection Management

The three-way handshake is used to create TCP connections in which the host machine executes a CONNECT primitive, specifying the IP address and port to which the connection is required, the maximum TCP segment size it is willing to accept and optionally some user data. The CONNECT primitive forwards a TCP segment with the SYN bit set to 1 and ACK bit set to 0 and waits for response. The sequences of events are illustrated in the Figure 11.8. The TCP entity at destination examines the segment when it reaches to the destination to ensure if there is a process that has done a LISTEN on the port that is provided in the Destination Port field. If not, it sends a reply with the RST bit on to reject the connection. The TCP connections are full duplex, which may be considered as a pair of simplex connections. A TCP segment with FIN bit set to 0 is sent by either of the hosts to release a connection when that host finishes of data to transmit. On the acknowledgment of FIN, the point-to-point connection from transmit side is closed. However, data may continue to flow indefinitely in other directions. When both directions are shutdown, the connection is released. To avoid unnecessary delay in receiving the

Notes

acknowledgement, timers are used. When a response to a FIN is not forthcoming within two maximum packet lifetimes, the sender of the FIN releases the connection. Eventually, the other host notices that nobody seems to be listening to it any more and that host also time out. The procedure followed for releasing and establishing a connection is represented as follows:

S. No	State	Description
1	CLOSED	Indicates no connection is active or pending.
2	LISTEN	The server is waiting for an incoming call.
3	SYN RECEIVED	A connection request has arrived; wait for acknowledgement.
4	SYN SENT	The application or process has started to open a connection.
5	ESTABLISHED	Indicates normal data transfer state.
6	FIN WAIT 1	The process or application has finished.
7	FIN WAIT 2	The hosts agreed to release the connection.
8	TIMED WAIT	Indicates wait for all packets die off.
9	CLOSING	Indicates that both hosts have attempted to close simultaneously.
10	CLOSE WAIT	One of the host has initiated a release.
11	LAST ACK	Indicates wait for all packets die off.

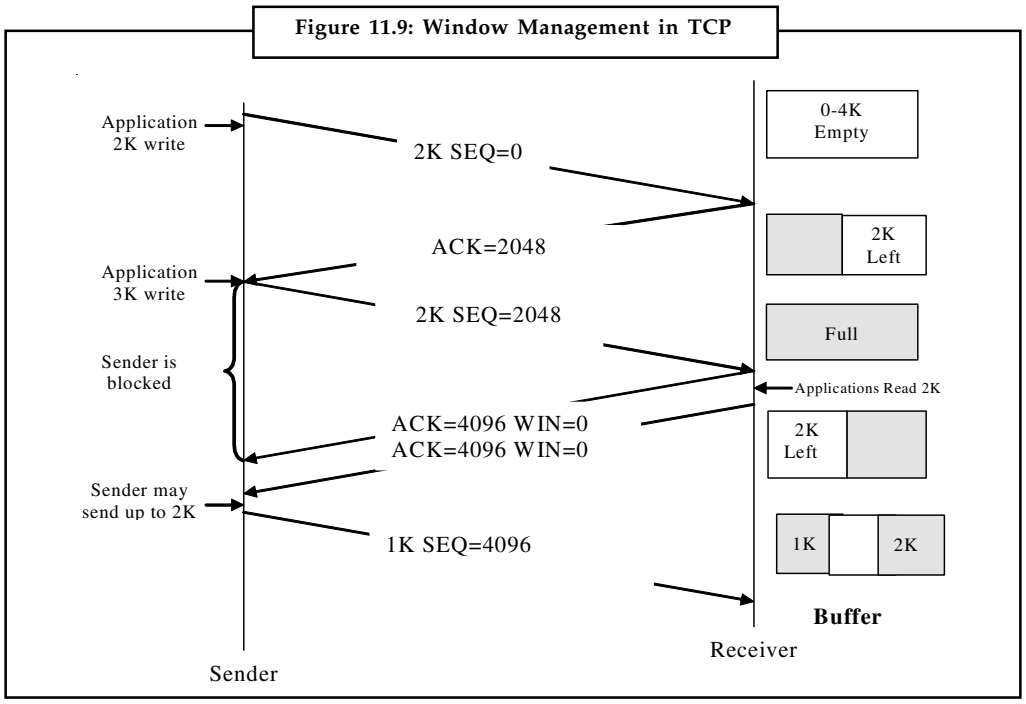
TCP Transmission Policy

Window management in TCP is not directly related to the acknowledgement. When the window is set to 0, the host machine at the sending end may not normally send segments. We may consider an example in which the receiving host has a 4096-byte buffer and sending host transmits a 2048-byte segment. The 2048-byte segment is correctly received and the receiving host acknowledges the segment. However, the buffer left with only 2048 of buffer space and the host at receiving side advertises a window of 2048 bytes starting at the next byte expected. Now the host at sending end transmits another 2048 bytes, which is acknowledged and the advertised window is 0. The host at sending end has to stop until the application process on the host at receiving end has removed some data from the buffer so that the TCP can advertise a larger window. It is observed if the window is zero, the host at sending side may not send segments. There are two exceptions. One of them is related to the urgent data that may be sent. Example of urgent data is to enable the host machine to finish the process running on the remote host machine. Figure 11.9 illustrates this concept.

Another exception is that the host machine at the sending may send a 1-byte segment to make the receiver re announce the next byte expected and the size of window. This is quite important in preventing deadlock if a window announcement ever gets lost. Senders are not required to transmit data immediately when they appear from the application as well as the remote host machine is not required to send acknowledgements as soon as possible. For example, consider a telnet connection to an interactive editor that reacts to every keystroke. In the worst case, if a character arrives at the TCP software, a 21-byte TCP segment is provided to IP to send as a 41-byte datagram. At the remote host machine at the receiving side, TCP returns a 40-byte acknowledgement (20-byte TCP header + 20-byte IP header). If the editor reacts to the character, it echoes it as a 41-byte packet, which is acknowledged with a 40-byte packet. Thus, 162 bytes and four segments are sent for each character typed. There are a number of issues that can degrade TCP performance. One of them is the *silly window syndrome* in which when data are passed in large blocks, but an application on the host machine at receiving side reads data one byte at a time. This is illustrated in Figure 11.9.

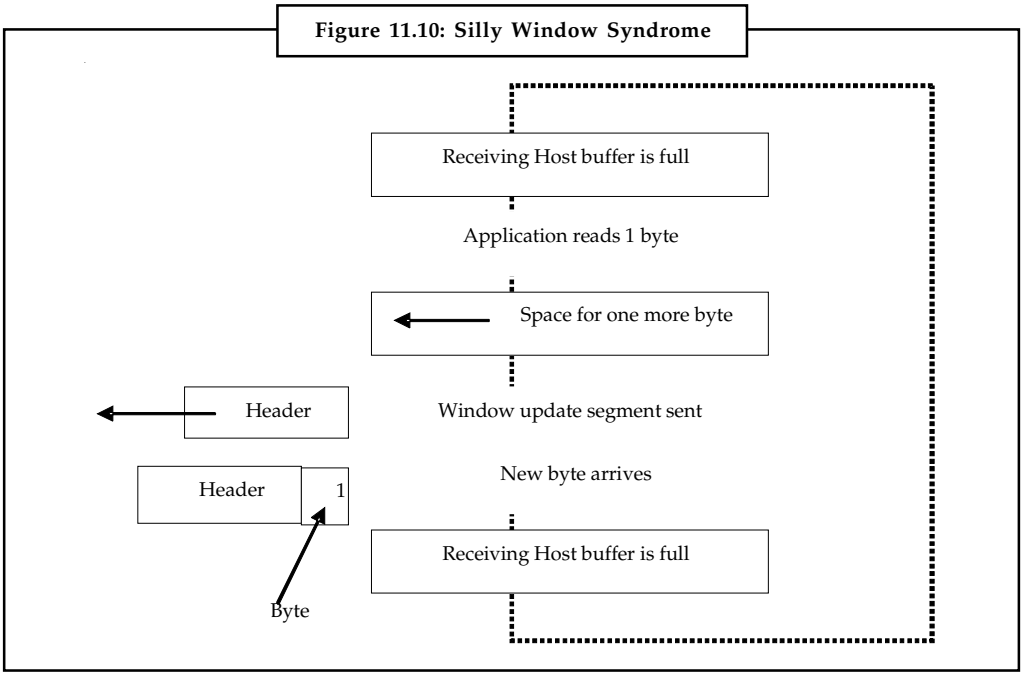
Notes

Figure 11.9: Window Management in TCP



The TCP buffer on the receiving side is full and the sending host knows this because the window size is set to zero. The process reads one byte. TCP forwards a window update of one. The sending host acknowledges and sends one byte. The buffer becomes full so the receiving host acknowledges the byte and sets the window size to zero.

Figure 11.10: Silly Window Syndrome



TCP Congestion Control

All Internet TCP algorithms are based on time-outs that are mostly caused by congestion due to network and receiving host capacity. The missing packets due to noise on the transmission lines

Notes

are rare nowadays. Each sending host happens to maintain two windows. One of them is the receiving host window indicating the receiving host capacity and another is the congestion window indicating the network capacity. The number of bytes to be transmitted should be the minimum of the 2 windows.

Initially the congestion window is the MTU that is increased to a double capacity on each burst successfully sent because an acknowledgement is received before the timeout is forwarded. This exponential increase is referred as the slow start that continues until the threshold, which is initially 64K, is reached. Thereafter, the increase is linearly with 1 MTU. If timeout happens, the threshold is set to half the current congestion window and the slow start is repeated. When an ICMP source quench packet comes in, it is treated the same way as a timeout.

TCP Timer Management

The retransmission timer intends to handle the large variation in round trip time occurring in TCP. The round trip time M is determined for each segment and the estimates of the mean and mean deviation are updated as:

Round trip time (RTT) = βRTT + (1-β)M

D = βD + (1-β) |RTT-M|

with β a smoothing parameter, typically 7/8. The timeout is then set to: RTT + 4 D

The Karn's algorithm does not update RTT and D for retransmitted segments. As an alternative, the timeout is doubled on each failure till the segments complete the first time. On receipt of a window size equals to 0, the persistence timer is used to guard against the lost of the next window update. Keepalive timer is also used in which if a connection is idle for a long time, the timeout causes a packet to be transmitted to check whether the other side is still alive. If the packet fails to respond, the connection is terminated. This feature, however is not recommended because it adds overhead and may terminate an otherwise healthy connection due to a transient network problem. The last timer is the one used in the TIMED WAIT state while closing, running for twice the maximum packet lifetime to make sure that when a connection is closed; all packets created by it have died off.

Self Assessment

Fill in the blanks:

8. TCP is an example of ……, reliable transport protocol.
9. The example of connectionless protocol is …….... Its advantage is low overhead.
10. A …… protocol set up a connection before it transmits information to a host.
11. The advantage of …… protocols are more reliable and keeps track of the delivery of the message.
12. The three errors that may be experienced and corrected by TCP service are lost frames; frames arrive out of order and …….. frames.

11.4 Summary

- Layer four of the OSI reference model is the transport layer that provides transparent transfer of data between the source and destination machines using the services of the network layer such as IP below to move PDUs of data between the two communicating machines.

Notes

- The transport layer is a true source-to-destination or end-to-end layer. The OSI Transport layer protocol (ISO-TP) manages end-to-end control and error checking to ensure complete data exchange. It provides "peer to peer" communication, with the transport entity of destination machine (remote peer).
- The transport layer provides a reliable on top of the unreliable services provided by the network layer. Option negotiation among different quality of service parameters renders an efficient, reliable and cost effective transport services to the user applications.
- Flow control manages data transmission between devices so that the transmitting device does not send more data than the receiving device can process. Multiplexing enables data from several applications to be transmitted onto a single physical link.
- Virtual circuits are established, maintained, and terminated by the transport layer. Error checking involves creating various mechanisms for detecting transmission errors, while error recovery involves taking an action, such as requesting that data be retransmitted, to resolve any errors that occur.
- Transport primitives are an effective way of exchanging data on top of network layer. The services provided at the transport layer appear to be similar to the services at the data link layer. However, they differ in many ways where data link layer provides connection between two routers using physical channel while the transport layer uses subnets.
- TCP is the protocol in the TCP/IP suite that provides reliable transmission of data. Applications that require the transport protocol to provide reliable data delivery use TCP because it verifies that data is delivered across the network accurately and in the proper sequence.
- UDP is a connectionless unreliable protocol that reduces load on the CPU's of the processes. The performance issues, which however, does not have scientific model to back them, are supported from experiences and examples. They attempt to address performance problems in computer networks, measuring network performance, system design for better performance, fast TPDU processing and protocols for future high-performance networks.

11.5 Keywords

Addressing: Transport Layer deals with addressing or labeling a frame.

