MSc-IT

DATA COMMUNICATION AND COMPUTER NETWORKS

GAUHATI UNIVERSITY
Institute of Distance and Open Learning

Semester- II

MSc-IT
Paper: INF 2016

Data Communication and Computer Networks

www.idolgu.in

M.Sc.-IT-19-II-2016

GAUHATI UNIVERSITY
Institute of Distance and Open Learning

SECOND SEMESTER

(under CBCS)

M.Sc.- IT

Paper: M.Sc.-IT-19-II-2016

DATA COMMUNICATION AND COMPUTER NETWORKS

Contents:

Contributors:

Mr. Bhaskarjyoti Choudhury (Block I : Unit- 1)
Asstt. Prof., Dept. of Computer Applications
Rangia College, Rangia, Assam
Dr. Kshirod Sarmah (Block I: Unit- 2)
Asstt. Prof., Dept. of Computer Science
PDUAM, Goalpara, Assam
Dr. Vaskar Deka (Block I : Unit- 3)
Asstt. Prof., Dept. of IT
Gauhati University, Assam
Mr. Nayan Mahanta (Block I : Unit- 4, Block II: Unit 3)
Asstt. Prof., Dept. of Computer Science
Pragjyotish College, Guwahati, Assam
Mr. Ainul Matin Choudhury (Block I: Units- 5 & 6)
Asstt. Prof., Dept. of Computer Science
Pragjyotish College, Guwahati, Assam
Dr. Satyajit Sarma (Block II: Units- 1 & 2)
Asstt. Prof., Dept. of IT
Gauhati University, Assam
Dr. Fakharuddin Ahmed (Block II : Unit- 4)
Asstt. Prof., Dept. of IT
LCB College, Guwahati, Assam
Mrs. Manisha Deka (Block II: Unit- 5, Block III: Unit- 4)
Asstt. Prof., Dept. of Computer Science
LCB College, Guwahati, Assam
Mr. Mridul Suklabaidya (Block III: Unit- 1)
Teaching Associate, Dept. of Computer Science
Gauhati University, Assam
Mr. Rahul Lahkar (Block III: Unit- 2)
Asstt. Prof., Dept. of Computer Science
Pub Kamrup College, Assam
Dr. Aniruddha Deka (Block III: Unit- 3)
Asstt. Prof., Dept. of Computer Science and Engineering
Royal Global University, Guwahati, Assam
Mr. Subrat Chetia (Block III: Unit- 5)
Asstt. Prof., Dept. of Computer Science
PDUAM, Dalgaon, Assam
Mrs. Arunima Devi (Block III: Units- 6 & 7)
Asstt. Prof., Dept. of Computer Science
NERIM, Guwahati, Assam

Course Coordination:

Prof. Dandadhar Sarma Director, IDOL, Gauhati University
Prof. Anjana Kakoti Mahanta Prof., Dept. Computer Science, G.U.

Cover Page Designing:

Bhaskar Jyoti Goswami IDOL, Gauhati University

ISBN:
August, 2021

Published on behalf of Institute of Distance and Open Learning, Gauhati University by the Director, and printed at Gauhati University Press, Guwahati-781014.

UNIT: 1
EVOLUTION OF COMPUTER NETWORKS

Contents

Introduction

In this unit you will learn the fundamental aspects pertaining the computer networks. You will learn types of computer networks such as LAN,MAN andWAN. You will learn about how they are created and configure and requirements. You will learn the phases of development of computer networks. We will study circuit switching and packet switching and their development.

Objectives:

After going through this unit ,you will be able to:

- Understand the evolutions of computer networks.
- Know different types of computer networks and why they are categorizes.
- Understand circuit switching and packet switching.
- How we internetworking of computers.

Basic terms and their definitions:

A computernetwork is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources ,data and applications.

The computer networks covered in this unit are obviously not the only type of networks created throughout human civilization. Possibly the oldest example of network covering large territories and serving multiple clients is the water supply system of ancient Rome. But remote and distinct by their mature different networks can seen, they all have something in common.

Topology: Network topology is a physical layout of the computer network and it defines how the computers, devices, cables, etc are connected to each other.

Router: The router is a network device that connects two or more network segments. It is used to transfer information from the source to the destination.

Server: A server is a computer program or device that provides a service to another computer program and its user, also known as the client. In a data center, the physical computer that a server program runs on is also frequently referred to as a server. That machine might be a dedicated server or it might be used for other purposes.A server is a computer program or device that provides a service to another computer program and its user, also known as the client. In a data center, the physical computer that a server program runs on is also frequently

referred to as a server. That machine might be a dedicated server or it might be used for other purposes.

LAN: The full form of LAN is local area network is a computer networks that connects a relatively small area. Most LANs are confined to a single buildingor group of buildings. LANs are capable of transmitting data at very fast rates and there is also a limit on the number of computers that can be attached to asingle LAN. A local area network is a group of computers to a server using a shared common communications line or wireless link.

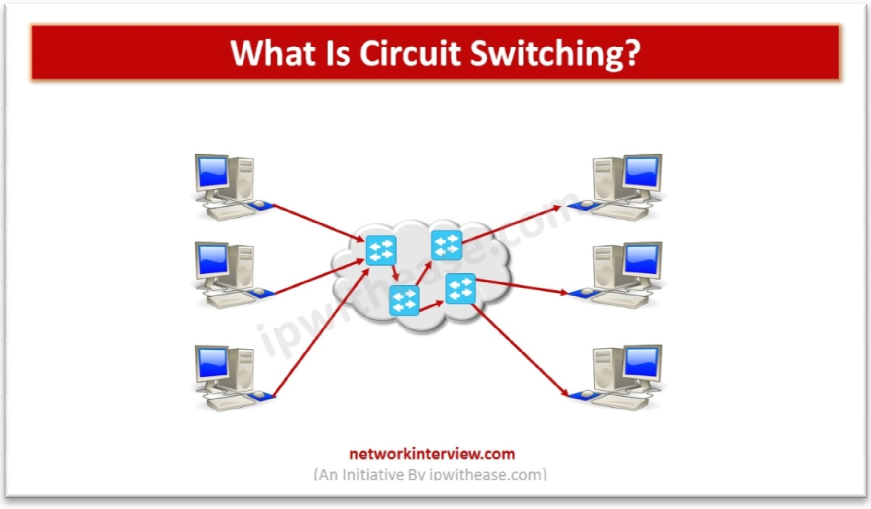
MAN: A metropolitan area network that interconnects users with a computer resources in a geographic area or region larger than local area network but smaller than WAN. It is also used to mean the interconnection of several local area networks by bridging them with backbone lines.

The working mechanism of MAN is similar to an Internet Service Provider, but a MAN is not owned by a single organization. Like a WAN, a MAN provides shared network connections to its users.

WAN: A wide area network is a network that covers a board area using leased telecommunication lines. WANs often connect multiple smaller networks, such as local area network or metropolitan area network. The internet can ne considered as well, and is used bybusinesses ,governments, organizations and individuals for almost any propose imaginable.

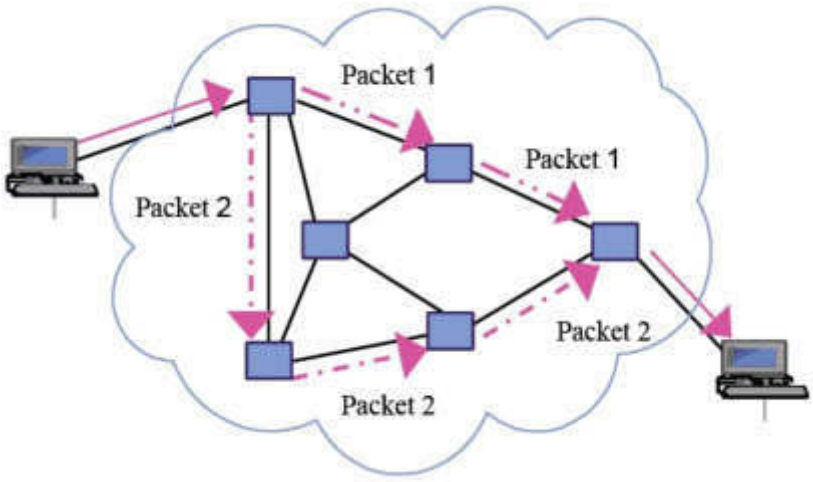
Switch: A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model.

Circuit switching: Circuit switching is a method of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate. The circuit guarantees the full



bandwidth of the channel and remains connected for the duration of the communication session. The circuit functions as if the nodes were physically connected as with an electrical circuit. Circuit switching originated in analog telephone networks where the network created a dedicated circuit between two telephones for the duration of a telephone call.[1] It contrasts with message switchingand packet switching used in modern digital networks in which the trunk lines between switching centers carry data between many different nodes in the form of data packetswithout dedicated circuits

Packetswitching: In telecommunications, packet switching is a method of grouping data that is transmitted over a digital network into *packets*. Packets are made of a header and a payload. Data in the header is used by networking hardware to direct the packet to its destination, where the payload is extracted and used by application software. Packet switching is the primary basis for data communications in computer networks worldwide.
In the early 1960s, American computer scientist Paul Baran developed the concept *Distributed Adaptive Message Block Switching*, with the goal of providing a fault-tolerant, efficient routing method for telecommunication messages as part of a research program at the RAND Corporation, funded by the US Department of Defense.[1]This concept contradicted then-established principles of pre-allocation of network bandwidth, exemplified by the development of telecommunications in the Bell System. The new concept found little resonance among network implementers until the independent work of Welsh computer scientist Donald Davies at the National Physical Laboratory (United Kingdom) in 1965. Davies is credited with coining the modern term *packet switching* and inspiring numerous packet switching networks in the decade following, including the incorporation of the concept into the design of the ARPANET in the United States.



Development of Packet switching: 1961-1972

The field of computer networking and today's Internet trace their beginnings back to the early 1960s, a time at which the telephone network was the world's dominant communication network. That the telephone network uses circuit switching to transmit information from a sender to receiver – an appropriate choice given that voice is transmitted at a constant rate between sender and receiver. Given the increasing importance (and great expense) of computers in the early 1960's and the advent of timeshared computers, it was perhaps natural (at least with perfect hindsight!) to consider the question of how to hook computers together so that they could be shared among geographically distributed users. The traffic generated by such users was likely to be "bursty" – intervals of activity, e.g., the sending of a command to a remote computer, followed by periods of inactivity, while waiting for a reply or while contemplating the received response.

Three research groups around the world, all unaware of the others' work [Leiner 98], began inventing the notion of packet switching as an efficient and robust alternative to circuit switching. The first published work on packet-switching techniques was the work by Leonard Kleinrock [Kleinrock 1961, Kleinrock 1964], at that time a graduate student at MIT. Using queuing theory, Kleinrock's work elegantly demonstrated the effectiveness of the packet-switching approach for bursty traffic sources. At the same time, Paul Baran at the Rand Institute had begun investigating the use of packet switching for secure voice over military networks [Baran 1964], while at the National Physical Laboratory in England, Donald Davies and Roger Scantlebury were also developing their ideas on packet switching.

The work at MIT, Rand, and NPL laid the foundations for today's Internet. But the Internet also has a long history of a Let's build it and demonstrate it attitude that also dates back to the early 1960's. J.C.R. Licklider [DEC 1990] and Lawrence Roberts, both colleagues of Kleinrock's at MIT, both went on to lead the computer science program at the Advanced Projects Research Agency (ARPA) in the United States. Roberts [Roberts 67] published an overall plan for the so-called ARPAnet [Roberts 1967], the first packet-switched computer network and a direct ancestor of today's public Internet. The early packet switches were known as Interface Message Processors (IMP's) and the contract to build these switches was awarded to BBN. On Labor Day in 1969, the first IMP was installed at UCLA, with three additional IMP being installed shortly thereafter at the Stanford Research Institute, UC Santa Barbara, and the University of Utah. The fledgling precursor to the Internet was four nodes large by the end of 1969. Kleinrock recalls the very first use of the network to perform a remote login from UCLA to SRI crashing the system

By 1972, ARPAnet had grown to approximately 15 nodes, and was given its first public demonstration by Robert Kahn at the 1972 International Conference on Computer Communications. The first host-to-host protocol between ARPAnet end systems known as the Network Control Protocol (NCP) was completed [RFC 001]. With an end-to-end protocol available, applications could now be written. The first e-mail program was written by Ray Tomlinson at BBN in 1972.

Proprietary Networks:

A network of automated teller machines (ATMs) available for use only by the customers of a specific bank or financial institution or some other limited group. Proprietary networks have been supplanted by ATM networks that allow the customers of a bank to use free of charge the withdrawal facilities of several other banks with which it has entered a reciprocal agreement.

Proprietary Networks and Internetworking: 1972–1980

The initial ARPAnet was a single, closed network. In order to communicate with anARPAnet host, one had to actually be attached to another ARPAnet IMP. In the early to mid 1970's, additional packet-switching networks besides ARPAnet came into being; ALOHAnet, a satellite network linking together universities on the Hawaiian islands [Abramson 1972]; Telenet, a BBN commercial packet-switching network based on ARPAnet technology; Tymnet; and Transpac, a French packet-switching network. The number of networks was beginning to grow. In 1973, Robert Metcalfe's PhD thesis laid out the principle of Ethernet, which would later lead to a huge growth in so-called Local Area Networks (LANs) that operated over a small distance based on the Ethernet protocol.

Once again, with perfect hindsight one might now see that the time was ripe for developing an encompassing architecture for connecting networks together. Pioneering work on interconnecting networks (once again under the sponsorship of DARPA), in essence creating a *network of networks*, was done by Vinton Cerf and Robert Kahn [Cerf 1974]; the term "internetting" was coined to describe this work. The architectural principles that Kahn' articulated for creating a so-called "open network architecture" are the foundation on which today's Internet is built [Leiner 98]:

- **minimalism, autonomy:** a network should be able to operate on its own, with no internal changes required for it to be internetworked with other networks;
- **best effort service:** internetworked networks would provide best effort, end-to-end service. If reliable communication was required, this could accomplished by retransmitting lost messages from the sending host;
- **stateless routers:** the routers in the internetworked networks would not maintain any per-flow state about any ongoing connection
- **decentralized control:** there would be no global control over the internetworked networks.