Connection Establishment Delay: It is the amount of time when an acknowledgement is received from the destination machine to which a connection is requested. Obviously, lesser is the delay, better is the service.

Connection Establishment Failure Probability: Due to congestion in the network, lack of availability of space in table, some internal problem etc, causes the connection not to set within the establishment delay.

Connection Establishment/Release: The transport layer for creating and releasing the connections across the network includes naming mechanism so that a process on one machine can indicate with whom it wishes to communicate.

Demultiplexing: When several connections are multiplexed, they call for demultiplexing at the receiving end.

Differentiated Service: It refers to provide predictable performance in terms of delay, through put, packet loss, etc. for a given load at a given time.

Error Control: To control errors from lost or duplicate segments the transport layer enables unique segment sequence numbers to the different packets of message, creating virtual circuits, allowing only one virtual circuit per session.

Notes

Flow Control: The underlying rule of flow control is to maintain a synergy between a fast process and a slow process. Transport layer enables a fast process to keep pace with a slow one.

Fragmentation: When transport layer receives large message from session layer, it breaks the message into smaller units depending upon the requirement.

Integrated Services: IETF working group had proposed the integrated services (IS) model based on outbound bandwidth policies for predictable resources in the network.

Leaky bucket: The algorithm enables to control the rate at which data is injected into a network and thus handling burstiness in the data rate.

Multiplexing: To improve throughput, the transport layer establishes multiple network connections.

Protection priority: It is defined as the capability of the transport layer to provide Protection against third parties who try to interfere with the data. It specifies the priority of the important connections so that high priority connections are served before the low priority connections in the event of congestion.

Quality of Service: is defined as a policy framework that describes the quality of a specific stream of data in terms of bandwidth, buffer usage, priority, CPU usage, etc.

Re-assembly: When transport layer acts as receiving process, it reorders the pieces of message before reassembling them into a message.

Residual error Ratio: It is the fraction of the lost data with respect to the total data sent over the network by source machine.

Resilience: It is the capability of the transport layer to terminate a connection itself spontaneously in the case of congestion.

Traffic Management: The traffic management facility allows maximizing available network resources and ensures efficient use of resources that have not been explicitly allocated.

Transport Protocol Data Unit (TPDU): It is a term used for exchanging data from transport entity to transport entity.

Traffic shaping: Refers to the transmission of packets at uniform rate and in more predictable rate in case of open loop method.

Transport Service Primitives: They are used to access transport services by the application layer or the users.

Transit Delay: It is the time gap between a transmitted data from source machine to the reception of the same data by the destination machine. Like, throughput, for each communication link it is measured separately.

Throughput: It defines the number of bytes of user data transferred per second in a defined time interval. For each communication link it is measured separately.

Transmission Control Protocol (TCP): It enables reliable data delivery service with end-to-end error detection and correction.

User Datagram Protocol (UDP): It is connectionless unreliable datagram protocol in which the sending terminal does not check whether data has been received by receiving terminal.

11.6 Review Questions

1. How is transport layer different from data link layer when the services provided at both the layers are almost similar?

Notes

2. Why transport layer is required when both the network and transport layers provide connectionless and connection oriented services?
3. What are the different quality of services parameters at the transport layer?
4. Why UDP is used when it provides unreliable connectionless service to the transport layer?
5. What is the purpose of flow control?
6. Describe the TCP and its major advantages over UDP.

Answers: Self Assessment

1.	Connection establishment delay	2.	Connection establishment failure probability
3.	Connection Establishment/Release	4.	Fragmentation
5.	Integrated Services	6.	Quality of Service
7.	Resilience	8.	connection oriented
9.	UDP	10.	connection oriented
11.	connection oriented	12.	Garbage

11.7 Further Readings

Books

Achyut S Godbole and Atul Kahate published, *Web Technologies*, Tata McGraw Hill.

Andrew S. Tanenbaum, *Computer Networks,* Prentice Hall.

Behrouz A. Forouzan, Sophia Chung Fegan, *Data Communications and Networking,* McGraw-Hill Companies.

Douglas Comer, *Computer Networks and Internets with Internet Applications,* 4th Edition, Prentice Hall.

Ferguson P., Huston G., *Quality of Service: Delivering QoS on the Internet and in Corporate Networks*, John Wiley & Sons, Inc., 1998.

J. D. Spragins, *Telecommunications Protocols and Design*, Addison-Wesley.

McDysan, David E. and Darren L. Spohn. ATM Theory and Applications, McGraw-Hill Osborne Media, 1998.

Nassar, Daniel J., *Ethernet and Token Ring Optimization*. iUniverse.com, 2000.

Spurgeon, Charles E. Ethernet, *The Definitive Guide*. O'Reilly & Associates, 2000.

William A Shay, *Understanding Communication and Networks,* 3rd Edition, Thomson Press.

Notes

Unit 12: Application Layer

CONTENTS

Objectives

After studying this unit, you will be able to:

- Know how DNS is able to provide the quick translation of text of the IP addresses into corresponding binary numbers?
- Learn about e-mail and its various features
- Know Hyper Text Transfer Protocol and its role in accessing the websites
- Conceptualize the World Wide Web
- Understand the concept of multimedia and its elements

Introduction

The upper three layers namely session, presentation and application layers are considered as user or application layers of the OSI models. They are implemented in software. In most of the protocols, the functions of these layers are converged into a single layer called the application layer. TCP is one of the examples of such types of protocols. The application layer, the highest layer of OSI model interacts with software applications, which enable source and destination machines to communicate properly. It provides different services, which are described herein.

12.1 Domain Name System (DNS)

Notes

Now we have two types IP address in the form of decimal numbers and text for the same host. You know that list of all IP addresses are maintained centrally by ICANN in the form of distributed database directory. There are several distributed servers, which maintain this list of IP addresses. The reasons behind the distributed server are very logical and simple. It helps in disaster management and in diverting the load of the traffics in the form of requests from clients to other DNS servers located at different sites. DNS server maintains database in both the form that is textual as well as decimal notations. For example, DNS server maintains the address of google site as www.google.com and 216.23.9.53.99. In this manner, DNS is used to provide host-to-IP address mapping of remote hosts to the local hosts and vice versa. It is now amply clear that the DNS maintains a distributed database to map between hostnames and IP addresses. Whenever a client requests a service from a site, then both the site runs DNS protocol to access the distributed database which is nothing but Domain Name Systems. Therefore, the DNS provides the protocol, which allows clients and servers to communicate with each other. DNS enables a system to use a resolver, which resolves the host name to IP address understandable by server.

You may be now thinking of how DNS is able to provide the quick translation of text of the IP addresses within fraction of seconds from a directory of billions of such addresses. This could be made possible by using Domain concepts, which uses hierarchical arrangements of text addresses translation.

You can see from the Figure 12.1 that at the top level is the root server, which has null label. Below this is another level domain or domain as com, edu, int and so on which are grouped together. Below this different sub domains or groups have been created. Table 12.1 corresponds to some commonly appearing domain names with their respective sites. The DNS can accommodate almost all kinds of organizations by allowing each group to choose between geographical or organizational naming hierarchies.

Figure 12.1: DNS Hierarchy

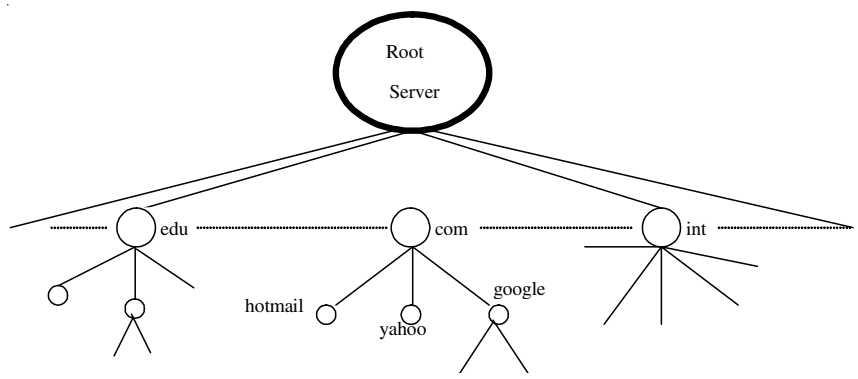


Table 12.1: Internet Domains

Domain	Indicative Site
Com	Commercial institute
Edu	Educational institute
Org	Nonprofit organization
Net	Network service provider
Gov	Government department

Contd...

Notes

Mil	Military
Biz	Business
Country code	For example, in for India, us for USA, au for Australia, jp for Japan and so on.

As we know that the servers maintaining addresses are distributed and have locations throughout the world. Then this question arises as to how text addresses are organized in hierarchical arrangement. You may refer Figure 12.1 above and Table 12.1. The hierarchy is represented into zones and each zones is a hierarchy of one or more nodes without any overlapping. Each zone is represented by a server and undoubtedly with one backup server. Root server as shown in Figure 12.1 is only one, which is just indicative; there may be several root servers at several locations in the world. Each root is aware of the location of each DNS server of specific domains.

The process is now very simple to understand. When you need to connect with a particular site, you first send your request to your local host. If your local host can provide the translation, your request is completed. If not, your local host then sends your request one level above in the hierarchy. If the server at one level above is able to handle the same, you get your intended website at your desktop through your local server. If not, then the server at one level above from your local server either sends your request again to another server or informs your local server that your request is failed and gives the address of another server to process your request. This process continues till a server is found who knows the address, otherwise, the request is filtered up to the root server. Depending upon the domain address, root server forwards the request to the one of the domain servers represented at the next level of hierarchy. This process continues and the information of text address is returned to Root server and then back to your local server.

12.2 Electronic Mail

Electronic mail is one of the most popular network services. The use of Electronic mail, or e-mail has probably may be cited as the foremost reason for the popularity of Internet. The proliferation of cyber café can be credited to e-mail or World Wide Web. E-mail provides an efficient and fast means of communication with relatives, friends or colleagues throughout the world. You cannot only communicate with one person at a time or thousands but also you can receive and send files and other information in a short time. In e-mail communication, the intended receiver or receivers of the message are not required to be present at their desktop at the time of receiving of the message by their computer. It works like a postal mail. In postal mail postman puts the sender's message in your mailbox and when you come back from your work, you access your mailbox to retrieve the message. Therefore, we may consider it in a way a substitute of postal mail. However, it has many-many more superior features than postal mail. E-mail has two parts:

User Agent: It is the user interface to the mail system. The user agent system enables to provide ways to view, edit, and reply to messages, etc. It also accesses messages stored in a system mailbox. The user agent enables the user to use a text editor to create a file that the user agent hands over to the message transfer agent.

Message Transfer Agent (MTA): It is a software package that transports messages created by a user to destination mailboxes possibly on remote machines. The MTA has to perform more complex jobs than other applications:

1. MTA handles temporary failures when a destination machine is temporarily unavailable; it stores the message on the local machine for later delivery. Thus, the User Agent typically just stores messages into a storage area.
2. MTA distinguishes between local and remote recipients.

Notes

3. MTA needs to deliver copies of a message to several machines.
4. MTA has to allow mixing text, voice, and video in a message and appending documents and files to a message.

As discussed above, the e-mail addresses consist of the following components:

Mailbox names: A mailbox is associated with one login id within a mail server to store the e-mails of the user. Therefore, a specific name is provided to the mailbox associated with each IDs.

Symbolic names: It refers to the name of a service rather than a specific user. For example, postmaster is universally recognized as an address for post mail problems. In e-mail system, the symbolic names are aliases for specific mailboxes.

Group names (mail exploders): It refers to an alias for a set of recipients. MTA consults an internal database to specify the mail addresses.

There are number of e-mail packages available. Some of them are free like Goggle's mail, Yahoo mail, hotmail etc while some are paid. All of them are also not alike but most of the e-mail software has some basic functionality common. These are:

- Send and receive mail messages
- Save your messages in a file
- Print mail messages
- Forward a mail message to other recipient
- Reply to mail messages
- Attach a file to a mail message

In order to send a message we need to first type the address of the intended recipient. E-mail addresses have some sort of similarity with phone numbers with regard to the identification of person, organization, or a geographic location. E-mail addresses likewise, telephone numbers, which have usually area code, have rules for use. Usually, the e-mail address has three parts:

1. A user identity or name
2. An "at" sign (@)
3. The domain name, which basically specifies the address of the user's mail server. It is the right most part of the address and follow a particular naming conventions. You can now understand the e-mail address by the help of the following example:-

Example - services@jalandhar.in

The left most part before the @ (at sign) is the identity or name if the user and the right most part after the @ is the server which indicates India. There are some naming conventions like edu, com, org etc used for education, commercial, organization respectively.

The Simple Mail Transfer Protocol is the de facto standard an electronic mail (e-mail) service provider. It is intended for the transfer of e-mail messages across the network. The protocol itself is simple because it uses the services of TCP where much of the hard work is handled by lower-level protocols. SMTP uses TCP transport for the reliable delivery of mail messages. For this purpose MTA opens a TCP connection to a destination location and sends the message to the destination at this location. The remote MTA at the mail server of remote location stores the message in its storage and returns an acknowledgment after it has saved the message successfully. Thereafter, the sender removes its copy. When the destination address is unavailable, the MTA

Notes

attempts to send message again later on. If a message event then cannot be delivered in specified days, the MTA returns an error to the user.

Briefly, when there is an outgoing mail, the SMTP client will connect to the SMTP server and sends the mail to the remote server. It uses simple and text-based protocol for one or more destinations of a message. SMTP server also allows telnet service. SMTP can be considered as a complement of UUCP. Machines connected together could very well transfer e-mails using UUCP but not the machine connected across a network all the time.

SMTP is also concerned with transferring mail from one MTA to another. The SMTP protocol is quite simple. It uses the query response model and only a few message types are defined. The other complex work is handled by TCP. SMTP commands consist of human-readable ASCII strings. A single TCP connection is used to serially process a set of message exchanges between a pair of hosts. SMTP never authenticates a sender. Initially, SMTP was implemented using Sendmail as the mail transfer agents in client server model. Subsequently, standard for binary file were included in addition to purely ASCII text-based standard. Multipurpose Internet Mail Extensions (MIME) standard were used to encode binary files for transfer through SMTP, which has now become a standard with its varied version. SMTP along with Post office Protocol (POP3) or Internet Message Access Protocol (IMAP) protocols allow retrieving mail from mail server.

Did u know? In other word, SMTP is a push kind of protocol while POP3 and IMAP are pull protocol.

Internet mail has an important advantage over other mail systems, for example, uucp or bitnet because Internet mail system provides an end-to-end reliable delivery system. In contrast to other mail systems, in the Internet mail system, all mail addresses have the same form: local-part@domain-name.

Self Assessment

Fill in the blanks:

1. SMTP commands consist of human-readable ……. strings.
2. A mailbox is associated with one login id within a …… to store the e-mails of the user.
3. …… refers to an alias for a set of recipients.
4. DNS server maintains database in both the form that is textual as well as ……... notations.
5. The …….. can accommodate almost all kinds of organizations by allowing each group to choose between geographical or organizational naming hierarchies.
6. …….. is a push kind of protocol while POP3 and IMAP are pull protocol.

12.2.1 Simple Mail Transfer Protocol (SMTP)

Electronic mail (E-mail) is considered the most widely used TCP/IP application. The Internet mail protocols enable a client machine to exchange mail and message between TCP/IP hosts. Three standard protocols are applied to provide such mail application. The SMTP is one of them. The three standards are given below:

1. ***SMTP:*** It is a standard for exchange of mail between two computers (STD 11/RFC 821), which specifies the protocol used to send mail between TCP/IP hosts.

Notes

2. ***Mail:*** It is a standard (STD 11) defining the format of the mail messages, syntax of mail header fields, a set of header fields and their interpretation and about a set of document types other than plain text ASCII to be used in the mail body.
3. ***DNS-MX:*** It is a standard for the routing of mail using the Domain Name System (RFC 974).

SMTP, an application layer protocol, is used to send e-mail messages across the Internet. It utilizes TCP as the transport protocol to send e-mail to a destination mail exchanger, referred as mail server. A client machine sends e-mail to a mail exchanger or an e-mail is sent from mail exchanger to another mail exchanger. E-mail transmitted using SMTP is normally transmitted from one mail exchanger to another directly. E-mail was never designed to be instantaneous but it appears so often.

Notes Mail Exchangers are nothing but the software application programs to support the SMTP protocol. Mail Exchangers such as sendmail or Microsoft Exchange wait for IP datagrams that arrive on the network interface with a TCP port number of 25. When a message is arrived, the mail exchanger checks to find out if it is for one of its users and accordingly move the mail to the user's mailbox. The data sent using SMTP is 7-bit ASCII data, with the high-order bit cleared to zero is found adequate in most instances for the transmission of English text messages but is inadequate for non-English text or non-textual data. To overcome these limitations, Multipurpose Internet Mail Extensions (MIME) defines a mechanism for encoding text and binary data as 7-bit ASCII within the mail envelope and SMTP Service Extensions specifies a mechanism to extend the capabilities of SMTP beyond the limitations.

How SMTP Works?

SMTP is end-to-end delivery in which an SMTP client machine contacts the destination host's SMTP server directly to deliver the mail. Unlike the store-and-forward principle that delivers the mail content to the destination host through a number of intermediary nodes in the same network, SMTP continues the mail content being transmitted until it has been successfully copied to the host's SMTP. In case of store and forward mechanism, the successful transmission from the sender only indicates that the mail content has reached the first intermediate hop. There are instances when mail is exchanged between the TCP/IP SMTP mailing system and the locally used mailing systems. Such applications are referred as mail gateways or mail bridges. However, SMTP guarantees only delivery to the mail-gateway host, not to the real destination host, which is located beyond the TCP/IP network. In case of a mail gateway, the SMTP end-to-end transmission is host-to-gateway, gateway-to-host or gateway-to-gateway. SMTP does not specify the format of mail beyond the gateway.

Each message of SMTP contains the following fields:

- A header or envelope that is terminated by a null line.
- *Contents* - Everything after the null or blank line is the message body with sequence of lines containing ASCII characters.

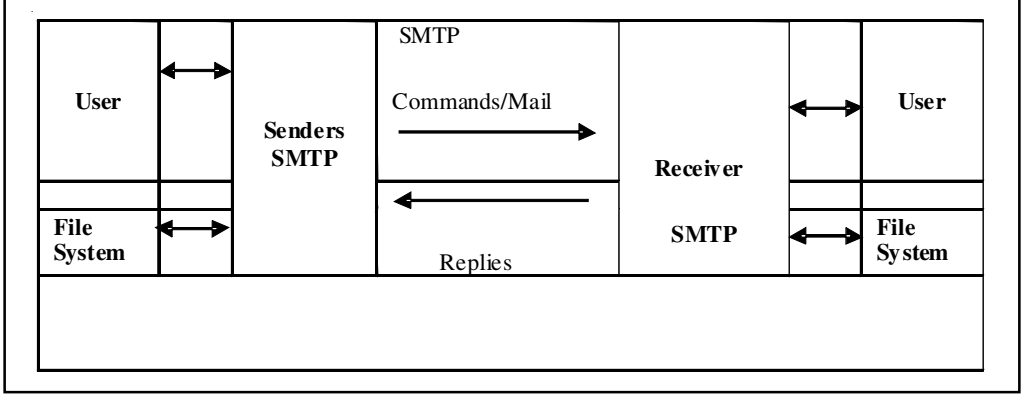
Simple Mail Transfer Protocol defines a client/server protocol. The client SMTP machine initiates the session by sending SMTP message and the mail server responds by receiving SMTP message to the session request.

Notes

12.2.2 Mail Exchange

The SMTP design is based on the model of communication illustrated Figure 12.2. After the client machine mail request, the sender-SMTP sets a two-way connection with a receiver-SMTP. The receiver-SMTP may be the destination machine or an intermediate machine (mail gateway). The sender-SMTP will initiate commands which are replied to by the receiver-SMTP.

Figure 12.2: SMTP Communication



1. The client machine SMTP sets a TCP connection with the destination machine SMTP and then waits for the server to send a service ready message or a service not available message.
2. HELO (HELO is an abbreviation for hello) is sent and the receiver machine will identify itself by sending back its domain name. The client machine SMTP uses this to verify if it reached the right destination SMTP. If the client machine SMTP supports SMTP Service Extensions, it substitutes an EHLO command in place of the HELO command. A destination machine SMTP which does not support service extensions responds with a 500 Syntax error, command unrecognized message. The client machine SMTP then retries with HELO, or if it cannot transmit the message without one or more service extensions, it should send a QUIT message. If a receiver-SMTP supports service extensions, it responds with a multi-line 250 OK message which includes a list of service extensions which it supports.
3. The client machine now initiates the start of a mail transaction by sending a MAIL command to the destination machine. This command has the reverse-path that is used to report errors. It should be noted that a path is more than just the user mailbox@host domain name pair. Besides, it has a list of routing hosts.
4. The next step of the actual mail exchange provides the server SMTP with the destinations for the message; the message may go to more than one recipient. This is accomplished by sending one or more RCPT TO:<forward-path> commands. Each of them will receive a reply 250 OK when the destination is known to the server or a 550. No such user here when it is not known to the server.
5. When all RCPT commands are sent, the sender forwards a DATA command to notify the destination machine that the message contents are following. The server replies with 354 Start mail input, end with <CRLF>.<CRLF>. It should be noted that the ending sequence that the client machine uses to terminate the message data.
6. The client machine now sends the data line by line ending with the 5-character sequence <CRLF>.<CRLF> line upon which the destination machine acknowledges with a 250 OK or an appropriate error message when anything went wrong.

Notes

7. Now, there are several possible actions:

   - The destination machine has no more messages to transmit, it will end the connection with a QUIT command. This command is answered with a 221 Service closing transmission channel reply.
   - The destination machine has no more messages to transmit, but it is ready to receive messages (if any) from the other side. It will issue the TURN command. The two SMTPs now switch their role of sender/receiver and the client machine that was previously the destination machine now transmits messages by starting with step 3 above.
   - The client machine wants to transmit another message and simply follows step 3 to transmit a new MAIL command.

Task List the advantages and disadvantages of SMTP.

12.3 World Wide Web

You must be very much familiar with the term World Wide Web, which is also known as web or WWW or W3 and has established itself as the most popular part of the Internet by far. It is an incredible mines of information, once you start searching anything ranging from documents to pictures to software, it almost appears limitless. It provides you documents, sound files, view images, animation, and video, speak and hear voice, and view programs that run on practically on any software in the world. Therefore, it facilitates the rich and diverse communication by enabling you to access and interact with text, graphics, animation, photos, audio and video. It has now become so simple for you to understand how the web works and what it is. Its implementation is based on client server system and employs your personal computer as client, web browser software, a connection to an Internet service provider, servers, routers and switches to direct the flow of information. You may be aware of all terms used in the formation of a web except web browser.

A browser is software, which your computer uses to view WWW documents and access the Internet. The browser program residing in your computer facilitates you with the advantages of text formatting, hypertext links, images, sounds, motion, and other features. Internet Explorer and Netscape are some of the widely used browsers. Browsers have sub programs called plug-ins to handle the documents you find on the Web. It may also other plug-ins stored elsewhere in your computer.

Web is very simple to use. Whenever you wish to visit any website, say your institute's website, you simply enter the address or URL of the website in your web browser to forward your request to the web server of the institute to provide you the intended web-page. The institute's web server then sends your request on the Internet to find the intended website. Once it is obtained, the web server returns the same to your computer where the browser loaded with different plug-ins interprets the data, displaying it on your computer screen. The intended webpage, which is now available on your desktop, may have click able links. On clicking on the same, you may visit other pages. In this manner, the information scattered across the globe can be linked together.

It now becomes essential to explain as to how the different webpages with different text format and standards could be linked to a particular web page. The binding forces that hold the Web

Notes

together are the hypertext and the hyperlinks. The hyperlink allows electronic files on the Web to be linked so you can jump easily between them using hypertext protocol. As you have learnt that web browsers that enables you to access the Web also distinguish between web pages and other types of data on the Internet because web pages are written in a computer language called Hypertext Markup Language or HTML.

Hypertext: The operation of the www is based on hypertext through which it interacts with web users or web browsers. Like normal text, the hypertext can be stored, read, searched or edited. It differs from the normal text that hypertext contains connections within the text to other documents. The hypertext links are used to create hyperlinks that can further create a complex virtual web of connections. The hypertext enables the web user to go forward or back, get much more detail on the current topic, change direction and navigate in any way that the web user desires wile surfing webpages instead of following text in a liner fashion like a book. This is possible because hypertext has text with pointers to other text.

Hypermedia: It is hypertext with some differences. The hypermedia documents not only provide links to other pieces of text, but it also provides link to other forms of media like sounds, images and movies. In other words, the hypermedia is used to combine hypertext and multimedia.

Caution Hypermedia and hypertext are similar in concept but yet different. Hypermedia is considered as a superset of hypertext.

12.3.1 WWW Functioning

World Wide Web is software that works in the client-server architecture in which web browser is a web client and web server that serves requests raised by the web client is called the server. The client is a browser like Internet Explorer, Netscape Navigator or Mozilla. Browsers are used to interact with the server using a set of instructions called protocols. These protocols facilitate in the accurate transfer of data through requests from a browser and responses from the server. Many protocols exist on the Internet for communication among several hosts. The World Wide Web is a part of the Internet and puts all these protocols under one group. They may be HTTP, FTP, Telnet, e-mail etc. The www employs a connectionless protocol.