These principles continue to serve as the architectural foundation for today's Internet, even 25 years later – a testament to insight of the early Internet designers.

These architectural principles were embodied in the TCP protocol. The early versions of TCP, however, were quite different from today's TCP. The early versions of TCP combined a reliable in-sequence delivery of data via end system retransmission (still part of today's TCP) with forwarding functions (which today are performed by IP). Early experimentation with TCP, combined with the recognition of the importance of an unreliable, non-flow-controlled end-end transport service for application such as packetized voice, led to the separation of IP out of TCP and the development of the UDP protocol. The three key Internet protocols that we see today – TCP, UDP and IP – were conceptually in place by the end of the 1970's.

In addition to the DARPA Internet-related research, many other important networking activities were underway. In Hawaii, Norman Abramson was developing ALOHAnet, a packet-based radio network that allowed multiple remote sites on the Hawaiian islands to communicate with each other. The ALOHA protocol [Abramson 1970] was the first so-called multiple access protocol, allowing geographically distributed users to share a single broadcast communication medium (a radio frequency). Abramson's work on multiple access protocols was built upon by Robert Metcalfe in the development of the Ethernet protocol [Metcalfe 1976] for wire-based shared broadcast networks. Interestingly, Metcalfe's Ethernet protocol was motivated by the need to

connect multiple PCs, printers, and shared disks together [Perkins 1994]. Twenty-five years ago, well before the PC revolution and the explosion of networks, Metcalfe and his colleagues were laying the foundation for today's PC LANs. Ethernet technology represented an important step for internetworking as well. Each Ethernet local area network was itself a network, and as the number of LANs proliferated, the need to internetwork these LANs together became all the more important. An excellent source for information on Ethernet is Spurgeon's Ethernet Web Site, which includes Metcalfe's drawing of his Ethernet concept, as shown below in Figure 1.9-2. We discuss Ethernet, Aloha, and other LAN technologies in detail.

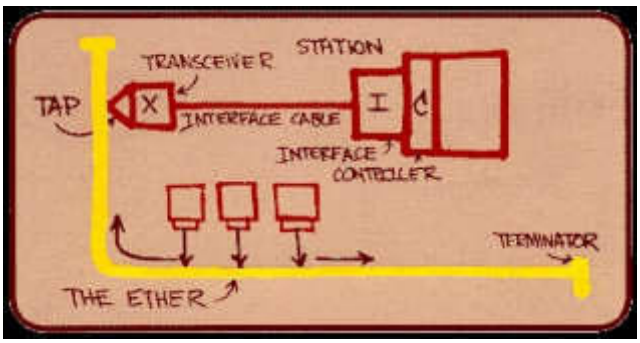


Figure 1.9-2: A 1976 drawing by R. Metcalfe of the Ethernet concept (from Charles Spurgeon's Ethernet Web Site)

In addition to the DARPA internetworking efforts and the Aloha/Ethernet multiple access networks, a number of companies were developing their own proprietary network architectures. Digital Equipment Corporation (Digital) released the first version of the DECnet in 1975, allowing two PDP-11 minicomputers to communicate with each other. DECnet has continued to evolve since then, with significant portions of theOSI protocol suite being based on ideas pioneered in DECnet. Other important players during the 1970's were Xerox (with the XNS architecture) and IBM (with the SNAarchitecture). Each of these early networking efforts would contribute to the knowledge base that would drive networking in the 80's and 90's.

It is also worth noting here that in the 1980's (and even before), researchers (see, e.g., [Fraser 1983, Turner 1986, Fraser 1993]) were also developing a "competitor" technology to the Internet architecture. These efforts have contributed to the development of the ATM (Asynchronous Transfer Mode) architecture, a connection-oriented approach based

on the use of fixed size packets, known as cells. We will examine portions of the ATM architecture throughout this book.

Proliferation of Networks:1980-1990

By the end of the 1970's approximately 200 hosts were connected to the ARPAnet. By the end of the 1980's the number of host connected to the public Internet, a confederation of networks looking much like today's Internet would reach 100,000. The 1980's would be a time of tremendous growth.

Much of the growth in the early 1980's resulted from several distinct efforts to create computer networks linking universities together. BITnet (Because It's ThereNETwork) provided email and file transfers among several universities in the Northeast. CSNET (Computer Science NETwork) was formed to link together university researchers without access toARPAnet. In 1986, NSFNET was created to provide access to NSF-sponsored supercomputing centers. Starting with an initial backbone speed of 56 Kbps, NSFNET's backbone would be running at 1.5 Mbps by the end of the decade, and would be serving as a primary backbone linking together regional networks.

In the ARPAnet community, many of the final pieces of today's Internet architecture were falling into place. January 1, 1983 saw the official deployment of TCP/IP as the new standard host protocol for ARPAnet(replacing the NCP protocol). The transition [Postel 1981] from NCP to TCP/IP was a "flag day" type event – all host were required to transfer over to TCP/IP as of that day. In the late 1980's, important extensions were made to TCP to implement host-based congestion control [Jacobson 1988]. The Domain Name System, used to map between a human-readable Internet name (e.g., gaia.cs.umass.edu) and its 32-bit IP address, was also developed [Mockapetris 1983, Mockapetris 1987].

Paralleling this development of the ARPAnet(which was for the most part a US effort), in the early 1980s the French launched the Minitel project, an ambitious plan to bring data networking into everyone's home. Sponsored by the French government, the Minitel system consisted of a public packet-switched network (based on the X.25 protocol suite, which uses virtual circuits), Minitel servers, and inexpensive terminals with built-in low speed modems. The Minitel became a huge success in 1984 when the French government gave away a free Minitel terminal to each French household that wanted one. Minitel sites included free sites – such as a telephone directory site – as well as private sites, which collected a usage-based fee from each user. At its peak in the mid 1990s, it offered more than 20,000 different services, ranging from home banking to specialized research databases. It was used by over 20% of France's population, generated more than $1 billion each year, and created 10,000 jobs. The Minitel was

in a large fraction of French homes ten years before most Americans had ever heard of the Internet. It still enjoys widespread use in France, but is increasingly facing stiff competition from the Internet.

Explosion 1990s:

The 1990's were issued in with two events that symbolized the continued evolution and the soon-to-arrive commercialization of the Internet. First, ARPAnet, the progenitor of the Internet ceased to exist. MILNET and the Defense Data Network had grown in the 1980's to carry most of the US Department of Defense related traffic and NSFNET had begun to serve as a backbone network connecting regional networks in the United States and national networks overseas. Also, in 1990, The World (http://gaia.cs.umass.edu/kurose/introduction/www.world.std.com) became the first public dialup Internet Service Provider (ISP). In 1991, NSFNET lifted its restrictions on use of NSFNET for commercial purposes. NSFNET itself would be decommissioned in 1995, with Internet backbone traffic being carried by commercial Internet Service Providers.

The main event of the 1990's however, was to be the release of the World Wide Web, which brought the Internet into the homes and businesses of millions and millions of people, worldwide. The Web also served as a platform for enabling and deploying hundreds of new applications, including on-line stock trading and banking, streamed multimedia services, and information retrieval services.

The WWW was invented at CERN by Tim Berners-Lee in 1989–1991 [Berners-Lee 1989], based on ideas originating in earlier work on hypertext from the 1940's by Bush [Bush 1945] and since the 1960's by Ted Nelson [Ziff-Davis 1998]. Berners-Lee and his associates developed initial versions of HTML, HTTP, a Web server and a browser – the four key components of the WWW. The original CERN browsers only provided a line-mode interface. Around the end of 1992 there were about 200 Web servers in operation, this collection of servers being the tip of the iceberg for what was about to come. At about this time several researchers were developing Web browsers with GUIinterfaces, including Marc Andreesen, who developed the popular GUI browser Mosaic for X. He released an alpha version of his browser in 1993, and in 1994 formed Mosaic Communications, which later became Netscape Communications Corporation. By 1995 university students were using Mosaic and Netscape browsers to surf the Web on a daily basis. At about this time the USgovernment began to transfer the control of the Internet backbone to private carriers. Companies – big and small – began to operate Web servers and transact commerce over the Web. In 1996 Microsoft got into the Web business in a

big way, and in the late 1990s it was sued for making its browser a central component of its operating system. In 1999 there were over two-million Web servers in operation. And all of this happened in less than ten years!

During the 1990's, networking research and development also made significant advances in the areas of high-speed routers and routing and local area networks. The technical community struggled with the problems of defining and implementing an Internet service model for traffic requiring real-time constraints, such as continuous media applications. The need to secure and manage Internet infrastructurealso became of paramount importance as e-commerce applications proliferated and the Internet became a central component of the world's telecommunications infrastructure.

References

Two excellent discussions of the history of the Internet are [Hobbes 1998] and [Leiner 1998].

- **[Abramson 1970]** N. Abramson, The Aloha System – Another Alternative for Computer Communications, Proceedings of Fall Joint Computer Conference, AFIPS Conference, 1970, p. 37.
- **[Baran 1964]** P. Baran, On Distributed Communication Networks, *IEEETransactions on Communication Systems*, March, 1964. Rand Corporation Technical report with the same title (Memorandum RM-3420-PR, 1964).
- **[Berners-Lee 1989]** Tim Berners-Lee, CERN, Information Management: A Proposal,March 1989, May 1990
- **[Bush 1945]** V. Bush, As We May Think, The Atlantic Monthly, July 1945.
- **[Cerf 1974]** V. Cerf and R. Kahn, A protocol for packet network interconnection, IEEETransactions on Communications Technology, Vol. COM-22, Number 5 (May 1974), pp. 627–641.
- **[DEC 1990]** Digital Equipment Corporation, In Memoriam: J.C.R. Licklider 1915–1990,SRC Research Report 61, August 1990.
- **[Hobbes 1998]** R. Hobbes Zakon, Hobbes Internet Timeline, Version 3.3, 1998.
- **[Fraser 1983]** Fraser, A. G. (1983). Towards a universal data transport system. *IEEEJournal on Selected Areas in Communications*, SAC-1(5):803–816.
- **[Fraser 1993** Fraser, A. G. (1993). Early experiments with asynchronous time division networks. *IEEE Network Magazine,*7(1):12–27.

- **[Jacobson 1988]** V. Jacobson, Congestion Avoidance and Control, *Proc. ACMSigcomm 1988 Conference*, in Computer Communication Review, vol. 18, no. 4, pp. 314–329, Aug. 1988
- **[Kleinrock 1961]** L. Kleinrock, Information Flow in Large Communication Networks,RLE Quarterly Progress Report, July 1961.
- **[Kleinrock 1964]** L. Kleinrock, 1964 Communication Nets: Stochastic Message Flow and Delay, McGraw-Hill 1964, later re-issued by Dover Books.
- **[Kleinrock 1998]** L. Kleinrock, The Birth of the Internet,http://millenium.cs.ucla.edu/LK/Inet/birth.html.
- [**Leiner 98]** B. Leiner, V. Cerf, D. Clark, R. Kahn, L. Kleinrock, D. Lynch, J. Postel, L. Roberts, S. Woolf, A Brief History of the Internet,http://www.isoc.org/internet/history/brief.html
- **[Metcalfe 1976]** Robert M. Metcalfe and David R. Boggs. Ethernet: Distributed Packet Switching for Local Computer Networks,Communications of the Association for Computing Machinery, Vol 19/No 7, July 1976.
- **[Mockapetris 1983]** P.V. Mockapetris, Domain names: Implementation specification, RFC 833, Nov-01-1983.
- **[Mockapetris 1987]** P.V. Mockapetris, Domain names – concepts and facilities,RFC 1034, Nov-01-1987.
- **[Perkins 1994]** A. Perkins, Networking with Bob Metcalfe, The Red Herring Magazine, November 1994.
- **[Postel 1981]** J. Postel, NCP/TCP Transition Plan, RFC 7801, November 1981.
- **[RFC 001]** S. Crocker, Host Software,RFC 001 (the *very first* RFC!).
- **[Roberts 1967]** L. Roberts, T. Merril Toward a Cooperative Network of Time-Shared Computers, Fall AFIPS Conference, Oct. 1966.
- **[Turner 1986]** J. Turner, New Directions in Communications (or Which Way to the Information Age?), *Proceedings of the Zurich Seminar on Digital Communication,*pp. 25–32, 3/86.
- **[W3C 1995]** The World Wide Web Consortium, A Little History of the World Wide Web, 1995.
- **[Ziff-Davis 1998]** Ziff-Davis Publishing, "Ted Nelson: hypertext pioneer,"

POSSIBLE QUESTIONS

1) What is Computer Network? What are its different types?

2) Is there any difference between Internet and Intranet?
3) LAN is bigger than MAN is it true?
4) Explain Internet impacton our society.
5) Explain difference between circuit and packet switching.
6) Explain proprietary networks and internetworking in the era of 1972-80.
7) Explain the explosion of Internet in 1990s.

UNIT 4: The Physical Layer: Introduction to Data Communication

Unit Structure:

4.1 INTRODUCTION TO PHYSICAL LAYER

SPACE FOR LEARNER NOTE

In OSI model, physical layer plays the role of interacting with actual hardware and signaling mechanism. This layer deals with the physical connectivity of two different stations. It provides its service to data link layer. Physical layer converts them to electricity pulses, which represent binary data. The binary data is then sent over the wired or wireless media.