The client server model uses a distributed architecture in which a client program may be running on a completely separate machine from that of the server possibly in another room or even in another country. In such case, the task of document storage is left to the server and the task of document presentation is left to the client so that each program can progress independent to each other. The web client is invoked and the web user selects a hyperlink in a piece of hypertext connecting to another document. The web browser uses the address associated with that hyperlink to connect to the web server at a specified network address and requests for the document.

The server responds back by sending the text and any other media within that text to the client browser, which the browser presents on the user's screen. The World Wide Web involves thousands of such virtual transactions per hour across the world and thus creating a web of information flow. The web servers are being equipped with encryption and client authentication abilities in which they will be able to send and receive secure data. The protocol used by the web clients and web servers to communicate with each other is called the HTTP. The webpages that are returned back use a programming language known as the Hypertext Markup Language (HTML).

Notes

12.3.2 Browser Architecture

A web browser is composed of three parts. They are controller, client programs and interpreters.

Controller: The controller obtains input from the keyboard or the mouse to access web-pages with the help of client program. After accessing the webpages, the controller uses one of the interpreters to display the web pages on the host screen.

Client Programs: They are used to establish TCP session with the web server or proxy server. The client programs use HTTP, FTP, Gopher or Telnet.

Interpreters: They are used to display the webpages on the web user's screen. The interpreters, which are used to translate web pages on the client's screen, are HTML, CGI or JAVA. They depend on the type of document. The HTML, which is a markup language and allows browser to change the format of the webpages, is used scripting web pages. The HTML also enables to store instructions with the text so that any browser can read the instructions and format the text according to the host machine being used.

Documents in the World Wide Web are classified into three types. They are static, dynamic and active documents.

Static Webpage: They are fixed content documents and always provides the same information in response to all download requests from all web users. Static documents are stored in a web server to be accessed by the web client. The web client while requesting a webpage gets a copy of it. The contents of the file are determined when it is created and not when it is used. However, the webpages can be modified in the server but the web user does not have right to alter them. Thus, the static webpages displays the same information for all web users from all contexts and provides hypertext links to perform navigation through static documents. The advantages of using static web pages are that they are cachet friendly in which one copy can be displayed to many people and provide ease to put them quickly even by someone who does not have much experience. However, they become difficult to maintain when a site gets large and difficult to keep consistent and up to date.

***Dynamic Webpage*:** They provide interactive web navigation and enable to modify the content like text, images, form fields, etc. on a webpage based on different contexts or conditions. The dynamic web pages use two types of interactivity:

1. ***Client side scripting:*** It us used to modify interface behaviors within a specific web page based on the mouse or keyboard actions or at specified timing events. The dynamic behavior happens within the presentation. The presentation technologies like JavaScript or ActionScript for dynamic HTML (DHTML) and Flash for media types of the presentation are used. The client side scripting also enables use of remote scripting in which the DHTML page requests additional information from a server. The content is generated on the web client's machine in which the web browser retrieves a page from the server and processes the code embedded in the webpage so that the contents of the retrieved can be displayed to web user. In the client-side dynamic pages, some web browsers do not support the language or they do not support some of the commands of the scripting language.
2. ***Server side scripting:*** It is used to modify the requested webpage source between pages to either adjust the sequence or reload of the web pages delivered to the browser. Server responses are based on certain conditions like data in a posted HTML form, parameters in the URL, the type of browser being used, the passage of time or a database or server state. Server side scripting dynamic webpages are designed with the help of server-side languages like PHP, Perl, ASP, JSP, etc.

Notes

Both of the above techniques may also be used concurrently to develop dynamic webpages. The advantages of dynamic webpages are that it enables easy update of the webpages and faster webpage loading. In dynamic webpage, the content and design are located separately and thus allowing frequent modifications to the web pages including text and image updates.

Active documents: The program that runs at the client side are known as the active documents. Whenever a web client requests an active document, the web server provides a copy of the document in the form of byte code. The document is now ready to run at the web client machine. As the active document is served in the binary form therefore it can be applied compression and decompression at server and client side to reduce the bandwidth requirement and throughput.

12.3.3 Hypertext Markup Language (HTML)

HTML is the standard language used by the WWW for creating and recognizing hypermedia documents. The webpages are written in HTML code and HTML files are saved with the suffix ".html". The HTML documents are standard 7-bit ASCII files with formatting codes that contain information about layouts, hyperlinks etc and users may control visual elements like fonts, font size, paragraph spacing, etc without changing the original information. Conversion software is used to translate documents from other formats into HTML. The documents in any language can be presented on the web by converting them into HTML format with the help of numbers of software available easily. There are filters available on web to convert files in RTF (Rich Text Format), WordPerfect and FrameMaker as well as mail archives and text-only documents. The HTML standard is used to support basic hypermedia document creation and layout. However HTML is limited in handling many complex layout techniques found in traditional document publishing. It can support interactive forms, defined "hot spots" in images, more versatile layout and formatting options and styles, formatted tables, etc. HTML+ enables the user to include an e-mail hyperlinks to send e-mail automatically in which selecting an e-mail address in a piece of hypertext would open a mail program, ready to send e-mail to that address. The characteristics of the HTML as a markup language is enable a user to embed formatting instructions in the file itself, which are stored with the text so that any browser can read the file itself.

12.3.4 Uniform Resource Locators (URL)

The WWW is not possible without Uniform Resource Locators (URLs). They are used to represent hypermedia links and links to network services within HTML documents. Any file or service on the Internet can be presented with a URL. The first part of the URL that comes before the two slashes is used to specify the method of access or protocol being followed for communications between browser and web server. The second part coming after two slashes represents the address of the host machine to which data or service is being sought. The other parts following the second part may specify the names of files, the port to connect to or the text to search for in a database. All the parts of an address for obtaining a file or service from a host machine in a URL are shown as a single unbroken line with no spaces and the locations of the host machines or websites that run www servers are typically named with a www at the beginning of the network address. In accessing web services, the web browsers enable the user to specify a URL and connect to that document or service. When the user gets connected with web serve, the user by selecting hypertext in an HTML document sends a request to open a URL. Thus, hyperlinks are used not only to provide other texts and media in the same document but also to provide other network services. Web browsers are not simply web clients. They are full-featured FTP, Gopher and telnet clients.

Common Gateway Interface

The Common Gateway Interface (CGI) is used as a standard protocol for interfacing external application software with a web server in which the web server responds to the request sent by

Notes

the web browser. In other words, it may understood as a connection between web server and webpages. The request may be for a file stored on the disk of webserver or an executable command and possibly arguments. CGI is used to provide responses for the second request type namely request for an executable commands. Therefore, CGI is inclusive of the web server and is used to communicate with other programs running on the web server. The CGI enables web user to ask questions and run applications in an interactive manner. The CGI is used to create web pages based on web user interaction in which the web users are able to read random pages on the website, create pages specific to them based on the form input and generate pages based on databases. Some of the CGI applications are interactive forms processing, gateways programming, etc. Gateways are also known as web gateways and are programs or scripts to access information that is not directly readable by the web client.

In its simplest form a web server receives request from the web client and responses back to the web client with requested web pages through HTTP program without processing the data of the web client. Sometimes the web client needs web server-side processing of the data. In many case web server also does not allow providing data verbatim. Such cases prompt the web client to send a fill-in HTML form to obtain data from the web server. Therefore to initiate data processing and manipulation at web server side, another program and a mechanism to forwards data to another program are required. Such secondary programs enabling data processing at web server are known as gateway programs. As its name implies, they act as a gateway between the web and other resources on the HTTP server machine like databases. The gateway programs are also used to return the processed data to the web client.

Normally, the CGI programs and scripts reside in a special directory, called cgi-bin. When a web user opens a URL associated with a CGI program, the web client sends a request to the web server asking for the file. Recognizing that it is a CGI program, the web server executes the program instead of returning the file contents exactly. When the CGI program begins running, it either creates and output a new document or provides the URL to an existing one. Thereafter, the CGI program sends the newly created data either directly to the web client or indirectly through the web server. When the output consists of a complete HTTP header, the data is sent directly to the web client without web server modification. Alternatively, the output is sent to the web server as a data stream and the web server then appends the complete header information and using the HTTP protocol to transfer the data to the client. The header is consisted of the details like type of communication protocol, the date and time of the response, the server name and version and the revision of the MIME protocol. MIME is a Multipurpose Internet Mail Extensions specification that is used for sending multiple types of data through e-mail. In brief the basic approach of CGI can be grouped into two categories. They are sending data to the gateway program and returning data to the web client. The disadvantage of CGI Scripts is to generate lot of loads on a web server and poorly written programs tend to fall into endless loops at the cost of the web server processor time. Such endless loops continue until a system administrator comes in and shuts off the faulty script. The browser based scripting tools use the processor locally instead of the Web server itself and so is less intense on the Web server.

Java

Java is a high-level third generation programming language to write computer applications. The Java shares lots of C's syntax but it is quire different from C language. The uniqueness of Java language is that it provides special programs called applets. The applets are downloadable from the Internet and can be played safely within a web browser. Java is a platform independent language for application development. It is so called because Java programs produce a special format called byte code written in hexadecimal byte by byte, which looks like machine language codes and are verbatim same on every platform. However, Java programs compiled into byte code needs an interpreter to execute them on any given platform. The Java provides automatic memory allocation and de-allocation to make it simple and bug free language. Some of the features of Java language are given as below:

Notes

- Java is Object-Oriented programming and therefore, it is simpler and easier to read programs. It provides more efficient reuse of code.
- Java is platform independent language in which a Java program never really executes natively on the host machine. Instead, a special native program called the Java interpreter reads the byte code and executes the corresponding native machine instructions.
- Java is considered safe and secure execution of code across a network, even when the source of that code was untrusted and possibly malicious.
- Java is high performance language in which Java byte codes are compiled on the fly to code while C++ uses just-in-time compiler. The native-machine-architecture compilers for Java are used to produce executable code that does not require a separate interpreter.
- Java is multi threaded and a single Java program can have many different threads executing independently and continuously.
- Java is garbage collected in which memory is allocated as needed and reclaimed by the garbage collector when it is no longer needed.

Self Assessment

State whether the following statements are true or false:

7. A browser is software, which your computer uses to view WWW documents and access the Internet.
8. The hyperlink allows electronic files on the Web to be linked so you can jump easily between them using FTP protocol.
9. The hypermedia documents not only provide links to other pieces of text, but it also provides link to other forms of media like sounds, images and movies.
10. The www employs a connection oriented protocol.
11. The protocol used by the web clients and web servers to communicate with each other is called the HTTP.
12. Documents in the World Wide Web are classified into five types.
13. The static webpages displays the same information for all web users from all contexts and provides hypertext links to perform navigation.
14. The dynamic web pages use three types of interactivity.
15. Server side scripting dynamic webpages are designed with the help of server-side languages like PHP, Perl, ASP, JSP, etc.

12.4 Multimedia

As the name suggests, multimedia is a set of more than one media element used to produce a concrete and more structured way of communication. In other words multimedia is simultaneous use of data from different sources. These sources in multimedia are known as media elements. With growing and very fast changing information technology, Multimedia has become a crucial part of computer world. Its importance has realised in almost all walks of life, may it be education, cinema, advertising, fashion and what not.

Throughout the 1960s, 1970s and 1980s, computers have been restricted to dealing with two main types of data - words and numbers. But the cutting edge of information technology

Notes

introduced faster system capable of handling graphics, audio, animation and video. And the entire world was taken aback by the power of multimedia.

Multimedia is the holy grail of networking. It brings immense technical challenges in providing (interactive) video on demand to every home and equally immense profits out of it.

Literally, multimedia is just two or more media. Generally, the term of multimedia means the combination of two or more **continuous media**. In practice, the two media are normally audio and video.

12.4.1 Multimedia Elements

There are many types of multimedia components. These are audio, video, pictures, animations, etc.

1. ***Text:*** Inclusion of textual information in multimedia is the basic step towards development of multimedia software. Text can be of any type, may be a word, a single line, or a paragraph. The textual data for multimedia can be developed using any text editor. However to give special effects, one needs graphics software which supports this kind of job. Even one can use any of the most popular word processing software to create textual data for inclusion in multimedia. The text can have different type, size, color and style to suit the professional requirement of the multimedia software.
2. ***Graphics****:* Another interesting element in multimedia is graphics. As a matter of fact, taking into consideration the human nature, a subject is more explained with some sort of pictorial/graphical representation, rather than as a large chunk of text. This also helps to develop a clean multimedia screen, whereas use of large amount of text in a screen make it dull in presentation.

Notes There are several graphics packages available to develop excellent images and also to compress them so that they take lesser disk-space but use higher resolution and more colours. Packages like Adobe PhotoShop, Adobe Illustrator, PaintShop Pro etc. are excellent graphics packages. There are Graphics gallery available in CD's (Compact Disk) with readymade images to suit almost every requirement. These images can directly be incorporated into multimedia development.