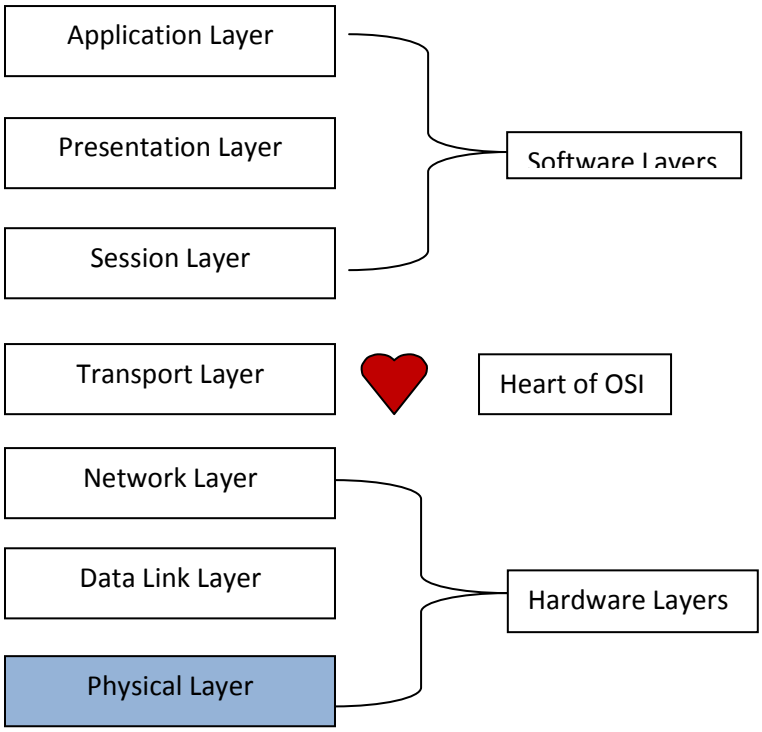


Figure: Physical Layer Position in OSI Model

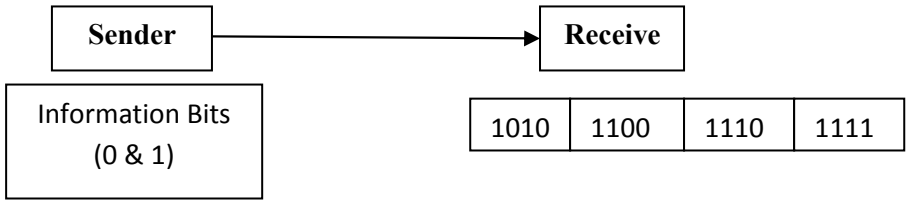
STOP TO CONSIDER

In Physical Layer:

1. Protocols: COAX, FIBER, WIRELESS
2. Network Devices: Repeater/ HUB
3. Data Unit: Bit
4. Type of Layer: Hardware Layer
5. Functions: Bit Synchronization, Bit rate control, Physical Topologies, Transmission mode
6. Transmission Mode: Simplex, Half Duplex & Full Duplex
7. Link Configuration: Point to Point, Multi Point.

STOP TO CONSIDER

8. Physical Layers (0's, 1's)-> Data Link Layer (used Frames)



CHECK YOUR PROGRESS 1

a) What is the data unit of Physical Layer?

1. Data
2. Packets
3. Bit
4. Frame
5. Segments

b) Repeaters operate in which layer?

1. Application Layer
2. Presentation Layer
3. Physical Layer
4. Network Layer

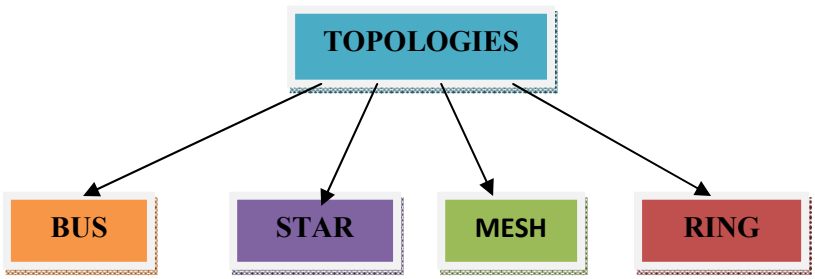


Figure: Different Topologies

4.2 DATA COMMUNICATION CONCEPTS AND TERMINOLOGIES

SPACE FOR LEARNER NOTE

4.2.1. DATA REPRESENTATION

Computer does not understand human language, so, any data, like letters, symbols, and pictures, audio, video, etc. should be converted to machine language. Computer represents data in three forms:
1) Number System, 2) Bits and Bytes and 3) Text Code

1) Number System: It is categories into four types:

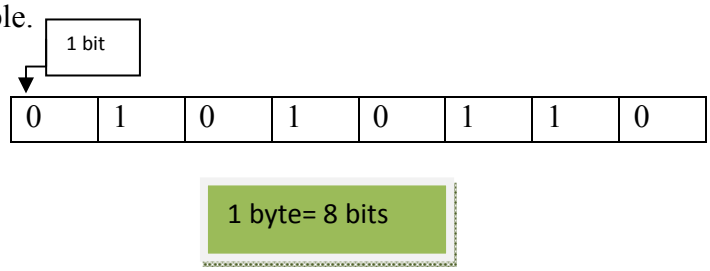
a) Binary number system consists of only two values, either 0 or 1.
b) Octal number system represents values in 8 digits.
c) Decimal number system represents values in 10 digits.
d) Hexadecimal number system represents values in 16 digits.

STOP TO CONSIDER

Number System:

System	Base	Digits
Binary	2	0 1
Octal	8	0 1 2 3 4 5 6 7
Decimal	10	0 1 2 3 4 5 6 7 8 9
Hexadecimal	16	0 1 2 3 4 5 6 7 8 9 A B C D E F

2) Bits and Bytes: Bits: It is smallest possible unit of data that computer can recognize or use.
Bytes: A group of eight bits is called a byte. Half a byte is called a nibble.



STOP TO CONSIDER

Byte Value	Bit Value
1 Byte	8 bits
1024 Bytes	1 Kilobyte
1024 kilobytes	1 Megabyte
1024 Megabytes	1 Gigabyte
1024 Gigabytes	1 Terabyte

SPACE FOR LEARNER NOTE

3**) Text Code:** It is format used commonly to represent alphabets, punctuation and other symbols. Four most popular text code systems are: a) EBCDIC, b) ASCII, c) Extended ASCII, d) Unicode

a) EBCDIC: Extended Binary Coded Decimal Interchange Code is an 8-bit code that defines 256 symbols.
b) ASCII: American Standard Code for Information Interchange is an 8-bit code that specifies character values from 0 to 127.
c) Extended ASCII: Extended American Standard Code for Information Interchange is an 8-bit code that specifies character values from 128 to 255.
d) Unicode: Unicode worldwide character standard uses 4 to 32 bits to represent letters, numbers and symbols.

Check Your Progress-2

2.***State TRUE or FALSE:***

a) Computer understands human languages.

b) Bit is a smallest possible unit of data.

c) 1 bits= 8 byte.

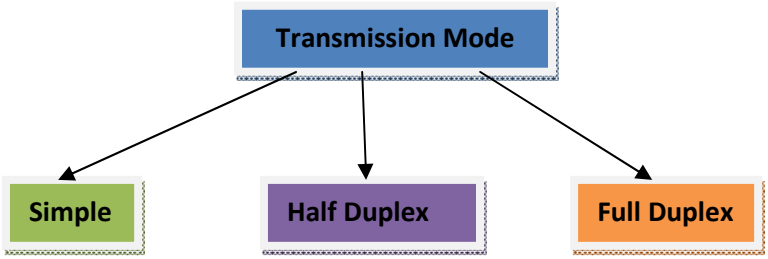
d) 1024 Gigabytes= 1 Terabyte.

e) EBCDIC is Extended Binary Coded Decimal Interchange.

4.2.2. DATA TRANSMISSION MEDIA AND CHANNELS

SPACE FOR LEARNER NOTE

Transformation media is anything that carries information from source to destination.



1) Simplex: In a simplex transmission mode, the communication between sender and receiver occurs only in one direction. The sender can only send the data and the receiver can only receive the data. The receiver cannot reply to the sender. Simplex is like a one-way road in which the traffic travels only in one direction, no vehicle from the opposite direction is allowed to enter.

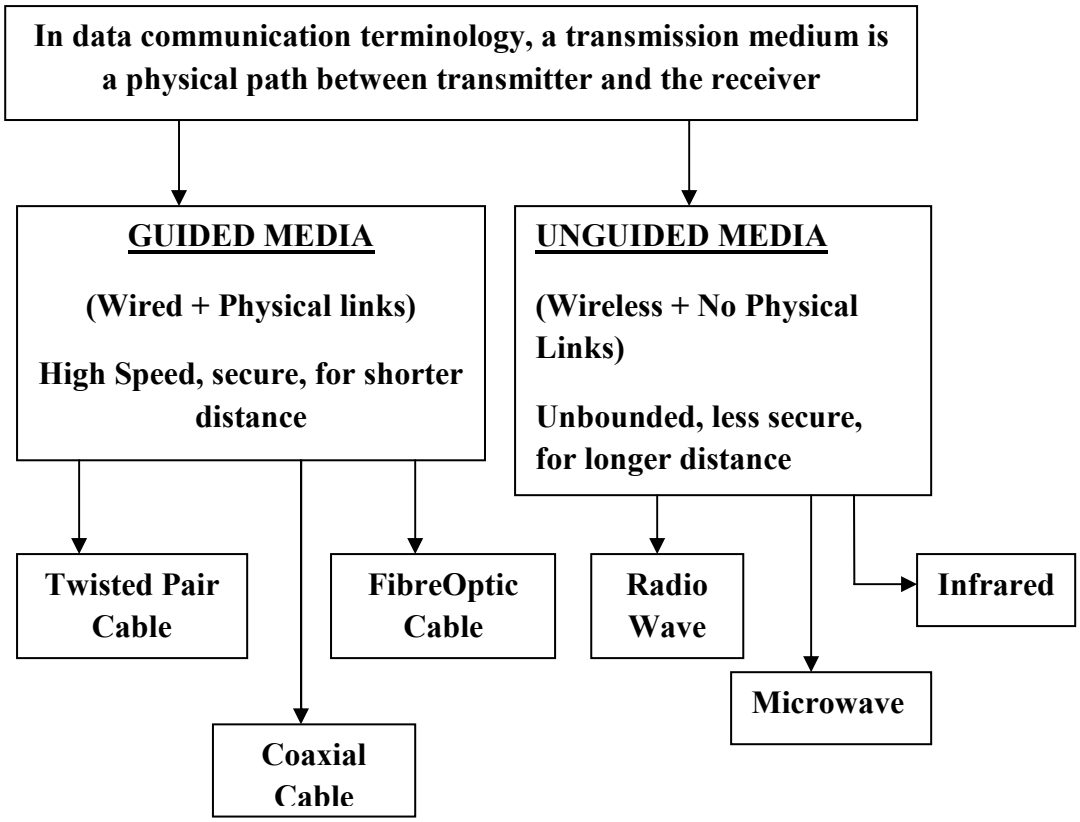
For example, the keyboard can only send the input to the monitor and the monitor can only receive the input and display it on the screen. The monitor cannot reply nor send any feedback to the keyboard.

2) Half Duplex: The communication between sender and receiver occurs in both the directions in a half-duplex transmission, but one at a time. The sender and receiver both can send and receive the information, but only one is allowed to send at a time. Half duplex is still considered a one-way road, in which a vehicle travelling in the opposite direction of the traffic has to wait till the road is empty.

For example, in walkie-talkies, the speaker at both ends can speak but they have to speak one by one. Both cannot speak simultaneously.

3) Full Duplex: In a full duplex transmission mode, the communication between sender and receiver can occur simultaneously. The sender and receiver can both transmit and receive at the same time. The full duplex transmission mode is like a two-way road in which traffic can flow in both directions at the same time.

For example, in a telephone, two people communicate, and both are free to speak and listen at the same time.



1. Guided Media:

a) Twisted Pair Cable: It consists of two conductors (normally copper) each with its own plastic insulation twisted together.

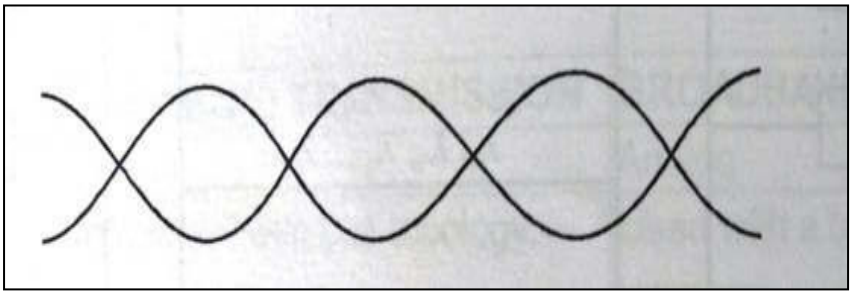


Figure: Twisted Pair Cable

One of the wires carries signal, other is ground, and the receiver receives the difference of the two. The wires are twisted, so that

the unwanted signals (interference and crosstalk) are balanced at the receiver side.

Twisted pair is of two types.

I. **Unshielded Twisted Pair (UTP)**: It is most common twisted pair cable.

II. **Shielded Twisted Pair (STP):** In this extra mesh covering that improves quality used only IBM.

Applications:

1. These are used in telephone lines to provide voice and data channels.
2. DSL lines used by telephone companies to provide high data rate use UTP.
3. LAN network, 10-Base T and 100-Base T use twisted pair cable.

b) Coaxial Cable: It carries signal of higher frequencies than in twisted pair. Coaxial cable has a central core conduction of solid or standard wire (usually copper) enclosed in insulating sheath, in turn in outer conductor of metal foil, or combination of two.