3. ***Animation:*** Moving images have an overpowering effect on the human peripheral vision. Followings are few points for its popularity.
   (a) Animation is a set of static state, related to each other with transition.
   (b) Indicates dimensionality in transitions
   (c) Illustrates change over time
   (d) Multiplexes the display
   (e) Enriches graphical representations
   (f) visualizing three-dimensional structures
4. ***Audio:*** The representation, processing, storage and transmission of audio signals are a major part of the study of multimedia systems. The frequency range of the human ear runs from 20 Hz to 20K Hz. The ear is very sensitive to sound variations lasting only a few milliseconds. The eye, in contrast, does not notice changes in light level lasting only a few

Notes

milliseconds. So, jitter of only a few milliseconds during a multimedia transmission affects the perceived sound quality more than it affects the perceived image quality.

5. ***Video:*** The human eye has the property that when an image is flashed on the retina, it is retained for a few milliseconds before decaying. If a sequence of images is flashed at 50 or more images/sec, the eye does not notice that it is looking at discrete images. All TV systems exploit this property to produce moving pictures.

   Currently, video is good for:

   (i) Promoting television shows, films, or other non-computer media that traditionally have used trailers in their advertising.

   (ii) Giving users an impression of a speaker's personality.

   (iii) Showing things that move. For example, a clip from a motion picture. Product demos of physical products are also well suited for video.

12.4.2 Uses of Multimedia

Placing the media in a perspective within the instructional process is an important role of the teacher and library professional. Following are the possible areas of application of multimedia:

- Can be used as reinforcement
- Can be used to clarify or symbolize a concept
- Creates the positive attitude of individuals toward what they are learning and the learning process itself can be enhanced.
- The content of a topic can be more carefully selected and organized
- The teaching and learning can be more interesting and interactive
- The delivery of instruction can be more standardized.
- The length of time needed for instruction can be reduced.
- The instruction can be provided when and where desired or necessary.

12.5 Summary

- The uppermost layer of OSI models provides a number of services to the users using the TCP/IP protocol. The Socket interface is used to provide a standard, well-documented approach to access kernel network resources.
- TCP/IP applications operate at the application or process layer of the TCP/IP hierarchy and split an application into server and client components.
- Domain Name System (DNS) provides the quick translation of text of the IP addresses within fraction of seconds from a directory of billions of such addresses. This could be made possible by using Domain concepts, which uses hierarchical arrangements of text addresses translation. The servers maintaining addresses are distributed and have locations throughout the world.
- Electronic mail is one of the most popular network services and uses user agent and message transfer agent to transport messages created by a user to destination mailboxes possibly on remote machines. Multimedia applications have enthused life in webpages making them interactive. The convergence of different media such as text, pictures, video and sound into a single media has contributed enormously for the growth of Internet and www.

Notes

- Applications of multimedia packages are found in all walks of life. With the advancement and innovation in presentation tools of multimedia, the multimedia applications have been giving impressions of virtual reality to its end users.
- Simple Mail Transfer Protocol (SMTP) is used to transfer mails from one computer system to another computer system attached to the same network or different networks and uses end-to-end delivery in which an SMTP client machine contacts the destination host's SMTP server directly to deliver the mail.
- The HTTP uses TCP transport service through sockets to transfer the data. The HTTP client initiates the TCP connection by using sockets on port 80 to the HTTP server. After accepting the connection from the client, the server response back to the client requests with the HTML pages and the objects. Thus, HTML pages and other objects are exchanged between the client browser and web server. After serving the client request, the TCP connection is terminated.
- Multimedia is nothing but the processing and presentation of information in a more structured and understandable manner using more than one media such as text, graphics, animation, audio and video.

12.6 Keywords

Browser: A browser is software, which your computer uses to view WWW documents and access the Internet.

Client: A client is a software entity within client machine that initiates a service request from a server.

Client Server Architecture: The client server architecture includes a host machine that makes a request to connect to another host machine for making available some services.

Cookies: Cookies that are small piece of data stored into the client's disk are used to identify the web browser.

Datagram Sockets: They are used for connectionless communication in which reliability is not important.

Domain Name System (DNS): It provides the protocol, which allows clients and servers to communicate with each other. DNS enables a system to use a resolver, which resolves the host name to IP address understandable by server.

Electronic Mail: It refers to the electronic version of the postal mail that uses user agent and message transfer agent to transport the message at the destination mailboxes. Multimedia.

Hyper Text Transfer Protocol: HTTP is a network protocol which is used to access any website.

HTTP Connections: Two types of HTTP connections are non-persistent (HTTP/1.0) and persistent (HTTP/1.1).

HTTPS: The HTTPS is a secure version of HTTP and indicates to use the port 443 instead of port 80.

Iterative: A client program is said to be running iteratively when it runs one by one.

Multimedia: Multimedia means the combination of two or more continuous media.

Non-persistent HTTP: This connection works on an individually established TCP connection for each object to be delivered by the HTTP server.

Persistent HTTP: The persistent HTTP connection enables the same TCP connection to be used for sending and receiving multiple HTTP requests and responses.

Notes

Processes: Program and process are distinct. A program is code that describes all the variables and actions to be performed on those variables while a process is an instance of the program.

Proxy Server: The proxy server acts like as a buffer between the client's web browser and the web server to provide the web browser's request without involving the original web server.

Raw Sockets: They are designed for applications like ICMP or OSPF that directly use the services of IP in such cases neither stream socket nor datagram socket be used.

Reserved Ports: The port numbers 0-1023 are reserved for the superuser and remaining ports starting from 1024 are for other users.

Round Trip Time (RTT): It is the time taken to send a packet to web server and receive a response from the web server.

Server: Like client, server is also a software entity that runs on a remote machine and provides requested services to client machines.

Simple Mail Transfer Protocol (SMTP): Enables a client machine to exchange mail and message between TCP/IP hosts.

12.7 Review Questions

1. Write a short note on DNS.
2. What are HTTP connections and how do they differ?
3. What are different types of user server identification? Explain them briefly.
4. How is www different from Internet? Explain.
5. How does SMTP work in transferring mails from one computer system to another computer system attached to different networks?
6. What is a web server? How does it function?
7. Describe the differences and similarities between a URL and an e-mail address.
8. Describe how e-mail is stored and transmitted by POP and SMTP servers.
9. Explain the concept of multimedia? What are the various components of multimedia?

Answers: Self Assessment

1. ASCII
2. mail server
3. Group names/mail exploders
4. decimal
5. DNS
6. SMTP
7. True
8. False
9. True
10. False
11. True
12. False
13. True
14. False
15. True

12.8 Further Readings

Notes

Books

Andrew S. Tanenbaum, *Computer Networks,* Prentice Hall.

Behrouz A. Forouzan, Sophia Chung Fegan, *Data Communications and Networking,* McGraw-Hill Companies.

Burton, Bill, *Remote Access for Cisco Networks,* McGraw-Hill Osborne Media.

Online links

http://www.boutell.com/faq/books.htm

Web Tutorials on HTML and Front Page

Notes

Unit 13: Session Layer and Presentation Layer

CONTENTS

Objectives

After studying this unit, you will be able to:

- Explain the concepts of session layer and related design issues
- Conceptualize the synchronization points as an effective mechanism for handling flow control and errors
- Describe the services offered by the presentation layer and related design issues

Introduction

The upper three layers namely session, presentation and application layers are considered as user or application layers of the OSI models. They are implemented in software. In most of the protocols, the functions of these layers are converged into a single layer called the application layer. TCP is one of the examples of such types of protocols.

The session layer is located above the transport layer and intends to provide value added services to the underlying transport layer services. The session layer creates, manages and releases communication sessions between presentation layer entities at source and destination machines. Session layer's protocols manage the communication sessions including creating a communication session service requests and service responses, security and authentication. They take place between applications located at source and destination machines in network. Protocol Data Unit (PDU) is the data at this layer. This layer responds to service requests from the presentation layer and issues service requests to the transport layer.

The presentation layer preserves and maintains the meaning of information transmitted across a network. It encodes the data in various ways, for example, data compression or encryption. Similarly, the receiving machine will convert the encoding back into its original form. The application layer, the highest layer of OSI model interacts with software applications which enable source and destination machines to communicate properly.

13.1 Session Layer – Design Issues

Notes

The session layer is thinnest layer with least numbers of protocols in the OSI model. The session layer aims to establish, maintain and synchronize dialogs between communicating upper layers. The communication may take place between either users or applications.

The functions of the session layers are as follows:

- ***Session to transport communication:*** To coordinate connection and release of connection of dialogs between the communicating applications.
- ***Dialog Management:*** To coordinate who sends when.
- ***Activity Management:*** To make sure that the data transfer is complete before the session closes.
- ***Synchronization:*** To provide synchronization points for data transfer.

Session to Transport Communication: The session layer helps to coordinate connection and release of connection of dialogs between the communicating applications, it communicates with the transport layer. The communication may be one to one, many to one and one to many. In one to one, one session layer connection establishes for each transport layer connection. In many to one, multiple session layer connections are shared with the services of one transport layer connection. The one to many connection communication is set up when one session layer connection calls for many transport layer connections to handle the service.

Dialog Management: Session layer aims to decide whose turn it is to talk. Some of the applications operate in half-duplex mode. The half duplex provides two sides alternate communication between sending and receiving messages and never send data simultaneously. The dialog management is implemented through the use of a data token which is transmitted back and forth to provide a user a right to transmit only when it possesses the token.

Activity Management: Session layer enables the user to delimit data into logical units called activities. Each activity is treated as a separate activity and independent from the preceding and following activities to that activity. Activities are used to delimit files of a multi-file transfer. Activities are used for quarantining, collecting all the data of a multi-message exchange together before processing them. The receiving application begins processing data only after all the data arrived. This ensures that all or none of a set of operations is performed. For example, a bank transaction may involve locking a record, updating a value, and then unlocking the record. When an application processes the first operation, but could not receive the remaining operations due to client or network failures. The record will remain locked forever. Quarantining solves this problem.

Exception handling: It is a general purpose mechanism for reporting errors.

Tasks

1. Define session layer.
2. What are the functions of session layer?

13.2 Session Layer – Synchronization

Many a times during data transmission, some sort of error may creep in due to various reasons, therefore the session layer aims to synchronise the data transmission so that the receiver receives the data unit as desired rather than in any distorted form. This requires synchronization.

Notes

For example, if you are performing a one-hour file transfer between two machines, and a network crash occurs approximately every 30 minutes, you might never be able to complete the file transfer. After each transfer aborts, you have to start all over again. To avoid this problem, you can treat the entire file transfer as a single activity with checkpoints inserted into the data stream. That way, if a crash occurs, the session layer can synchronize to a previous checkpoint. These checkpoints are called synchronization points.

There are two types of synchronization points: major and minor synchronization points. A major synchronized point inserted by any communicating side must be acknowledged by the other communicating side, whereas a minor synchronization point is not acknowledged. That portion of the session that is between two major synchronization points is called a dialog unit. The operation of managing an entire activity is called activity management. An activity can consist of one or more dialog units.

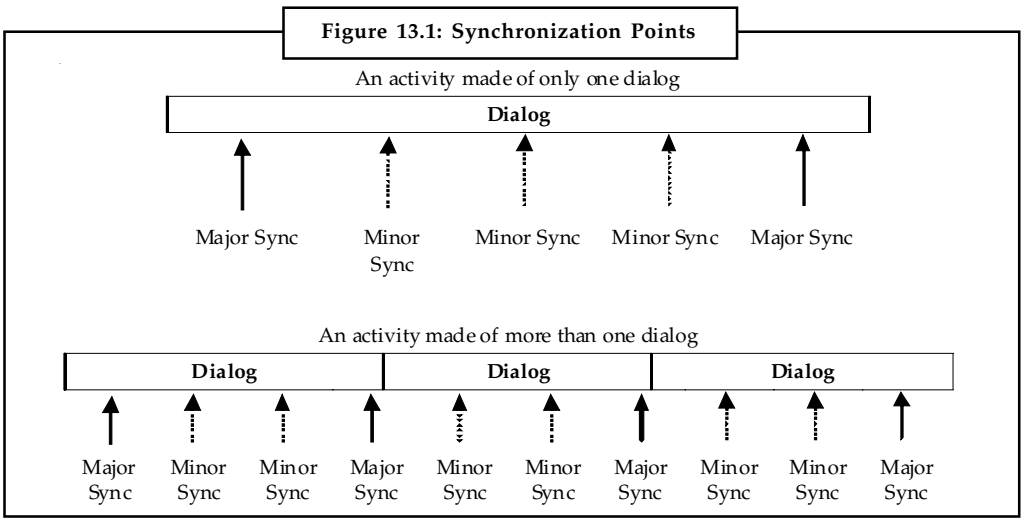
Synchronization is accomplished with the use of sequence numbers. The session layer protocols provide both major and minor synchronization points. Major synchronization points divide a message into a series of dialogs. Each major synchronization points are acknowledged before the session is continued. When an error happens, data is recovered only up to the last major point. A session layer activity is divided into a single dialog or several dialogs separated by major synchronization points. If resynchronizing, one only goes back as far as the previous major synchronization point. Besides, major synchronization points are acknowledged with the help of the explicit messages thus making their use expensive.