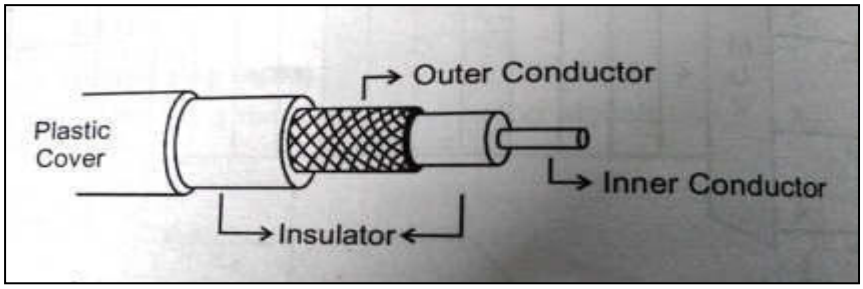


Figure: Coaxial Cable

Attenuation is much higher in coaxial cable than twisted pair cable. Although, coaxial cable has higher bandwidth signal weakens rapidly. So, requires frequent use of repeaters.

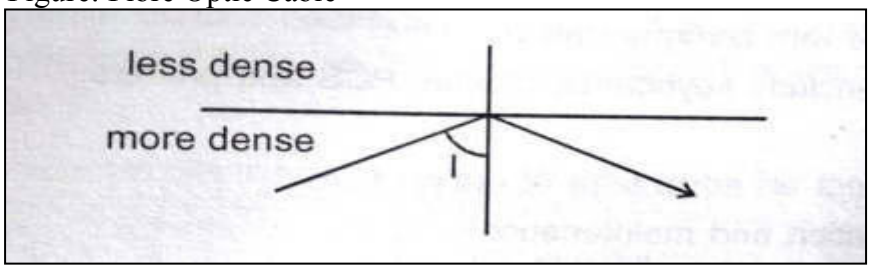
Application:

1. Digital Telephone Networks.
2. Cable TV Networks.

c) Fibre Optic Cable: It is made of glass or plastic and transmits signals in the form of light.

SPACE FOR LEARNER NOTE

Figure: Fibre Optic Cable



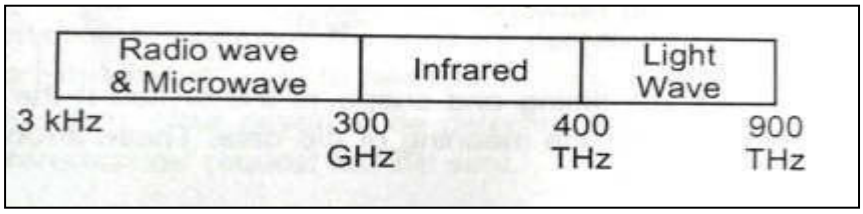
SPACE FOR LEARNER NOTE

STOP TO CONSIDER

- Attenuation is lesser in this case. So, less number of repeaters are required than twisted pair of coaxial cables.
- These are expensive.
- Higher Bandwidth.
- Less signal attenuation. Immune to noise interference.
- Light weight.
- Installation and maintenance is more.
- Unidirectional with one optical fibre.

2) Unguided Wireless Media: Transmission using electromagnetic waves without using a physical conductor.

Figure: Unguided Wireless Media



a) Radio Wave:

- Omnidirectional that is, signal flows in all direction. So, receiving and transmission antennas need not be aligned.
- It can penetrate walls.
- Long distance used in AM radio.

- Applications include- multicasting, AM, FM, television, cordless phone, and paging.

b) Microwave:

- Unidirectional that is, signal flows in a single direction, thus, antennas need to be aligned.
- Very high frequency microwaves cannot penetrate walls.
- Microwave bond is wide, thus, can be sub divided and higher data rate is possible.
- Applications include unicast in cellular phones, satellite networks, wireless LANs.

c) Infrared (300 GHz-400 THz):

- It is useful for short range communication.
- They cannot penetrate walls.
- Infrared cannot be used outside a building because sunlight contains infrared waves that can interfere with communication.
- Applications include- keyboards, mouse and printers.

SPACE FOR LEARNER NOTE

Check Your Progress 3

3.1) State True or False:

a) Easy installation and maintenance.

b) Immune to electromagnetic interference.

c) Less signal attenuation.

d) Greater immunity to tapping.

3.2) Choose the correct one:

a) Loss in signal as light travels down the fibre is called? (Attenuation/ Propagation/ Scattering/ Interruption)

b) Which type electromagnetic waves are used for unicast communication? (Infrared/ Microwaves/ Radio waves/ Light waves)

4.2.3 TRANSMISSION IMPAIRMENT

When signals travel through the medium they tend to deteriorate. Resources are:

1. **Attenuation:** When the signal passes through medium, it tends to get weaker. So, as it covers distance, it loses strength.
2. **Dispersion:** When signal travels through the media, it tends to spread and overlap. It depends upon the frequency used.
3. **Delay distortion:** If the signal speed and frequency do not match, there are possibilities that it reaches destination in arbitrary fashion.
4. **Noise:** Noise in signal is basically random disturbance or fluctuation in analog or digital signal. It can be
    I. **Thermal Noise:** It is basically happened because heat agitates conductor of a medium
    II. **Intermodulation:** It occurs if two different frequencies are sharing a medium and one of them has excessive strength or the component is not functioning properly.
    III. **Crosstalk:** It happens when a foreign signal enters into the media. This is because signal in one medium affects the signal of second medium.
    IV. **Impulse:** This noise is introduced because of irregular disturbance such as lightening, electricity, short-circuit, or faulty components. Digital data is mostly affected by this sort of noise.

4.2.4 DIGITAL TRANSMISSION AND SIGNAL ENCODING

Data can be represented in analog or digital form. Encoding is the process of converting the data or a given sequence of characters, symbols, alphabets etc, into a specified format, for the secured transmission of data. Decoding is the reverse process of encoding which is to extract the information from the converted format.

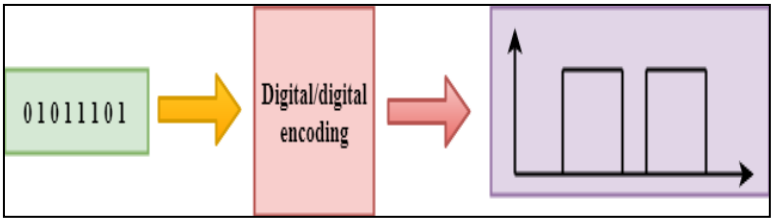
Data Encoding Techniques:

1. **Digital to digital conversion:** It is the representation of digital information by a digital signal. When binary 1s and 0s generated by the computer are translated into a sequence of voltage pulses that can be propagated over a wire, this process in known as digital-to-digital encoding. It is

SPACE FOR LEARNER NOTE

divided into three categories: **i) Unipolar Encoding, ii) Polar Encoding, iii) Bipolar Encoding.**

Figure: Digital-to-digital conversion



2. Analog to digital conversion: In this technique the transmission convert analog signal to digital signal. Here two techniques used:
i) PAM (Pulse Amplitude Modulation), ii) PCM (Pulse Code Modulation)

3. Digital to analog method: When data from one computer is sent to another via some analog carrier. It is first converted into analog signals. Analog signals are modified to reflect digital data.

Four methods are used:

I. **ASK (Amplitude Shift Key).**
II. **PSK (Phase Shift Key).**
III. **FSK (Frequency Shift Key).**
IV. **QAM (Quadrature Amplitude Modulation).**

Check Your Progress 3

State True or False:

a) Crosstalk is one of the reasons of transmission impairment.

b) Unipolar encoding is the conversion method of digital to analog.

c) Decoding is the process to extract the information from the converted format.

d) In intermodulation, two different frequencies sharing a medium.

SPACE FOR LEARNER NOTE

4.3ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress 1:

a) 3, b) 3

Check Your Progress 2:

a) False, b) True, c) False, d) True, e) True

Check Your Progress 3:

3.1) a, 3.2) (a) Attenuation, (b) Microwave

SPACE FOR LEARNER NOTE

4.4 SUMMING UP

- Physical layer interacting with hardware and signalling mechanism.
- In physical layer, we used bus, star, mesh and ring topology.
- Computer represents data in three forms: number system, bits and bytes, and text code.
- Data transmission mode is mainly simple, half duplex and full duplex.
- Data transmission medium is mainly two types that are guided media and unguided media.
- In guided media, three physical cables are used that is twisted pair cable, coaxial cable and fibre optic cable.
- In unguided media, we used radio wave, microwave and infrared.
- Transmission impairment resources are attenuation, dispersion, delay distortion and noise. Noise can be thermal, intermodulation, crosstalk and impulse.
- Data encoding techniques is mainly digital to digital conversion, analog to digital conversion and digital to analog conversion.

4.5POSSIBLE QUESTIONS

Short answer type questions:

1. Mention network devices used in physical layer?
2. What are the functions used in physical layer?
3. What are the transmission modes used in physical layer?
4. What is topology? What are the different types of topologies?
5. What is number system? Mention its types.
6. What is Unicode?
7. What are the resources of transmission impairment?
8. What are the data encoding techniques?

Long answer type questions:

1. Briefly explain all data representation techniques.
2. Explain all transmission modes with suitable examples.
3. What is guided media? Explain all its types.
4. What is unguided media? Explain all its types.
5. What is noise? Mention all its types.
6. Explain all transmission impairments resources.
7. Explain all data encoding techniques.
8. Write short notes on the following:
    a) Twisted Pair Cable.
    b) Coaxial Cable.
    c) Fibre Optic Cable.
    d) Radio Wave
    e) Microwave

4.6 FURTHER READINGS

- Computer Network, Fourth Edition, Andrew S. Tanenbaum

UNIT 5: The Physical Layer: Transmission Media

5.0 Introduction:

The physical layer defines the means of transmitting a stream of raw bits over a physical data link connecting network nodes. The bit-stream may be grouped into code words or symbols and converted to a physical signal that is transmitted over a transmission medium. The physical layer provides an electrical, mechanical, and procedural interface to the transmission medium. The shapes and properties of the electrical connectors, the frequencies to broadcast on, the line code to use and similar low-level parameters, are specified by the physical layer[1][3].

The physical layer consists of the electronic circuit transmission technologies of a network. It is a fundamental layer underlying the higher level functions in a network, and can be implemented through a great number of different hardware technologies with widely varying characteristics.

Within the semantics of the OSI model, the physical layer translates logical communications requests from the data link layer into hardware-specific operations to cause transmission or reception of electronic (or other) signals.[4][5] The physical layer supports higher layers responsible for generation of logical data packets.

5.1 Unit Objectives

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.
- In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.

- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

5.2 Some basic terms and their definition:

- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal [5].
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.
- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

5.3 Classification of Transmission Media:

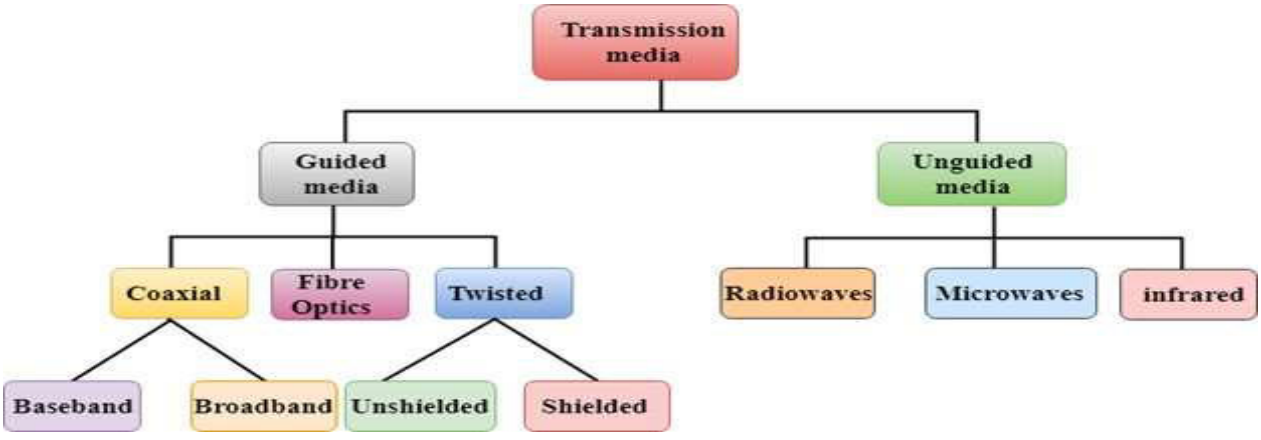


Fig: classification of Transmission media (Source: Internet)

5.3.1 Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

Types of Guided media:

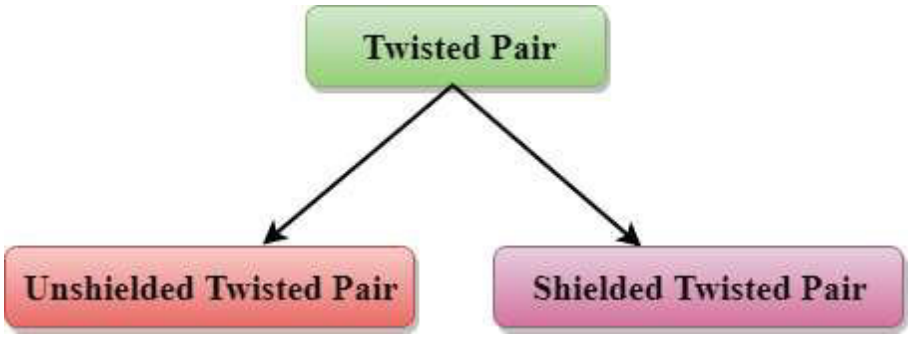
5.3.1.1 Twisted pair:

The oldest and still most common transmission medium is twisted pair. A twisted pair consists of two insulated copper wires, typically about 1 mm thick [6]. The wires are twisted together in a helical form, just like a DNA molecule. The purpose of twisting the wires is to reduce electrical interference from similar pairs close by. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.

Types of Twisted pair:



i) Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.

- **Category 5:** It can support upto 200Mbps.

Advantages of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

ii) Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

5.3.1.2 Coaxial Cable

Another common transmission medium is the coaxial cable. It has better shielding than twisted pairs, so it can span longer distance at higher speeds. Coaxial cable is a type of transmission line, used to carry high-frequency electrical signals with low losses [7]. It is used in such applications as telephone trunk lines, broadband internet networking cables, high-speed computer data busses, cable television signals, and connecting radio transmitters and receivers to their antennas. It differs from other shielded cables because the dimensions of the cable and connectors are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a transmission line.

Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages Of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

5.3.1.3 Fibre Optic

The world of telecommunications is rapidly moving from copper wire networks to fiber optics. Optical fiber is a very thin strand of pure glass which acts as a waveguide for light over long distances. It uses a principle known as total internal reflection [8]. Fiber optic cable is actually composed of two layers of glass: The core, which carries the actual light signal, and the cladding, which is a layer of glass surrounding the core. The cladding has a lower refractive index than the core. This causes Total Internal Reflection within the core. Most fibers operate in duplex pairs: one fiber is used to transmit and the other is used to receive. But it is possible to send both signals over a single strand. There are two main types of fiber optic cables: Single Mode Fiber (SMF) and Multi-Mode Fiber (MMF). The difference is basically in the size of the core. MMF has a much wider core, allowing multiple modes (or "rays") of light to propagate. SMF has a very narrow core which allows only a single mode of light to propagate. Each type of fiber has different properties with its own advantages and disadvantages.

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibre coated in plastic that are used to send the

data by pulses of light.

- The plastic coating protects the optical fibre from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires.

Following are the advantages of fibre optic cable over copper:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

5.3.2 Wireless Transmission

An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**. In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

5.3.2.1 Electromagnetic Spectrum

The electromagnetic (EM) spectrum is the range of all types of EM radiation. Radiation is energy that travels and spreads out as it goes – the visible light that comes from a lamp in your house and the radio waves that come from a radio station are two types of electromagnetic radiation. The other types of EM radiation that make up the electromagnetic spectrum are microwaves, infrared light, ultraviolet light, X-rays and gamma-rays.

5.3.2.2 Broadcast Radio Transmission

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are Omni-directional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3 Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.

Applications Of Broadcast Radio Transmission

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Broadcast Radio Transmission

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.
-
- Microwaves are of two types:

5.3.2.3 Infrared Transmission

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

5.3.2.4 Microwave Transmission

Microwaves are widely used point to point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. This frequency reuse conserves scarce radio spectrum bandwidth. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can[4].

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy

Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.

5.3.2.5 Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.

- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
- **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

5.3.2.6 Satellite Microwave Transmission

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

Advantages Of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the center of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.

- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

5.4 Check your progress

1. A transmission medium is located under and controlled by the

a) Transport layer
b) Physical layer
c) application layer
d) session layer

2. Guided transmission media include

a) Coaxial cable
b) Fiber optic cable
c) twisted pair cable
d) All of the above

3. Which of the following is not a type of twisted pair cable

a) UTP
b) FTP
c) STP
d) None of the above

4. BNC connectors are used with

a) Satellite
b) Fiber optic cable
c) Coaxial cable
d) twisted pair cable

5. The transmission medium with maximum error rate is

a) Coaxial cable
b) twisted pair cable
c) satellite link
d) optical fiber

6. Optical fibers transmit a beam of light by means of

a) Total internal reflection
b) Total internal refraction
c) Both a) & b)
d) None of these

7. In multimode step-index fibre, the density of the core----------from the center to the edges.

a) Increases
b) Decreases
c) remain constant
d) none of these

8. Which of the following is not a band?

a) VHF
b) UHF
c) VLF
d) SLF

9. Unguided signals can propagate in ----------

a) Two
b) Three
c) eight
d) four

10. The frequency at which a signal is received by a satellite is known as its ---------- frequency

a) Downlink
b) Microwave
c) terrestrial
d) uplink

Answer to check your progress:

1.(b) 2. (d) 3. (b) 4.(c) 5. (b) 6.(a) 7.(c) 8.(d) 9.(b) 10.(d)

5.5 Long answer type questions

i) What are transmission media? What are the different categories of transmission media?

ii) Differentiate guided and unguided transmission media.

iii) Explain in details the various types of guided transmission media.

iv) Why twisting of wires is necessary in twisted pair cable?

v) Write advantage and disadvantages of twisted pair cable and fibre optic cable.

vi) What are the different fibre sizes and connectors available?

vii) Explain the use of electromagnetic spectrum for communication.

vii) Explain the different propagation methods for unguided signals.

viii) Explain in details the different unguided media.

References

1. *Gorry Fairhurst (2001-01-01). "Physical Layer". Archived from the original on 2009-06-18.*
2. *Iyengar, Shisharama (2010). Fundamentals of Sensor Network Programming. Wiley. p. 136. ISBN 978-1423902454.*
3. *"The Physical Layer | InterWorks". InterWorks. 2011-07-30. Retrieved 2018-08-14.*
4. *Shaw, Keith (2018-10-22). "The OSI model explained: How to understand (and remember) the 7 layer network model". Network World. Retrieved 2019-02-15.*
5. *"DATA COMMUNICATION & NETWORKING". ResearchGate. Retrieved 2019-02-15.*
6. This article incorporates public domain material from the General Services Administration document: *"Federal Standard 1037C"*.
7. *"physical signaling sublayer (PLS)". Archived from the original on 2010-12-27. Retrieved 2011-07-29.*
8. *"rfc1122". datatracker.ietf.org. Retrieved 2021-07-28.*

UNIT 1: The Data Link Layer: Design Issues

CONTENTS

1.1 INTRODUCTION

In this unit, you will learn the design principles and the basic role of layer 2, the data link layer. This study deals with the techniques, algorithm and method for efficient and reliable communication between the two machines at data link layer. You will also learn the basic functions, services provided by the data link layer to its upper layer in OSI Reference Model. Framing is a major function of data link layer and using framing bit stream received from physical layer can be divided in to some frames. And the data is forwarded to its upper layer in terms of frame. The data link layer basically responsible for error control, flow control, error detection and correction mechanism. For flow control and error control, data link layer uses various mechanisms which are explained below in details.

1.2 UNIT OBJECTIVES

After going through this unit, you will be able to:

- Understand the functionalities of data link layer.
- Know different services provided by data link layer to its upper layer.
- Understand framing and the various framing methods.
- Describe error control and different error control mechanisms.
- Describe flow control and different flow control mechanisms.
- Describe error detection and error correction techniques.

1.3 SERVICES PROVIDED BY DATA LINK LAYER

The important and essential function of Data Link Layer is to provide an interface to Network Layer. Network Layer is third layer of seven-layer OSI reference model and it is present just above Data Link Layer. The main aim of Data Link Layer is to transmit data frames they have received to destination machine so that these data frames can be handed over to network layer of destination machine. At the network layer, these data frames are basically addressed and routed.

The Data link layer basically provides or offers three types of services as mentioned below.

a. Unacknowledged Connectionless Service
b. Acknowledged Connectionless Service
c. Acknowledged Connection-Oriented Service

1.3.1 Unacknowledged Connectionless Service

Unacknowledged connectionless service basically provides datagram modes delivery without any error, issue, or flow control. In this service, the sender host basically transmits independent frames to the receiver host without having the acknowledge frames from the receiver machine. This service is called as connectionless service because there is no connection established among sending or source machine and destination or receiving machine before the transferring of data or after releasing the data transfer. In Data Link Layer, due to some reasons like noise, if frame is lost, no attempt will be made to determine or sense the loss of the frames or recovery of the frames. This basically means that there will be no any possibility of error or no need of any flow control mechanism. A good example of this service is the Ethernet service.

1.3.2 Acknowledged Connectionless Service

This service basically provides acknowledged connectionless service and here delivery of packet is merely acknowledged, with the help of stop and wait for protocol. In this service, each data frame which is transmitted by the Data Link Layer is merely acknowledged separately and then sending host generally knows whether the transmitted data frames are received without any error or not. No logical connection is established between the source and destination host and each frame that is transmitted is acknowledged individually.

This mode basically provides a way by which a user of data link can simply transmit data and ask for return of data at the same time. It also uses specific time duration and if it has passed frame without getting acknowledgment, then it will retransmit the data frame on the specific time duration.

This service is considered more reliable than the unacknowledged connectionless service. This service is basically useful for different unreliable channels, such as wireless connections, wireless LAN, WiFi etc.

1.3.3 Acknowledged Connection-Oriented Service

In this Acknowledged Connection-Oriented Service, first connection is established between the source machine (sender) and the destination machine (receiver) before sending the data frames. After that the data frames are sent or transmitted by the sender using the newly established connection or path. In this service, each of the data frames that are sent or transmitted is assigned individual numbers first. Using this individual numbers, it confirms and guarantees that each of the data frames is received successfully at the receiver side without any duplication and with proper order and sequence.

Check Your Progress-1

State TRUE or FALSE:

1. Data Link layer provides service to its upper layer.
2. The data link layer transmits data in terms of packet.
3. Unacknowledged connectionless service simply provides datagram style delivery.
4. Duplication of data delivery is done with the help of sequence number.
5. In acknowledged connectionless service, each data frame which is transmitted by the data link layer is not acknowledged individually.

1.4 FRAMING IN DATA LINK LAYER

To provide service to its upper layer, i.e. network layer, the data link layer must take the services provided by its lower layer, i.e. the physical layer. Physical layer at sender side accepts a row bit stream and attempt to deliver it to the destination. The job of the data link layer is to break the bit stream into some frames and compute the checksum for each frame. Frames are the basic units of digital transmission mainly in computer networks and telecommunications. Framing provides a means for a source machine to transfer a set of bit streams that are meaningful to the intended receiver. Frame with different technology like Ethernet, token ring etc have their own structures. Each frame has frame headers which includes some information like error-checking codes etc. From the sender frame header information, it extracts the message and using receiver address, it provides the frame to the receiver. The advantage of using frames is that message or data is broken up into some recoverable chunks which can be checked and verified easily for any error.

There are some problems in Framing –

- Detecting start of the frame: When a frame is sent, each station must be able to find the start of the frame. Stations detect frames by verifying the special sequence of bits that marks the starting of the frame which is known as SFD (Starting Frame Delimeter).
- How does a station detect a frame: Each station listen to the link for SFD pattern through a sequential circuit. If it detects SFD, sequential circuit do the necessary job for make alert the station. Station verifies destination address so that it can accept or reject frame.
- Detecting end of frame: Another issue of framing is to know when to stop reading the frame.

1.4.1 FRAMING METHODS

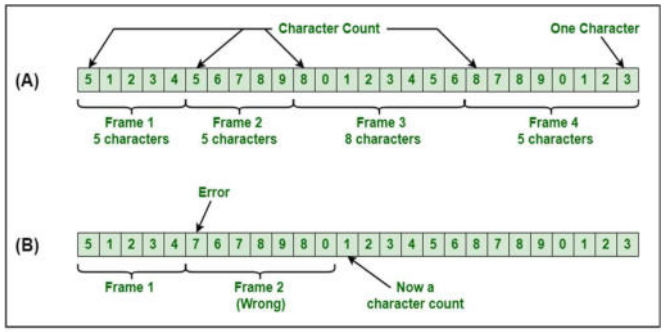
In data link layer, after receiving the bit stream from physical layer, it is transmitted in terms of frame. Using framing technique, we can break the bit stream into frame but practically breaking bit

stream into frame is not easy. One approach for framing technique is to introduce time gap between frames, such as the space that we put in between words in normal text. But this time gap method has no any guarantee. Here, we will discuss some popular framing methods.

1.4.1.1CHARACTER COUNT

Character count method is rarely used and it is basically required to count the total number of characters that are present in the frame. Frame header field is used to keep the track of that count. In data link layer, character count method ensures the total number of characters present in the frame and the end of each frame at receiver or destination host.

There are some disadvantages also in this character count method. If anyhow character count is distorted or unclear by an error happening during transmission, then destination or receiver host may face synchronization problem. The destination or receiver host also may not be able to locate or identify the starting of next frame.



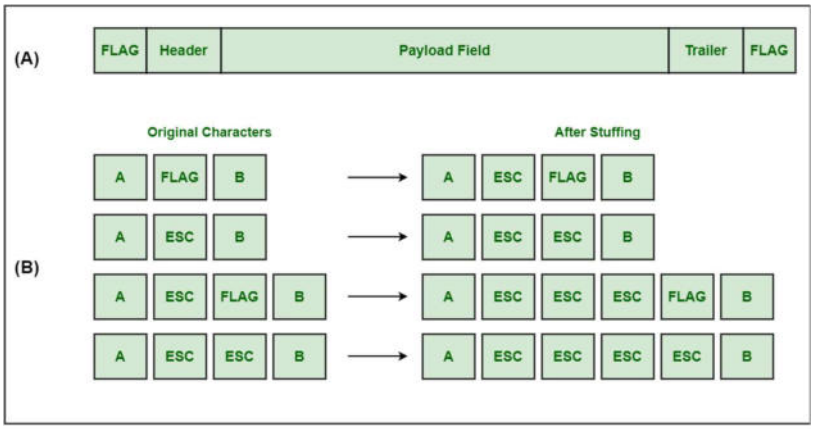
A Character Stream

(A) Without Errors
(B) With one Error

1.4.1.2 FLAG BYTES WITH BYTE STUFFING

Character stuffing method is also known as byte stuffing or character-oriented framing. This method is same as bit stuffing method, only byte stuffing works on bytes whereas bit stuffing

works on bit. In this byte stuffing method, special byte which is simply known as ESC (Escape Character) is normally added to the data stream or frame. This ESC is the same pattern with the flag byte. Same Flag bytes are used at the starting and ending of the frame. If the receiver sometimes loses synchronization due to some problem, it tries to find the flag byte to locate the end of the frame. Two consecutive flag bytes specify the end of one frame and the beginning of the next frame.



A Character Stuffing
(A) A frame delimited by flag bytes
(B) Four examples of byte sequences before and after byte stuffing

1.4.1.3 BIT STUFFING

Bit stuffing is also known as bit-oriented framing. In this bit stuffing method, additional bits are added to the data streams. A special bit pattern indicates the starting and end of the frame.
Whenever the sender's data link layer encounter five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream and at the receiver side receiver de-stuffs the 0 bit when it gets a 0 bit after five consecutive 1s. Whole procedure is explained below.

(a) **0110111111111110** [Original data]

(b) **011011111011111010** [After bit stuffing]

(c) **0110111111111110** [After de-stuffing at receiver side]

1.4.1.4 PHYSICAL LAYER CODING VIOLATIONS

This method is generally applicable to the networks where the encoding on the physical medium contains some sort of redundancy

For example,

- Some LANs encode 1 bit of data by taking 2 physical bits.
- Generally, a 1 bit is a high-low pair and a 0 bit is a low-high pair.
- 11 or 00 are not used for data but are used for delimiting frames in some protocols.

STOP TO CONSIDER

The main function of data link layer is framing, i.e. to break the bit stream received from physical layer into some frames and compute the checksum for each frame. In data link layer, frames are the basic units of digital transmission.

Check Your Progress-2

6. One approach for _____ technique is to introduce time gap between the frames.
7. In data link layer, _____ method ensures the total number of characters present in the frame.
8. In bit stuffing method, additional _____ are added to the data streams
9. The job of the data link layer is to compute _____ the for each frame.
10. This ESC is the same pattern with the _____ byte.

1.5ERROR CONTROL

In data link layer, error control is the process of detecting and correcting data frames which have been corrupted or lost during transmission. In case of lost or corrupted frames, the receiver does not receive the correct data-frame and sender does not know about the loss. Data link layer follows a method to detect transit errors

and takes the required actions. It retransmits the frames whenever error is detected or frame is lost.

The error control mechanism in data link layer involves the following phases −

Detection of Error − In data link layer, sender or the receiver detects the error, if any transmission error occurs.

Acknowledgment – Receiver sends acknowledgment to sender, the acknowledgement may be positive or negative.

Positive ACK – After receiving a correct frame, the receiver sends a positive acknowledgement.

Negative ACK – After receiving a corrupted frame or a redundant frame, the receiver sends back a negative acknowledgment to the sender.

Retransmission − The sender uses a timer and sets a timeout period. If an acknowledgment of an earlier transmitted data-frame does not arrive before the timeout period, or sender receives a negative acknowledgment, the sender retransmits the frame.

1.6 FLOW CONTROL

Flow control is a method which allows two stations working at different speeds to communicate with each other. If the sender is sending at high speed and the receiver can't accept at that speed, data may be lost. So some flow control method is needed to regulate the data frame that is sent by a sender so that a fast sender does not overwhelm a slow receiver.

In data link layer, in one approach, the sender continues to send frames only after it has received acknowledgments from the user for the previous frames. This is called feedback based flow control. Here, a restriction is imposed on the number of frames the sender can send before it waits for an acknowledgment from the receiver.

Stop and Wait

In this stop and wait protocol, the sender sends a frame and waits for an acknowledgment for that particular frame. Once the receiver receives the frame, it sends back an acknowledgment frame to the sender. After receiving the acknowledgment frame, the sender understands that the receiver is ready to accept the next frame. So it sends the next frame to the queue.

Sliding Window

This protocol improves the efficiency of stop and waits protocol by allowing multiple frames to be transmitted before receiving an acknowledgment. The methodology of this protocol is explained as follows −

Both sender and the receiver have fixed sized buffers called windows. Based on the size of the buffer, the sender and the receiver agree upon the number of frames to be transmitted. The sender transmits multiple frames sequentially, without waiting for acknowledgment. When the window is filled, then it waits for the acknowledgment. After receiving the acknowledgment, it advances the window and sends the next frames, as per the number of acknowledgments received.

STOP TO CONSIDER

In data link layer, error control is the process of detecting and correcting data frames that been corrupted or lost during transmission. Flow control method allows two stations working at different speeds to communicate with each other so that no frame is lost during transmission.

1.7 ERROR DETECTION AND CORRECTION

Error detection and correction is one of the major functions of data link layer. While sending a frame from sender to the receiver, there may be errors in the frame due to various reasons at the receiver side. In the following section, some error detection and correction techniques are discussed.

1.7.1 ERROR DETECTION CODES

Error-correcting codes are often used on wireless connection, which are very much noisy and erroneous compared to a wired connection. In case of fiber or copper wire, the error rate is comparatively lower, therefore error detection and retransmission is more efficient in case wired connection. We have three main methods for detecting errors in frames. Those are Parity Check, Checksum and Cyclic Redundancy Check (CRC).

1.7.1.1 Parity Check

In data link layer, the parity checking is done by adding an extra bit, called parity bit to the data to make a number of 1s either even to make it even parity or odd to make it odd parity. While making a frame, the sender counts the number of 1s in it and adds the parity bit in the following way.

To make it even parity, if the number of 1s is even then the value of parity bit is 0 and if the number of 1s is odd then the value of parity bit is 1. Similarly, in case of odd parity, if the number of 1s is odd then the value of parity bit 0 and if the number of 1s is even then the value of parity bit 1.After receiving a frame, the receiver counts the number of 1s in the frame. When even parity is used, if the number of 1s is even, the frame is accepted, otherwise it is rejected. Similarly if odd parity is used, if the number of 1s is odd, it is accepted otherwise it is simply rejected. This parity bit checking method works better for single bit error detection only.

1.7.1.2 Checksum

In this checksum error detection method data is divided into fixed sized frames. The sender adds the frame segments using 1's complement arithmetic to get the sum. Then it complements the sum to get the checksum and transmits it along with the data frames. At the receiver side, the receiver adds the incoming frame segments along with the checksum using 1's complement arithmetic. If the result is zero, the received frames are accepted; otherwise, frames are discarded.

1.7.1.3 Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check (CRC) which is also known as polynomial code involves binary division of the data bits being sent by a predetermined divisor agreed upon by the communicating system. CRC or Cyclic Redundancy Check is a method of detecting accidental changes/errors in the communication channel. CRC uses Generator Polynomial which is available on both sender and receiver side. An example of generator polynomial is $x^3 + x + 1$. This generator polynomial represents the key 1011. Another example is $x^2 + 1$ which represents the key 101.

Before sending the frame, following points are performed at the sender side.

a. The binary data is first augmented by adding k-1 zeros in the end of the data.
b. Use modulo-2 binary division to divide binary data by the key and store remainder of division.
c. Append the remainder at the end of the data to form the encoded data and send the same.

Once the frame has been received, modulo-2 division again performed at the receiver side. If the remainder is 1 then there must be errors and if the remainder is 0, then there are no errors. If there is error, that must be handled properly.

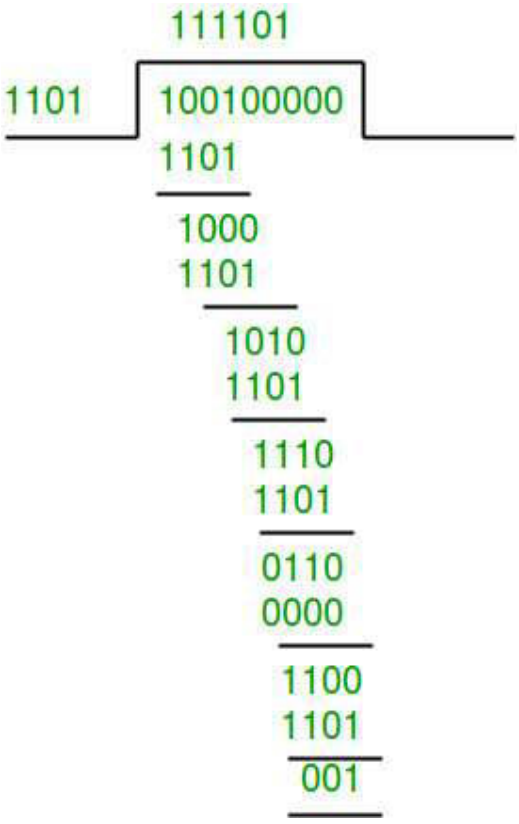
Modulo 2 Division:
The process of modulo-2 binary division is the same as the familiar division process that we use for decimal numbers. In this modulo-2 division, instead of subtraction, we use XOR here. The steps are mentioned below.

- In each step, a copy of the divisor (or data) is XORed with the k bits of the dividend (or key).
- The result of the XOR operation (remainder) is (n-1) bits, which is used for the next step after 1 extra bit is pulled down to make it n bits long.
- When there are no bits left to pull down, we have a result. The (n-1)-bit remainder which is appended at the sender side.

The polynomial method is explained below by taking an example below.

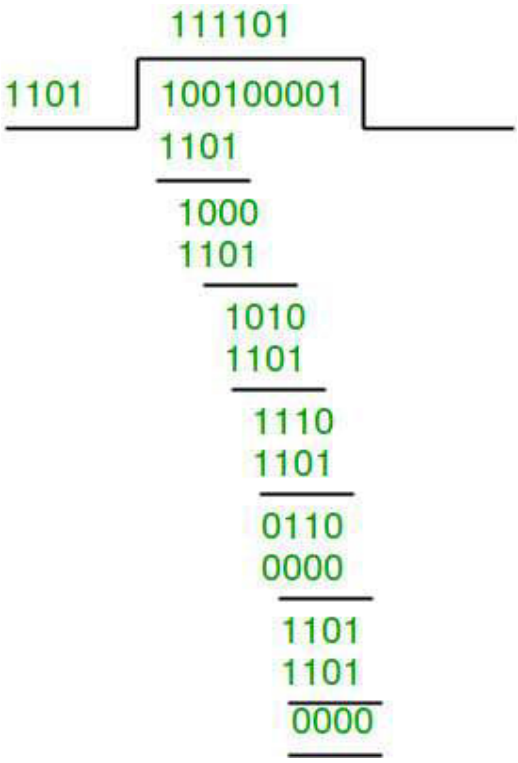
The data word to be sent by the sender is 100100
And the key taken is 1101 [or generator polynomial x3 + x2 + 1]

At the sender s side-



From the above calculation, we have seen that the remainder is 001. Therefore, the encoded data sent is 100100001.

At the receiver side, the code word received by the receiver is 100100001. Again the calculation is done as follows.



Here, at the receiver side we have seen that the remainder is all zeros. Hence, the data received has no any error.

1.7.2 ERROR CORRECTION TECHNIQUES

Error correction techniques are used to find out the exact number of bits that have been corrupted and as well as their locations. There are two principle ways for error correction.

Backward Error Correction (Retransmission) − If the receiver detects an error in the incoming frame, it requests the sender to retransmit the frame. This technique can be efficiently used only where retransmitting is not expensive and the time for retransmission is low compared to the requirements of the application.

Forward Error Correction − If the receiver detects some error in the incoming frame, it performs error-correcting code that generates the actual frame. Using this method saves the bandwidth

requirement for retransmission. However, if there are too many errors, the frames need to be retransmitted.

The codes which are used for both error detecting and error correction are called as "Error Correction Codes". The error correction techniques are of two types. They are as follows.

a. Single bit error correction: Here only single bit error is corrected.
b. Burst error correction: In this method, burst errors in the data sequence are detected and corrected.

1.7.2.1 Hamming Distance

Normally a frame consists of m data (i.e. message) bits and r redundant or check bits. Let the total length be n (i.e. n = m+r). An n-bit containing m data bit and r-redundant bit is called n-bit codeword. Let us take two codewords, 10001001 and 10110001. Here, 3 bits differ between the two codewords. To determine, how many bits differ, just perform exclusive OR between the codewords and count the number of 1 bits in the result.

Here we have taken an example as follows-

$$\begin{array}{r} 10001001 \\ \underline{10110001} \\ 00111000 \end{array}$$

The number of bit positions in which two codewords differ is called Hamming distance. The number of parity bits to be added to a data string depends upon the number of information bits of the data string which is to be transmitted. Number of parity bits will be calculated by using the data bits. This relation is given below.

$$\mathbf{2^P >= n + P + 1}$$

Here, n represents the number of bits in the data string and P represents number of parity bits.

For example, if we have 4 bit data string, i.e. n = 4, then the number of parity bits to be added can be found by using trial and error method.

Let's take P = 2, then
$2^P = 2^2 = 4$ and n + P + 1 = 4 + 2 + 1 = 7
This violates the actual expression.

So let's try P = 3, then
$2^P = 2^3 = 8$ and n + P + 1 = 4 + 3 + 1 = 8
So we can say that 3 parity bits are required to transfer the 4 bit data with single bit error correction.

After calculating the number of parity bits required, we should know the appropriate positions to place them in the information string, to provide single bit error correction. In the above considered example, we have 4 data bits and 3 parity bits. So the total codeword to be transmitted is of 7 (4 + 3) bits. We generally represent the data sequence from right to left, as shown below.

bit 7, bit 6, bit 5, bit 4, bit 3, bit 2, bit 1, bit 0

The parity bits have to be located at the positions of powers of 2. i.e. at 1, 2, 4, 8 and 16 etc. Therefore the codeword after including the parity bits will be like this

D7, D6, D5, P4, D3, P2, P1

Here P1, P2 and P3 are parity bits and D1-------D7 are data bits.

Now we have to see how to operate with this code word.
P1 depends on upon the value of D3, D5 and D7. P2 depends on upon the value of D3, D6 and D7 and similarly P4 depends on upon the value of D5, D6 and D7.
Now we are taking an example. We want to transmit a 4-bit data having value 1011. Now depending upon this data we have to remind the value of P1, P2 and P4. Here the D7, D6, D5 and D3 will have values 1011 respectively.

D7	D6	D5	P4	D3	P2	P1
1	0	1		1		

We know that P1 depends upon D3, D5 and D7.
P1=D3, D5, D7
P1= 1 1 1
To make it even parity, the value of P1 will be 1.

D7	D6	D5	P4	D3	P2	P1
1	0	1		1		1

P2 depends upon D3, D6 and D7.
P2= D3, D6, D7
P2= 1 0 1, to make it even parity the value of P2 will be 0.