Minor synchronization points are just markers and inserted into the middle of dialogs. They, depending on the applications, may or may not require acknowledgement. They are security zones to recover the data from one or more minor synchronization points within a dialog when an error happens.

Notes It is to be noted carefully that major synchronization points are required to be acknowledged so that the control could begin retransmission of data from the point of last major synchronization points just before the point of occurrence of the errors. The minor synchronization points are used as security blankets and therefore do not need to acknowledge. When an error happens, the control goes back to one or more minor synchronization points to retransmit the data.

Figure 13.1 explains the concept of synchronization point lucidly.

Figure 13.1: Synchronization Points



Self Assessment

Notes

Fill in the blanks:

1. The …… layer is located above the transport layer and intends to provide value added services to the underlying transport layer services.
2. The …… layer preserves and maintains the meaning of information transmitted across a network.
3. The …….. layer is thinnest layer with least numbers of protocols in the OSI model.
4. Session layer enables the user to delimit data into logical units called ……
5. There are …… types of synchronization points.
6. Synchronization is accomplished with the use of …….. numbers.

13.3 Presentation Layer

The presentation layer in a network model is concerned with the syntax and semantics of the information exchanged between two systems.

The presentation layer determines how computers represent data format such as ASCII, GIF, etc and implements coding and conversion functions for application layer data to ensure that data sent from the application layer of source machine will be readable by the application layer of destination machine. The presentation layer coding and conversion methods provide common data representation formats, conversion of character representation formats, common data compression techniques and common data encryption techniques. Common data representation formats that may involve the use of standard image, sound and video formats allow to exchange the application data between different types of computer systems from source machine to destination machine. The machines interchanging data may use different text and data representations like EBCDIC and ASCII. The data compression techniques allow a compressed data at the source machine to be properly decompressed at the destination machine. Likewise, data encryption techniques allow data encrypted at the source machine to be properly decryption at the destination machine. Thus, the presentation layer makes the application layer free of the responsibility of syntactical differences in data representation within the source and destination machine or end user systems.

13.4 Presentation Layer – The Design Issues

The presentation layer deals with the translation, encryption/decryption, authentication and compression which are explained as below:

Translation: It converts the complex data structures used by an application strings, integers, structures, etc. into a byte stream that may be transmitted across the network. The message is represented in such a way that communicating machines agree to the format of the data being exchanged. For example, ASCII or EBCDIC character set.

The translation may be direct or indirect. In direct translation method, ASCII code is translated as the EBCDIC at the destination machine. In the indirect method, the ASCII code is first translated to a standard format at the source machine itself before transmission. The destination machine converts it into EBCDIC code. Direct method is not desirable with obvious reasons as the destination machine needs to deal with several computers in the network and therefore are required to have a table of conversion for different data formats. The indirect method that

Notes

includes Abstract Syntax Notation 1 (ASN.1) is recommended by OSI. This method takes care of formatting, diverse nature of data such as text, programs, etc. and the diversity in data storage format.

Abstract Syntax Notation

Abstract Syntax Notation (ASN.1) is an OSI standard dealing with the issue of representing, encoding, transmitting, and decoding data structures. It has two parts as given below:

1. An abstract syntax describing the data structures in an unambiguous manner. The syntax enables users to use integers, character strings, and structures instead of bits and bytes.
2. A transfer syntax describing the bit stream encoding of ASN.1 data objects. Data and additional fields are sent to describe the type of data. At the destination machine, the reverse operation is applied to convert from ASN.1 format to the internal representation of the destination machine.

There are alternative approaches to the data representation but they have disadvantages. In one approach, the source machine converts data into the format expected by the destination machine so that the destination machine does not need to perform any decoding. The disadvantage to this approach is that every source machine needs to know how to encode data for every possible destination machine. In another approach, ASN.1 converts everything into a common form similarly to the network standard representation of TCP/IP. However, the disadvantage of this method is that communication between two identical machines results in needless conversions.

ASN.1's abstract syntax is much like in form to that of any high level programming language. ASN.1 comprises of primitive types and complex types building on primitive types.

Encryption/Decryption: It deals with security and privacy issues. Encryption is used to scramble the data so that only authorized persons can unscramble the data of a conversation. Decryption reverses the encryption process to translate the message back into its original form. To encrypt the data, the sender in the source machine uses an encryption algorithm and a key to transform the plaintext (original message) into a ciphertext (encrypted message). At the destination machine, the reverse process takes place. The receiver has a key and decryption algorithm to translate back the ciphertext into the original plaintext.

Encryption and decryption methods are of two types. They are conventional and public key methods. In the conventional method, the encryption and decryption keys are the same and secret. The disadvantage of the conventional method is that the decryption algorithm is always the inverse of the encryption algorithm and therefore whoever knows the encryption algorithm will be able to deduce the decryption algorithm and thus the secrecy and privacy of message is threatened.

In the public key encryption approach, every user has the same key and algorithm for encryption of the message. However, the decryption algorithm and key are kept secret. Thus, the message could be encrypted by anyone; however, it could be decrypted by an authorized person. The decryption algorithm is designed in such a way that it could not be deduced from the inverse of the encryption algorithm. Also, different encryption and decryption keys make it difficult to decrypt the message by an unauthorized person.

Authentication: It verifies the antecedents of the remote party being the real party rather than an impostor. It means that the message is received from an authentic person not from an impostor. Digital signature is one of the several authentication approaches that use public key encryption method.

Data Compression: It compresses data to reduce the amount of transmitted data thus saving in bandwidth and money. There are three general methods to data compression. Each method

Notes

considers that the data stream may be transformed into a more compact representation. This compact data stream is reconstructed back into the original data at the destination machine.

Finite Set of Symbols: It is considered that a library with many branch offices in which the previous days transactions are transmitted to every other branch after closing. Transactions are comprised of checked out and returned books. The information could be exchanged in the following manners:

1. The name of the book, its author, the copy number, etc. together with the type of transaction are sent.
2. The library needs to maintain an office wise table assigning a unique ID number to every book in every branch. Transactions then refer to the book's ID number instead of its title. As the book IDs are small and contain few bytes, so less data will be transmitted.

Note: It may be noted from the above descriptions that the above technique is used throughout programming and pointers and array subscripts are frequently exchanged to avoid the cost of transferring large amounts of data between subroutines. It is also assumed that all objects occur with equal frequency and that the set of objects, books in this case, is finite. When text is examined, it is immediately noticed that some words appear more often than others. Taking cue from this, the number of bits could be reduced that are required to represent a document by using a coding scheme that employs small code words to represent common words and longer code words to represent words that appear infrequently.

Huffman Encoding: Huffman encoding is used to encode symbols according to the frequency of their use which is explained as below:

1. A set of nodes, one node per symbol with a node's value given by the probability of its occurrence in the data is created.
2. The two nodes having the smallest value are found. They are removed from the set and a new node having the two removed nodes as children are created. The new node is then assigned a value equal to the sum of its children's values. The new node is added back to the set of nodes.
3. Step 2 is repeated until only one node remains. This generates a tree, whose probability value is one.
4. The encoding for each symbol is done that is the path from the root to the symbol. A code 0 is used for a left child and 1 for a right child. Thus, the length of each symbol's encoding is proportional to the relative probability of its occurrence.

Did u know? The disadvantage of the Huffman encoding is that symbols have differing lengths so it becomes relatively expensive to decode. Also, a single-bit error will corrupt the entire message.

Context Dependent Encoding: It recognizes that the probability of a particular symbol occurring next depends on the previous symbol. For instance, the probability that a P directly follows M is about 4 times less than the probability of a Q following M. The drawback of conditional probability methods is the increase in table space. Each symbol needs its own table to give the codes for those symbols immediately following it. However, this approach has an advantage over Huffman encoding. It is that symbols are all fixed length and therefore makes encoding and decoding using table lookups very efficient. It is also more immune to transmission errors.

Run Length Encoding: Run length encoding is an alternative to encode data containing repetitive symbols. Let us assume binary strings of 0s and 1s. The long runs of 0 are handled by using a k-bit symbol that indicates how many 0 bits occurred between consecutive 1s. A code word of all

Notes

1's indicates that the true distance is $2^K - 1$ plus the value of the following symbols. Consider the following example:

000100001010011000000000000000000000001000000011 (48 bits) comprises of runs of length 3, 4, 1, 2, 0, 23, 7 and 0. Using 4-bit symbols, it is encoded as:

0011 0100 0001 0010 0000 1111 0100 0111, for 32 bits and a savings of 16/48 = 33%.

Using 3-bit symbols, it would be encoded as: 011 100 001 010 000 111 111 111 010 111 000 for 33 bits.

Self Asessment

Fil in the blanks:

7. Encryption/decryption is taken care of at …….. layer.
8. The …….. layer is responsible for establishing, maintaining, synchronizing and terminating dialogs.
9. The …….. layer disconnects a session abruptly, while the …….. layer provides for graceful closure.
10. …….. points recovers data that have been delivered but not yet used.
11. …….. is the major function of the presentation layer.

13.5 Summary

- The session layer is located above the transport layer and intends to provide value added services to the underlying transport layer services. The session layer creates, manages and releases communication sessions between presentation layer entities at source and destination machines.
- The session layer implements the mechanism for managing the dialogue between end-user application processes. It facilitates in creating either duplex or half-duplex operation to implement check-pointing, adjournment, termination, and restart procedures.
- The synchronization points which are introduced as reference points in the data control flow and error in the session layer.
- Major synchronization points divide a message into a series of dialogs. Each major synchronization points are acknowledged before the session is continued. When an error happens, data is recovered only up to the last major point.
- Minor synchronization points are just markers and inserted into the middle of dialogs. They, depending on the applications, may or may not require acknowledgement. They are security zones to recover the data from one or more minor synchronization points within a dialog when an error happens.
- The presentation layer deals with the translation, encryption/decryption, authentication and compression.
- Encryption is used to scramble the data so that only authorized persons can unscramble the data of a conversation. Decryption reverses the encryption process to translate the message back into its original form.

13.6 Keywords

Notes

Abstract Syntax Notation (ASN.1) is an OSI standard dealing with the issue of representing, encoding, transmitting, and decoding data structures.

Activity management enables the user to delimit data into logical units called activities.

Authentication verifies the antecedents of the remote party being the real party rather than an impostor.

Dialog management works towards to decide whose turn it is to talk.

Huffman encoding is used to encode symbols according to the frequency of their use.

Major synchronization points divide a message into a series of dialogs.

Minor synchronization points are just markers and inserted into the middle of dialogs.

Run Length Encoding is an alternative to encode data containing repetitive symbols.

Synchronization provides synchronization points for data transfer.

Translation converts the complex data structures used by an application strings, integers, structures, etc. into a byte stream that may be transmitted across the network.

13.7 Review Questions

1. Explain briefly the functions of the presentation layer.
2. What is the difference between minor synchronization points and the major synchronization points?
3. What are the elements of the presentation layer?
4. Explain the process of synchronization with respect to session layer.
5. Differentiate between session layer and presentation layer.

Answers: Self Assessment

1. session
2. presentation
3. session
4. activities
5. two
6. Sequence
7. Presentation
8. Session
9. Transport, session
10. Synchronization
11. Encryption

13.8 Further Readings

Books

Andrew S. Tanenbaum, *Computer Networks,* Prentice Hall.

Behrouz A. Forouzan and Sophia Chung Fegan, *Data Communications and Networking,* McGraw-Hill Companies.

Notes

Burton, Bill, *Remote Access for Cisco Networks*, McGraw-Hill, Osborne Media.

J.D. Spragins, *Telecommunications protocols and design*, Addison-Wesley, Reading MA.

Rajneesh Agrawal and Bhata Bhushan Tiwari, *Computer Networks and Internet*, Vikas Publication.

Unit 14: Network Security

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Explain various aspects of network security for TCP/IP network
- Discuss the possible issues for data security and how the same can be protected
- Analyze the importance of data encryption and related technologies
- Describe the concept of cryptography and its use in data security

Introduction

Over the past several years, the world has become interconnected in ways not previously imaginable. Small and large companies have presence on WWW and their offices spread across the globes have inter-office collaboration on a daily basis. Hence, all of these interconnections rely in large part on our ability to protect the networks that create those connections. Network security is a broad topic with multi-layered approach. It can be addressed at the data link layer, network layer and application layer. The issues concerned are: packet intrusion and encryption, IP packets and routing tables with their update version, and host-level bugs occurred at data link layer, network layer and application respectively.

Notes

The TCP/IP protocols are being used globally irrespective of the nature of the organizations whether it belongs to general category of organizations or security specific sensitive organizations. The news or information about hacking of some web site or portal by some undesired people is very common nowadays. This shows that TCP/IP protocols are susceptible to intercept. This generated a need to ensure all round security for the network in an organization. The task of network administrator had to widen to include the overall security of the network. He has to ensure that all parts of this network are adequately protected and adequate measures of security have been implemented within a TCP/IP network. He should be aware of an effective security policy. He should also be able to pinpoint the main areas of risk that the network may face. Basically, these main areas of risk vary from network to network depending upon the organization functioning. There are therefore various security related aspects, which have direct implications for network administrator along with the means to monitor the implemented measures of security effectively and to tackle the problem of breach of security if it happens.

14.1 Network Security

The main objective of the network is to share information among its users situated locally or remotely. Therefore, it is possible that undesired user can hack the network and can prove to be harmful for the health of the network or user. There are few basic points, which must be followed by network administrator to provide the network an adequate security other than network specific security as in case of e-commerce, etc. These are given below:

- Networks are designed to share information. Therefore, the network must be clearly configured to identify the shareable information and non-shareable information.
- The network should also clear with whom the shareable information could be shared.
- With the increase of system security, the price for its management will also increase accordingly; therefore a compromising level between security and prices should be established as per the requirement of the network security system policy. This will largely depend upon the level of security needed to apply in the network, overall security requirements and the effective implementation of chosen level of security.
- Division of the responsibilities concerning the network security must be clearly defined between users and system administrator.
- The requirements for security must be detailed within a network security policy of the organization that indicates the valuable data and their associated cost to the business.
- After defining the detailed network security policy and identifying the clear cut responsibilities in the organization, the system administrator should be made then responsible for ensuring that the security policy is effectively applied to the company environment, including the existing networking infrastructure.

14.4.1 Levels of Security

Did u know? The evolution of security levels can be looked into different form, contributed by the US Department of Defense. The first step in this direction was the describing of the Trusted Computer System Evaluation Criteria in December 1985 that is popular by the name as Orange Book. In continuation with the this Orange Book security level another security level known as Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria or Red Book was described in July 1987.

Notes

The security levels contain the security-related problems in the component or modular form. Each level contains the specific security problem, which is broken down into different divisions. Each of the divisions or classifications provides a representation of a security level defined in terms of the following general categories:

- User identification and authentication
- The capability to monitor and audit system activity
- Provision of discretionary access
- Control of the reuse of resources
- Identifying specific areas of possible attack
- Provision of suitable countermeasures
- The level of system trusts, including systems architecture, design, implementation, transport, and trust of other hosts.

14.2 Data Security

Data security concerns with the protection of data contained in a file or many files in a computer either as a standalone or on a network from unauthorized interception by providing some sort of security.

In case of postal system, a postcard as a carrier of information is open to all. It does not have any sort of security measures. An envelope is used to hide information from other people. It means that envelope here acts as a mean for security. Therefore, postcard and envelope has different purpose with respect to security issue. These two particular cases initiated similar actions to solve the security-related issues in case of data communication. Emails are open to all as post cards. Following the envelope example in postal system will enable users to secure at least some of their data.

The access protection provided by logon passwords are not a full proof system and these may easily be bypassed. The bypassed methods include booting from a diskette or connecting the stolen hard drive as a secondary one to another computer. In this manner, any vital data might easily be accessed. Consequently, encryption of the information seems to be the only effective way to protect data from going or intercepting by unauthorized persons. The encryption must be developed with the philosophy to ensure reliable data security and almost impossible to decrypt data without the right password or right user. The main drawback of the password-based encryption includes the loss of password or registration of wrong password due to wrong spelling or some other human mistakes. In this case, it becomes absolutely impossible to restore the data. There are other rules to avoid such situations.

14.3 Security Threats

The invalid access to the host can be prevented to a certain extent in case of conventional host to terminal as there is number of terminals connected is limited. The situation is entirely different in case of Internet where Internet allows access from any terminal connecting on a network. Therefore this requires proper security measures. Below is the list of some of the threats happening frequently in the network:

1. ***Viruses and Worms:*** The term virus refers specifically to malware inserting malicious code into existing documents or programs. It spreads itself by various means. Still viruses are considered the most common type of network security threat. Almost 90 percent of

Notes

viruses are spread through attachments on emails. However, a cautious user action may prevent the spread of virus because virus requires a user action to insert itself into a computer. It is therefore suggested that never open an email attachment, which is not expected, even though the sender appears to be known. However, this preventive measure will do little to stop worms from infecting the network because worms do not need a host file and they propagate themselves. When they infect a computer, they often make quick copies of it and infect an entire network within a few hours. To avoid attacks from viruses and worms, a latest version of anti virus software should be used.

2. ***Trojan Horses:*** This malware attack disguises itself as something innocent like a computer game or a search results page. Once installed on a computer, the Trojan horse may download and install a keylogger onto the infected computer to record every keystroke by a computer's user, thus stealing vital details of the users. They usually hide themselves in a downloadable free software on a website. The users should detest themselves from downloading freeware. It is often observed that organizations block free download software to prevent themselves from the attack of Trojan horses. Sometimes, a computer infected with Trojan horse are required to be reformatted, therefore, it is suggested that preventive steps need to enforced effectively than curing the infected computer system.

3. ***Spam:*** Spam constitutes 70 to 84 percent of daily emails sent throughout the world that demands an ever increasing need for IT resources to filter out this irritating and potentially malicious menace. Spam email comprises of unsolicited emails promoting products and coordinated spam attacks to consume so much bandwidth on a network so as to cause it to crash. Spam may use techniques "news service" spam, which uses legitimate news headlines to trick recipients into opening spam emails. Good email filters are used to filter the spams. And much of what slips through can be avoided by staying away not to trick with the emails. There should be check for signing of any online service or freebie. The naming system for creating email accounts should not be easily guessable because spammers are increasingly going through common name lists in order to harvest emails to spam.

4. ***Phishing:*** Emails with titles such as, "URGENT: Update Account Status" are all attempts by a spammer to "phish" the account details. The Phishing refers to spam emails to trick recipients into clicking on a link to an insecure website and provide details considering the website as genuine one. Typically, phishing attempts are carried out to steal account information for e-commerce sites such as banks, eBay or regular financial institutions' websites. A phishing email tricks the user to click a link, which will take the user to a page where the user is asked to re-enter all his or her account details including credit card number(s) and/or passwords. These websites are not actual site, even though they look like it. To protect the network, users should be cautious and detest themselves to opening and providing vital details requested by any financial institutions. They should confirm the integrity before supplying such details. Financial institution should also educate their employees about the most common ways in which hackers try to phish the account information.

5. ***Packet Sniffers:*** Packet sniffers are the technique used to capture data streams over a network to obtain sensitive data like usernames, passwords, credit card numbers, etc. Thus, packet sniffers are more malicious forms of threats to the network security. Packet sniffers monitor and record details that are coming from and going to a computer over a compromised network. To get access to a network, packet sniffer use honeypots. They are simply unsecured wifi access points that hackers create to trap users who are using them. Making users aware about the threat of packet sniffers is best prevention policy. A user should be aware not to access the Internet through an unsecured connection. Falling to packet sniffers technique will lead to compromise with sensitive network data. In addition, the user should use a variety of different sign on names and passwords to access various

Notes

levels of network security. This helps at the instance when login information is compromised, the damage can at least be limited in scope.

6. ***Maliciously-Coded Websites:*** Maliciously coded Websites create chartable websites enabling a user to make donations and thus stealing the vital personal information. Maliciously coded websites are also used to enter networks for installing keylogger. Information regarding some charitable institution should be obtained from security certified sites.

7. ***Password Attacks:*** A 'Password Attack' includes a number of techniques used by hackers to steal passwords. Some of them are listed below:

   - *Brute-force:* It is method in which a hacker tries to guess a password by repeatedly entering in new combinations of words and phrases compiled from a dictionary to steal the password. Developing difficult to guess usernames and passwords can prevent it.
   - *Packet sniffers*: It has been discussed above.
   - *IP-spoofing:* Like honeypots, IP spoofing involves the interception of data packets by a computer successfully pretending to be a trusted server/resource.

8. ***Zombie Computers and Botnets:*** 'Zombie' computer is a computer under seize of a spammer who has infected the computer attached to a network with malware so that it acts as a tool of a spammer by silently sending out thousands of emails from the owner's email address. Thus, an innocent user's computer sends thousands of spam messages without the knowledge of the user. The spammers organize zombie computers into small groups called 'botnets'. These 'botnets' then transmits spam including phishing attempts, viruses and worms. The botnets normally send spamming and phishing attacks.

9. ***Denial-of-Service attack (DoS):*** Denial-of-Service attack (DoS) is an attack method to deny the access to webpages of a website or network to the legitimate users.

14.4 Data Encryption

Encryption is a technique to hide data from unauthorized persons by encoding data so that it may not viewed and modified. The process of data encryption involves converting the data into encrypted data called ciphertext using a mathematical formula called an algorithm. These algorithms generate a key and then encapsulate the message with this key. Two types of encryptions such as asymmetric and symmetric are in vogue. The presentation layer deals with the translation, encryption/decryption, authentication and compression, which are explained as below:

14.4.1 Translation

It converts the complex data structures used by an application strings, integers, structures, etc. into a byte stream that may be transmitted across the network. The message is represented in such a way that communicating machines agree to the format of the data being exchanged. For example, ASCII or EBCDIC character set.

The translation may be direct or indirect. In direct translation method, ASCII code is translated as the EBCDIC at the destination machine. In the indirect method, the ASCII code is first translated to a standard format at the source machine itself before transmission. The destination machine converts it into EBCDIC code. Direct method is not desirable with obvious reason as the destination machine needs to deal with several computers in the network and therefore are required to have a table of conversion for different data formats. The indirect method that

Notes

includes Abstract Syntax Notation 1 (ASN.1) is recommended by OSI. This method takes care of formatting, diverse nature of data such as text, programs, etc. and the diversity in data storage format.

14.4.2 Encryption/Decryption

It deals with security and privacy issues. Encryption is used to scramble the data so that only authorized persons can unscramble the data of a conversation. Decryption reverses the encryption process to translate the message back into its original form. To encrypt the data, the sender in the source machine uses an encryption algorithm and a key to transform the plaintext (original message) into a ciphertext (encrypted message). At the destination machine, the reverse process takes place. The receiver has a key and decryption algorithm to translate back the ciphertext into the original plaintext.

Authentication refers to keep a secret of two persons secure from the third person. However, the non-repudiation requires to prove that even the sender could not have generated the message. To implement security issues as given above, a technique called cryptography is applied. Encryption is of two types:

1. ***Asymmetric Encryption:*** Two mathematically related keys namely public key and private keys are generated to encrypt and decrypt the message. Asymmetric encryption is considered more secure than symmetric encryption. Asymmetric key encryption that involves a key pair as public and private keys involves six major steps:

   (a) ***Plaintext:*** Plaintext is the text message to which an algorithm is applied.

   (b) ***Encryption Algorithm:*** It provides mathematical operations to conduct substitutions and transformations to the plaintext.

   (c) ***Public and Private Keys:*** They constitute a pair of keys which are used for encryption and decryption of the message.

   (d) ***Ciphertext:*** Application of algorithm on plaintext produces the encrypted or scrambled message.

   (e) ***Decryption Algorithm:*** This algorithm is applied to generate the ciphertext and the matching key to produce the plaintext.

   The encryption process converts the text message to a hash code by using a mathematical formula. This hash code is then encrypted with the help of the sender's private key. The private key is generated with the help of the algorithm.

   The encrypted hash code and the message are encrypted again using the sender's private key. Subsequent to this, the sender encrypts the secret key with the recipient's public key, so only the recipient can decrypt it with his or her private key.

   In the decryption process, the recipient using his or her private key long with the secret key to decipher the encrypted hash code and the encrypted message. The recipient then uses the sender's public key to decrypt the hash code and to verify the sender's identity. The recipient generates a hash code from the message. If thus generated hash code equals the hash code forwarded by sender, then this verifies that the message has not been changed on the way.

2. ***Symmetric Encryption:*** Symmetric encryption also referred to as conventional or single-key encryption is based on a secret key, which is shared by both communicating parties. The sending party encrypts the plain text to cipher text message using the secret key. The receiving party on receipt of the cipher text message uses the same secret key to decrypt it

Notes

to plain text. Examples of symmetric encryption are the RSA algorithm. Symmetric encryption method has the following five major parts:

(a) ***Plaintext:*** It is the text message to be transmitted on which an algorithm is applied.