D7	D6	D5	P4	D3	P2	P1
1	0	1		1	0	1

P4 depends on upon the value of D5, D6 and D7.
P4= D5, D6, D7
P4= 1 0 1, here also number of 1 is even, so the value P4 will be 0 to make it even parity.

D7	D6	D5	P4	D3	P2	P1
1	0	1	0	1	0	1

Therefore we have to transmit the codeword 1010101 with even parity. Now the receiver will analyse the codeword for error detection and correction. Receiver will check for the parity bit. If it is even parity, then there is no error and if the codeword is having no even parity, then there must be error. In this way error is detected using parity bit.
Now we are taking an example to show how error is corrected below.

Example- If the 7-bit hamming code word received by a receiver is 1011011 with even parity. State whether the code word received is correct or wrong.

Solution-
The 7-bit hamming code is

D7	D6	D5	P4	D3	P2	P1

1	0	1	1	0	1	1

P4 is associated D5, D6 and D7, i.e. it depends upon D5, D6 and D7.

P4	D5	D6	D7	
1	1	0	1	-which is odd parity

But the code word was transmitted with even parity, hence there must be error. Here we have seen number of 1 is 3, i.e is odd. So P4=1.

P2 is associated D3, D6 and D7, i.e. it depends upon D3, D6 and D7.

P2	D3	D6	D7	
1	0	0	1	-which is even parity

Hence, there is no error. Here we have seen number of 1 is 2, i.e is even. So P2=0.

P1 is associated D3, D5 and D7, i.e. it depends upon D3, D5 and D7.

P1	D3	D5	D7	
1	0	1	1	-which is odd parity

Hence, there is error. Here we have seen number of 1 is 3, i.e is odd. So P1=1.

We have to find out P4, P2 and P1depending upon whether they are depicting the true value or not.
P4 P3 P1 = 1 1 1 = (1 1 1)$_2$ = (5)$_{10}$
If we convert it to decimal, we get 5. Hence the 5th bit having the error, i.e. D5 is having the error and D5 should be 0 instead of 1. Hence the error has been located in the code word and error has been corrected at the receiver side.

STOP TO CONSIDER
We have three methods for detecting errors in frames. These are Parity Check, Checksum and Cyclic Redundancy Check (CRC). We may have single bit error and burst error in framing. Using Hamming Distance, this error can be corrected.

Check Your Progress-3

11. Parity checking is done by adding extra bit, called _____ bit.
12. Cyclic redundancy check (CRC) is also known as _____.
13. Normally a frame consists of m data bit and r _____ bits.
14. The number of bit positions in which two codewords differ is called _____ .
15. In _____ , the number of 1s is even.

1.8 SUMMING UP

- One of the major functions of Data Link Layer is to provide service to Network Layer.
- Unacknowledged connectionless service basically provides datagram modes delivery without any error, issue, or flow control.
- In acknowledged connectionless service, no logical connection is established between the source and destination host and each frame that is transmitted is acknowledged individually.
- In acknowledged connection-oriented service, first connection is established between the source and the destination. After that the data frames are transmitted by the sender using the newly established connection.
- The job of the data link layer is to break the bit stream into some frames and compute the checksum for each frame.
- In data link layer, character count method ensures the total number of characters present in the frame and the end of each frame at receiver side.

- In this bit stuffing method, additional bits are added to the data streams. A special bit pattern indicates the starting and end of the frame.
- In data link layer, error control is the process of detecting and correcting data frames that have been corrupted or lost during transmission.
- Flow control is a method which allows two stations working at different speeds to communicate with each other.
- In data link layer, the parity checking is done by adding an extra bit, called parity bit to the data to make a number of 1s either even to make it even parity or odd to make it odd parity.
- CRC or Cyclic Redundancy Check is a method of detecting accidental errors in the communication channel.
- In single bit error correction, only single bit error is corrected and in case of burst error correction, burst errors in the data sequence are detected and corrected.
- Normally a frame consists of m data (i.e. message) bits and r redundant bits.
- The number of bit positions in which two codewords differ is called Hamming distance.

1.9 ANSWERS TO CHECK YOUR PROGRESS

1.True 2.False 3.True 4.True 5.False 6.Framing 7.Character Count 8.Bits 9.Checksum 10.Flag 11. Parity 12.Polynomial Code 13.Redundant 14.Hamming Distance 15.Even

QUESTIONS AND ANSWERS

1. What is the upper layer of data link layer in OSI Reference Layer?
2. Give an example of unacknowledged connectionless service.

3. What is the basic unit for digital transmission in data link layer?
4. In which protocol, the sender sends a frame and waits for the acknowledgement?
5. Give an example single bit error detection method.
6. In case of odd parity number of 1s in _____.
7. _____ specify end of one frame and start of next frame in byte stuffing.

Answers: 1.Network Layer 2.Wifi 3.Frame 4.Stop and Wait 5.Parity Checking 6.odd 7. Two consecutive flag bytes

1.10 POSSIBLE QUESTIONS

Short answer type questions:

1. What is the lower layer of data link layer in OSI Reference Layer?
2. Give an example of unacknowledged connectionless service.
3. What is starting frame delimeter (SFD)?
4. What is bit oriented framing?
5. What is feedback based flow control?
6. What is burst error?
7. What is bit stuffing?
8. Why negative acknowledgement is used in error control?

Long answer type questions:

1. What are the different services provided by data link layer?
2. What are the major problems of framing?
3. Explain different Framing methods.
4. What are the different phases of error control mechanism in data link layer?
5. Explain the two principle ways for error correction?

6. Explain cyclic redundancy check (CRC) method with an example.
7. Explain how hamming distance metod can be used for single bit error correction?

1.11 FURTHER READINGS

1. Computer Networks, Andrew S. Tanenbaum, David J. Wetherall.
2. Data Communications and Networking, Behrouz A. Forouzan.

UNIT 2: The Data Link Layer: The Protocols

CONTENTS

2.1 INTRODUCTION

In this unit, you will learn about the second layer of the OSI model in computer networking, which is the Data Link Layer (DLL). It is also known as the protocol layer as it assumes responsibility of data transmission between adjacent network nodes in a wide area network (WAN) or between nodes on the same local area network (LAN) segment. This layer is involved in multiple activities including framing, addressing, synchronization, error control, flow control, and multi access. The different protocols and how they function to accomplish all the tasks will be discussed in detail in this unit.

2.2 UNIT OBJECTIVES

After going through this unit, you will be able to:

- Understand the functions of the data link layer.
- Know about data link layer protocols.
- Understand the concept of simplex, half duplex, and full duplex communication.
- Learn about noisy and noiseless channels.
- Learn about flow control protocols.

2.3 BASIC TERMS AND THEIR DEFINITIONS

When discussing about protocols in computer networks some terms find very frequent usage. For a better grip on the concepts let us learn about some of those basic terms here, to facilitate our learning.

i. **Data link frame**: A frame is a unit of communication in the data link layer. Data link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

ii. **Simplex:** The transmission mode defines the direction of signal flow between two connected devices. There exists three modes of communication, namely simplex, half-duplex, and full-duplex. A simplex mode of transmission the communication is unidirectional, or one-way, for e.g. keyboard, monitor etc.

iii. **Half-duplex:** The second type of transmission mode is the half-duplex, in such a transmission the communication is two-directional, but the channel is interchangeably used by both of the connected devices, for e.g. walkie talkie.

iv. **Full-duplex:** The third type of transmission mode is the full-duplex, in this transmission mode the communication is bi-directional or two-way, and the channel is used by both of the connected devices simultaneously, for e.g. telephone.

v. **Noiseless channel:** An idealistic channel in which no frames are lost, corrupted or duplicated is called a noiseless channel. The protocols do not implement error control in this category as it being an idealistic channel, it is considered to be error-free.

vi. **Noisy channel:** Unlike a noiseless channel, it is not an idealistic channel. A noisy channel signifies disturbances or occurrence of unwanted interference during data transmission from sender to receiver. It is also a practical and realistic approach towards data transmission, as noiseless channel is a hypothetical concept.

Check Your Progress-1

1. The _____ of signal flow between two _____ devices is defined by transmission mode.
2. A simplex mode of transmission is _____.
3. _____ is an example of a half-duplex device.
4. In _____ transmission mode both sender and receiver can communicate at the same time.
5. A noiseless channel is _____ in nature.

2.4 THE PROTOCOLS

Data-link frames do not cross the boundaries of a local network. Inter-network routing and global addressing are higher-layer functions, allowing data-link protocols to focus on local delivery, addressing, and media arbitration. The layer also takes care of flow control of the data as when devices attempt to use a medium simultaneously, frame collisions occur. Therefore, data-link protocols also specify how devices detect and recover from such collisions, and may provide mechanisms to reduce or prevent them. As the DLL assumes various roles and responsibilities, these are carried out with the help of some protocols specifically designed for the purpose. One of the major functions of the data link layer is to control the flow of data to and from the adjacent layers. A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.

Many protocols are defined for the data transmission in the DLL. The protocols have been categorized as shown in Fig 1.

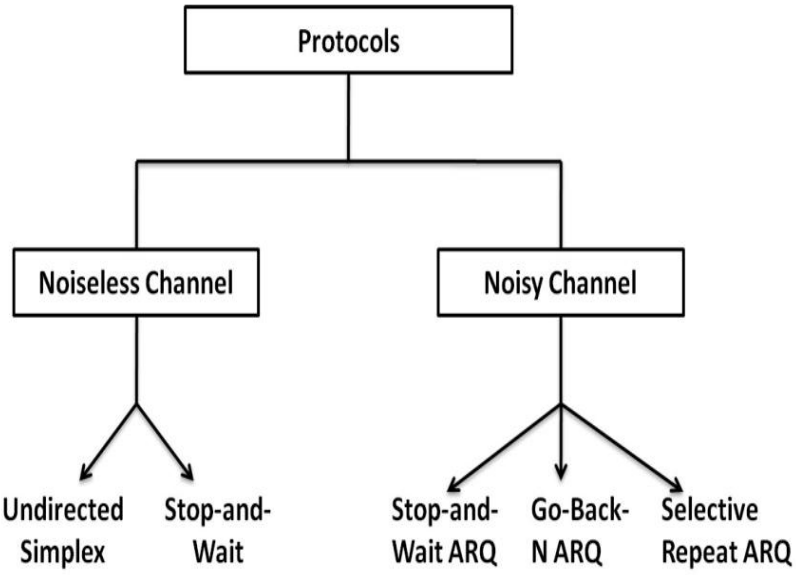


Fig 1: Categorization of flow control protocols

2.5 NOISELESS CHANNEL PROTOCOLS

In this type of noiseless protocol, no frames are lost, corrupted or duplicated. So no error control mechanism is implemented here. Some of the noiseless channel protocols are explained below.

2.5.1 UNRESTRICTED SIMPLEX PROTOCOLS

The simplex protocol is a data link layer protocol for transmission of frames over the computer network. It is a hypothetical protocol designed for unidirectional data transmission over an ideal channel, i.e. a channel through which transmission can never go wrong.

It is assumed that both the sender and the receiver are always ready for data processing and both of them have infinite buffer. The sender simply sends all the available data onto the channel as soon as buffer is available. The receiver is assumed to process all incoming data instantly. It does not handle flow control or error control. Since this protocol is totally unrealistic, it is often called Utopian Simplex protocol.

The significance of this protocol lies in the fact that it shows the basic structure on which the usable protocols are built.

Design:

- **Sender Side**: The data link layer in the sender side waits for the network layer to send a data packet. On receiving the packet, it immediately processes it and sends it to the physical layer for transmission.
- **Receiver Side**: The data link layer in the receiver side waits for a frame to be available. When it is available, it immediately processes it and sends it to the network layer.

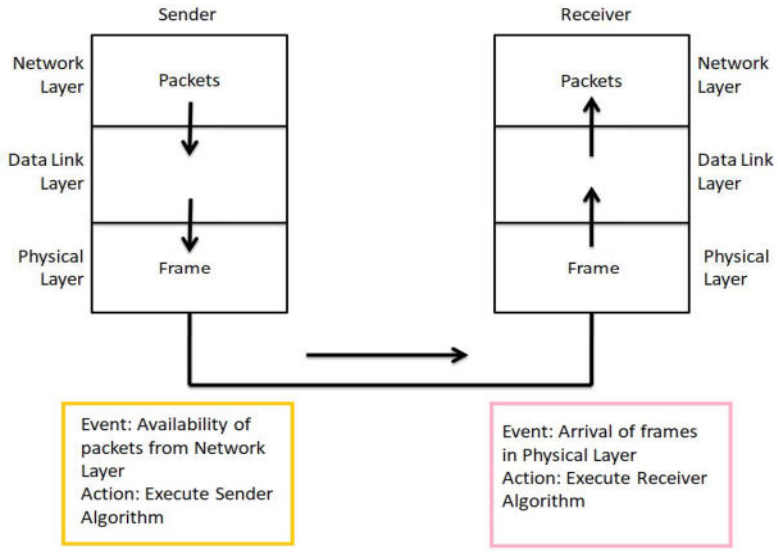


Fig 2: Unidirectional Simplex Protocol

```
     Algorithm
     Sender Side:
1    while (true)                          # repeat forever
2    {
3    EventWait();                          # sleep until an
                                             event occurs
4    if  (Event (SendRequest))             # there is a packet
                                             to send
5    {
6            GetData();
```

```
7           MakeFrame();
8           SendFrame();                    # send the frame
9   }
10  }
```

```
    Algorithm
    Receiver Side:
1   while (true)                            # repeat forever
2   {
3   EventWait();                            # sleep until an
                                              event occurs
4   if  (Event (ArrivalNotification))       # frame arrived
5   {
6           ReceiveFrame();
7           ExtractData();
8           DeliverData();                  # deliver data to
                                              network layer
9   }
10  }
```

The Fig 3 depicts communication via unrestricted simplex protocol for noiseless channel.