(b) ***Encryption Algorithm:*** It enables mathematical operations to conduct substitutions and transformations to the plaintext.

(c) ***Secret Key:*** They constitute a part of algorithm for encryption and decryption of the message.

(d) ***Ciphertext:*** This is the encrypted message generated by applying the algorithm to the plaintext message using the secret key.

(e) ***Decryption Algorithm:*** This is the encryption algorithm that decrypts the cipher text into plain text by using the ciphertext and the secret key.

In the application of the symmetric encryption, the sender and receiver are required to exchange secret keys in a secure manner with the aid of a strong encryption algorithm.

14.4.3 Authentication

It verifies the antecedents of the remote party being the real party rather than an impostor. It means that the message is received from an authentic person not from an impostor. Digital signature is one of the several authentication approaches that use public key encryption method.

14.4.4 Data Compression

It compresses data to reduce the amount of transmitted data thus saving in bandwidth and money. There are three general methods to data compression. Each method considers that the data stream may be transformed into a more compact representation. This compact data stream is reconstructed back into the original data at the destination machine.

Finite Set of Symbols

It is considered that a library with many branch offices in which the previous days transactions are transmitted to every other branch after closing. Transactions are comprised of checked out and returned books. The information could be exchanged in the following manners:

1. The name of the book, its author, the copy number, etc. together with the type of transaction are sent.
2. The library needs to maintain a officewise table assigning a unique ID number to every book in every branch. Transactions then refer to the book's ID number instead of its title. As the book IDs are small and contain few bytes, so less data will be transmitted.

Notes The above descriptions that the above technique is used throughout programming and pointers and array subscripts are frequently exchanged to avoid the cost of transferring large amounts of data between subroutines. It is also assumed that all objects occur with equal frequency and that the set of objects, books in this case, is finite. When text is examined, it is immediately noticed that some words appear more often than others. Taking cue from this, the number of bits could be reduced that are required to represent a document by using a coding scheme that employs small code words to represent common words and longer code words to represent words that appear infrequently.

Notes

Self Assessment

Fill in the blanks:

1. In secret key encryption, the secret key is used for ..... .
2. In the public key encryption, the public key is used for ..... of the massage.
3. Encryption and decryption normally takes care of ..... of a network.
4. In public key encryption the private is used to ..... the message to the plaintext.
5. ..... involves the interception of data packets by a computer successfully pretending to be a trusted server/resource.

14.5 Cryptography

Substitution and transposition ciphers are two categories of ciphers used in classical cryptography. Substitution and transposition differ in how chunks of the message are handled by the encryption process.

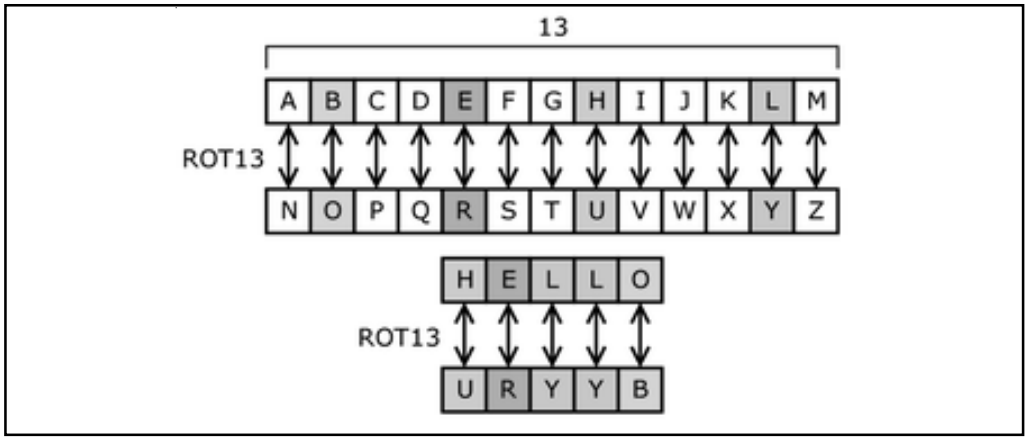
14.5.1 Substitution Ciphers

In cryptography, a substitution cipher is a method of encryption by which units of plaintext are replaced with ciphertext according to a regular system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution.

Substitution ciphers can be compared with transposition ciphers. In a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged. By contrast, in a substitution cipher, the units of the plaintext are retained in the same sequence in the ciphertext, but the units themselves are altered.

There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different times in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice-versa.

Simple Substitution



Notes

ROT13 is a Caesar cipher, a type of substitution cipher. In ROT13, the alphabet is rotated 13 steps.

Substitution over a single letter—**simple substitution**—can be demonstrated by writing out the alphabet in some order to represent the substitution. This is termed a **substitution alphabet**. The cipher alphabet may be shifted or reversed (creating the Caesar and Atbash ciphers, respectively) or scrambled in a more complex fashion, in which case it is called a *mixed alphabet* or *deranged alphabet*. Traditionally, mixed alphabets are created by first writing out a keyword, removing repeated letters in it, then writing all the remaining letters in the alphabet.

Examples

Using this system, the keyword "zebras" gives us the following alphabets:

Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Ciphertext alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY

A message of

flee at once. we are discovered!

enciphers to

SIAA ZQ LKBA. VA ZOA RFPBLUAOAR!

Traditionally, the ciphertext is written out in blocks of fixed length, omitting punctuation and spaces; this is done to help avoid transmission errors and to disguise word boundaries from the plaintext. These blocks are called "groups", and sometimes a "group count" (i.e., the number of groups) is given as an additional check. Five letter groups are traditional, dating from when messages used to be transmitted by telegraph:

SIAAZ QLKBA VAZOA RFPBL UAOAR

If the length of the message happens not to be divisible by five, it may be padded at the end with "nulls". These can be any characters that decrypt to obvious nonsense, so the receiver can easily spot them and discard them.

The ciphertext alphabet is sometimes different from the plaintext alphabet; for example, in the pigpen cipher, the ciphertext consists of a set of symbols derived from a grid. For example:

Such features make little difference to the security of a scheme, however – at the very least, any set of strange symbols can be transcribed back into an A-Z alphabet and dealt with as normal.

In lists and catalogues for sales people sometimes a very simple encryption is used to replace numeric digits by letters.

Plain digits: 1234567890

Ciphertext alphabet: MAKEPROFIT

Example: MAT would be used to represent 120.

Security for Simple Substitution Ciphers

A disadvantage of this method of derangement is that the last letters of the alphabet (which are mostly low frequency) tend to stay at the end. A stronger way of constructing a mixed alphabet

Notes

is to perform a columnar transposition on the ordinary alphabet using the keyword, but this is not often done.

Although the number of possible keys is very large (26! H" 288.4, or about 88 bits), this cipher is not very strong, being easily broken. Provided the message is of reasonable length, the cryptanalyst can deduce the probable meaning of the most common symbols by analyzing the frequency distribution of the ciphertext—frequency analysis. This allows formation of partial words, which can be tentatively filled in, progressively expanding the (partial) solution (see frequency analysis for a demonstration of this). In some cases, underlying words can also be determined from the pattern of their letters; for example, attract, osseous, and words with those two as the root are the only common English words with the pattern ABBCADB. Many people solve such ciphers for recreation, as with cryptogram puzzles in the newspaper.

Notes According to the unicity distance of English, 27.6 letters of ciphertext are required to crack a mixed alphabet simple substitution. In practice, typically about 50 letters are needed, although some messages can be broken with fewer if unusual patterns are found. In other cases, the plaintext can be contrived to have a nearly flat frequency distribution, and much longer plaintexts will then be required by the user.

14.5.2 Transposition Cipher

In cryptography, a **transposition cipher** is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

Following are some implementations:

Transposition ciphers encrypt plaintext by moving small pieces of the message around. Anagrams are a primitive transposition cipher.

This table shows "VOYAGER" being encrypted with a primitive transposition cipher where every two letters are switched with each other:

V	O	Y	A	G	E	R
O	V	A	Y	E	G	R

14.5.3 Substitution and Transposition Ciphers in Modern Times

Modern cryptanalysis makes simple substitution and transposition ciphers obsolete. However, these techniques remain useful for understanding cryptography and the workings of more complex modern ciphers.

Task Differentiate between substitution and transposition cipher.

Self Assessment

Notes

State whether the following statements are true or false:

6. Modern cryptanalysis makes simple substitution and transposition ciphers obsolete.
7. According to the unicity distance of English, 20 letters of ciphertext are required to crack a mixed alphabet simple substitution.
8. In substitution cipher, a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.
9. Traditionally, the ciphertext is written out in blocks of fixed length, omitting punctuation and spaces.
10. ROT13 is a Caesar cipher, a type of transposition cipher.

14.6 Summary

- Data on the network is not secret and therefore requires to be kept secure from undesirable persons sitting behind the machines attached to the network.
- The malicious intentions may include bringing down of servers attached to the network, using people's private information like credit card numbers for fraudulent activities and sabotaging of major organizations by accessing their websites. It is therefore aimed to secure data and prevent from eavesdroppers from listening to and stealing data. The user data on a computer is also protected by providing password restricted access to the data and resources so that only authorized people get to use these. Security aspects also involve identifying miscreants and thwarting their attempts to cause damage to the network among other resources.
- A*uthentication* involves verifying of the antecedents of the person who has requested for services from a remote machine or access to the remote machine either through physically or by sending an e-mail before allowing him or her to do so. Authentication involves a process to authenticate person's identity to a remote machine.
- ***Integrity*** involves the veracity of the message which is received by a remote machine. In other words, it is indeed the same message without any alteration which was sent by the source machine. In this case, cyclic redundancy code method will not be enough as intruders in the system or communication channel may deliberately alter the message. Security should ensure that nobody along the entire route should be able to alter the message.
- ***Confidentiality:*** It ensures that no person should be able to read the message on the way. This necessitates implementation of the encryption techniques down the line.
- The message is encrypted at the sender end and decrypted at the receiving end to maintain privacy with the help of the encryption and decryption techniques. The secret key and public key techniques are the available techniques with their advantages and disadvantages.
- Substitution and transposition ciphers are two categories of ciphers used in classical cryptography. Substitution and transposition differ in how chunks of the message are handled by the encryption process.

14.7 Keywords

Ciphertext: This is the encrypted message generated by applying the algorithm to the plaintext message using the secret key.

Notes

IP-spoofing: Like honeypots, IP spoofing involves the interception of data packets by a computer successfully pretending to be a trusted server/resource.

Maliciously: Coded Websites - Maliciously coded Websites create chartable websites enabling a user to make donations and thus stealing the vital personal information.

Packet Sniffers: Packet sniffers are the technique used to capture data streams over a network to obtain sensitive data like usernames, passwords, credit card numbers, etc.

Password Attacks: A 'Password Attack' includes a number of techniques used by hackers to steal passwords.

Phishing: Emails with titles such as, "URGENT: Update Account Status" are all attempts by a spammer to "phish" the account details.

Plaintext: It is the text message to be transmitted on which an algorithm is applied.

Private Key: The key of a key pair, which is used to create a digital signature. It can be used to sign a message that only the corresponding public key can verify.

Public Key: It is the key of a key pair that is used to verify a digital signature. Key pair consists of private and public key.

Secret Key: They constitute a part of algorithm for encryption and decryption of the message.

14.8 Review Questions

1. What are different criterions to keep information private when it is sent over a public network?
2. How does the encryption affect performance of network?
3. There are certain information bases on the Internet that need to be prevented by undesirable person to get. How can undesirable person be kept from accessing this?
4. How do we keep our own and other people's computers safe from hackers? Explain with the help of a hypothetical situation.
5. What is a Cipher? Why are cipher used for large messages?
6. Describe briefly two kinds of security attacks, which can be directed against an Internet-connected computer system.
7. What is the difference between secret key and public key encryption?
8. What is cryptography? What are the benefits of using this technique?
9. What do you mean by substitution and transposition ciphers? Differentiate between the two.

Answers: Self Assessment

1. encryption and decryption
2. encryption
3. privacy
4. decrypt
5. IP spoofing
6. True
7. False
8. True
9. True
10. False

14.9 Further Readings

Notes

Books

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall

Behrouz A. Forouzan and Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies

Burton, Bill, *Remote Access for Cisco Networks*, McGraw-Hill, Osborne Media

Dale Tesch/Greg Abelar, *Security Threat Mitigation and Response: Understanding CS-MARS*, Cisco Press, Sep. 26, 2006.

Gary Halleen/Greg Kellogg, *Security Monitoring with Cisco Security MARS*, Cisco Press, Jul. 6, 2007.

Web Tutorials on HTML and Front Page

LOVELY PROFESSIONAL UNIVERSITY
Jalandhar-Delhi G.T. Road (NH-1)
Phagwara, Punjab (India)-144411
For Enquiry: +91-1824-521360
Fax.: +91-1824-506111
Email: odl@lpu.co.in