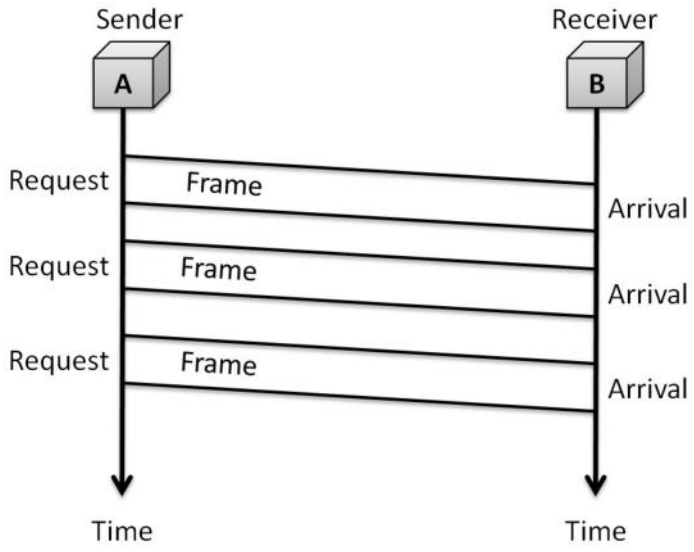


Fig 3: Flow of Unrestricted Simplex Protocol

2.5.2 SIMPLEX STOP-AND-WAIT PROTOCOL

Stop and Wait protocol is a data link layer protocol for transmission of frames over noiseless channels. It provides unidirectional data transmission with flow control facilities but without error control facilities.

This protocol takes into account the fact that the receiver has a finite processing speed. If data frames arrive at the receiver's end at a rate which is greater than its rate of processing, frames are dropped out. In order to avoid this, the receiver sends an acknowledgement for each frame upon its arrival. The sender sends the next frame only when it has received a positive acknowledgement from the receiver that it is available for further data processing.

Design

- **Sender Side**: The data link layer in the sender side waits for the network layer for a data packet. It then checks whether it can send the frame. If it receives a positive notification from the physical layer, it makes frames out of the data and sends it. It then waits for an acknowledgement before sending the next frame.
- **Receiver Side**: The data link layer in the receiver side waits for a frame to arrive. When it arrives, the receiver processes it and delivers it to the network layer. It then sends an acknowledgement back to the sender.

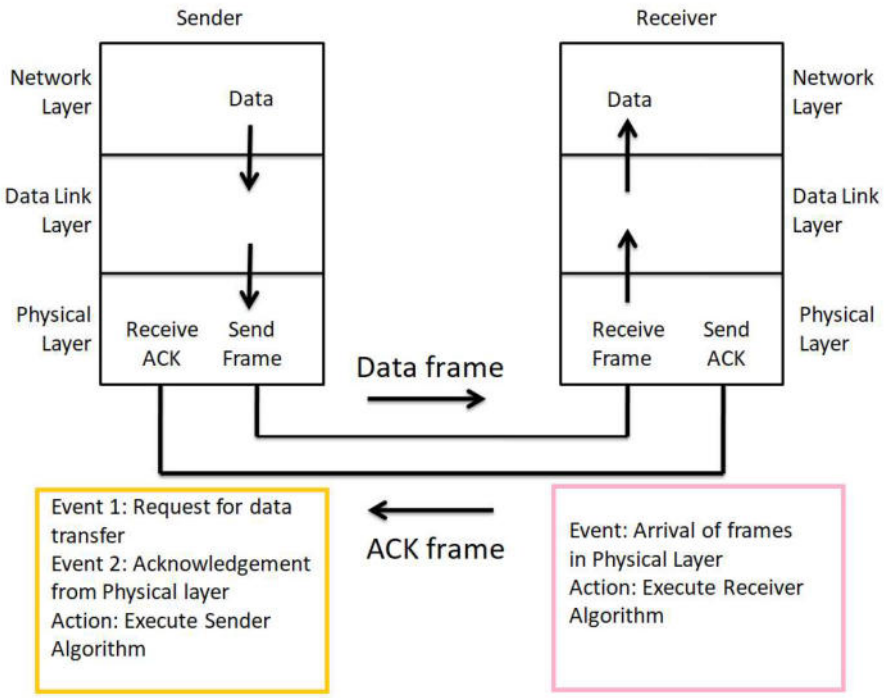


Fig 4: Simplex Stop-and-Wait protocol

```
     Algorithm
     Sender Side:
1    while (true)                          # repeat forever
2    canSend = true;                       # allow first frame to
                                           go
3    {
4    EventWait();                          # sleep until an event
                                           occurs
5    if  (Event (SendRequest) AND          # there is a packet to
     canSend)                              send
6    {
7            GetData();
8            MakeFrame();
9            SendFrame();                  # send the frame
10           canSend = false;              # cannot send until
                                           ACK arrives
11   }
12   EventWait();                          # sleep until an event
                                           occurs
```

```
13  if  (Event (ArrivalNotification))        # an ACK has arrived
14  {
15          ReceiveFrame();                  # receive the ACK
                                               frame
16          canSend = true;
17  }
18  }
```

```
    Algorithm
    Receiver Side:
1   while (true)                             # repeat forever
2   {
3   EventWait();                             # sleep until an
                                               event occurs
4   if  (Event (ArrivalNotification))        # frame arrived
5   {
6           ReceiveFrame();
7           ExtractData();
8           DeliverData();                   # deliver data to
                                               network layer
9           SendFrame();                     # send an ACK
                                               frame
10  }
11  }
```

The Fig 6 depicts communication via simplex stop–and–wait protocol for noiseless channel.

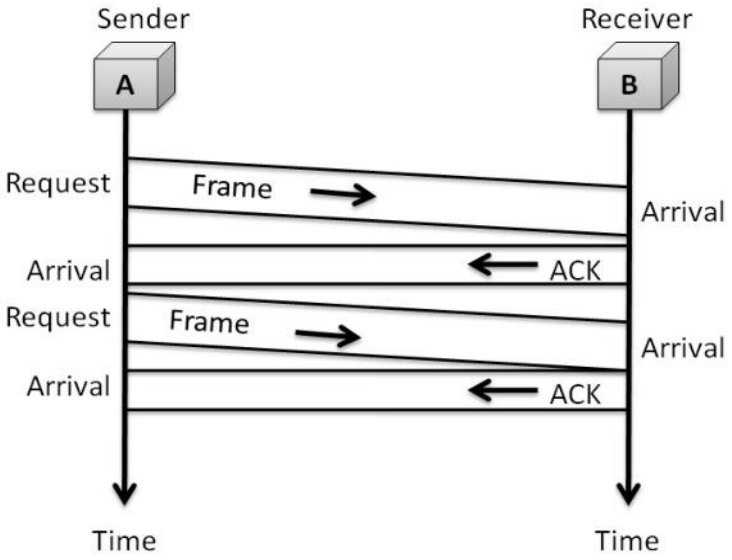


Fig 5: Communication via Simplex Stop-and-Wait protocol

STOP TO CONSIDER

- Data link layer protocols can be categorized on the basis of type of channel, i.e. noiseless or noisy.
- Flow control is a way of controlling the amount of data being sent or received in order to avoid unnecessary collisions and reduce network traffic or congestion.

Check Your Progress-2

8. The unrestricted simplex protocol can be implemented for a _____ channel.
9. State true or false:
   a. In unrestricted protocol it is assumed that both stations have infinite buffer.
   b. Simplex Stop-and-Wait allows data transmission with error control facilities but without flow control facilities.

2

U
c
unwanted interference during data transmission from sender to receiver. Some of the noisy channel protocols are explained below.

2.6.1 SIMPLEX PROTOCOL FOR NOISY CHANNEL

Simplex Stop and Wait protocol for noisy channel is a data link layer protocol for data communications with error control and flow control mechanisms. It is popularly known as Stop–and–Wait Automatic Repeat Request (Stop–and–Wait ARQ) protocol. It adds error control facilities to Stop–and–Wait protocol.

This protocol takes into account the facts that the receiver has a finite processing speed and that frames may get corrupted while transmission. If data frames arrive at the receiver's end at a rate which is greater than its rate of processing, frames can be dropped out. Also, frames may get corrupted or entirely lost when they are transmitted via network channels. So, the receiver sends an acknowledgment for each valid frame that it receives. The sender sends the next frame only when it has received a positive acknowledgment from the receiver that it is available for further data processing. Otherwise, it waits for a certain amount of time and then resends the frame.

Design:

- **Sender Side**: At the sender side, a field is added to the frame to hold a sequence number. If data is available, the data link layer makes a frame with the certain sequence number and sends it. The sender then waits for arrival of acknowledgment for a certain amount of time. If it receives a positive acknowledgment for the frame with that sequence number within the stipulated time, it sends the frame with next sequence number. Otherwise, it resends the same frame.
- **Receiver Side**: The receiver also keeps a sequence number of the frames expected for arrival. When a frame arrives, the receiver processes it and checks whether it is valid or not. If it is valid and its sequence number matches the sequence number of the expected frame, it extracts the data and delivers it to the network layer. It then sends an acknowledgement for that frame back to the sender along with its sequence number.

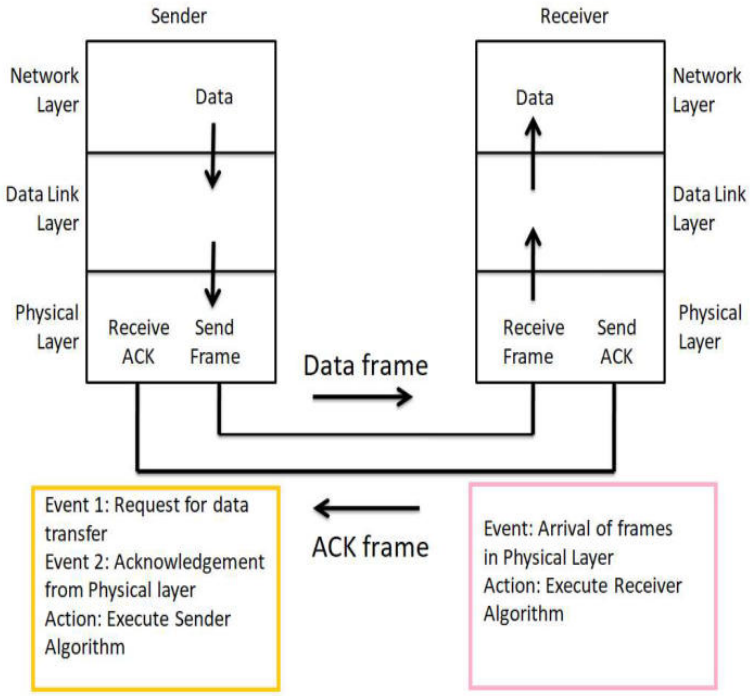


Fig 6: Stop-and-Wait Protocol for noisy channel

The following flow diagram depicts communication via simplex stop – and – wait ARQ protocol for noisy channel −

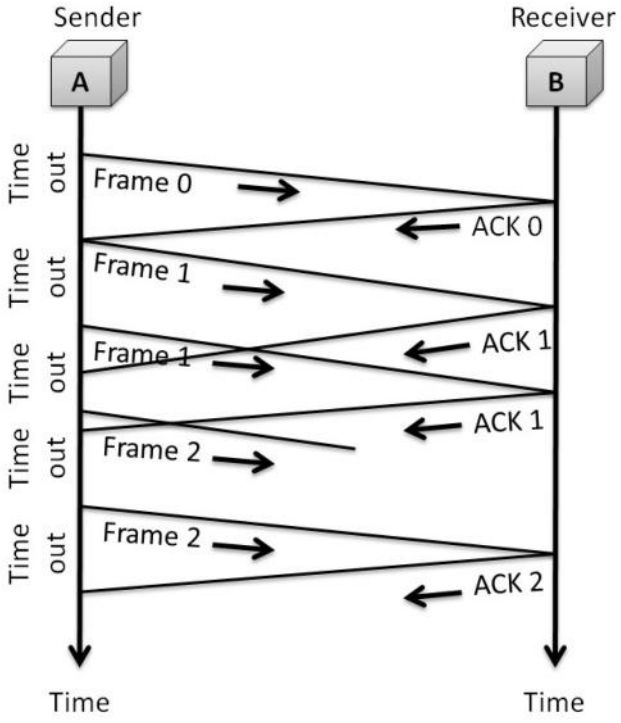


Fig 7: Communication via Simplex Stop-and-Wait ARQ protocol for noisy channel

The Stop-and-Wait protocol is inefficient if the channel is thick and long. By thick, a channel with a large bandwidth is indicated and by long the round trip delay is indicated to be long. The product of both is the bandwidth delay product. The bandwidth delay product is a measure of the number of bits that can be sent out of the system while waiting for news from the receiver.

Example 1:

Assume that in a Stop-and-Wait ARQ system, the bandwidth of the line is 1.5 Mbps, and 1 bit takes 10 ms to make a round trip. What is the bandwidth delay product? If the system data frames are 1000 bits in length, what is the utilization percentage of the link?

Solution: The bandwidth delay product is $(1.5\times10^{6})\times(10\times10^{-3})$ = 15,000 bits

The system can send 15,000 bits during the time it takes for the data to go from sender to receiver and back to again. But, the system sends only 1000 bits. We can say that the link utilization is only 1000/15,000, or 6.67%. For this reason, for a link with a high bandwidth or long delay, the use of Stop-and-Wait ARQ wastes the capacity of the link.

Example 2:

In the previous example what is the utilization percentage of the link if we have a protocol that can send up to 10 frames before stopping and worrying about acknowledgements?

Solution: The bandwidth delay product continues to be 15,000 bits. The system can send up to 10 frames or 10,000 bits during a round trip. This means the utilization is 10,000/15,000, or 66.67%. In case there are damaged frames, the utilization percentage is much less as frames have to be resent.

2.6.2 SLIDING WINDOW PROTOCOL

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this technique, each sending frame has the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number. Sliding window protocol has two types:

1. Go-Back-N ARQ
2. Selective Repeat ARQ

2.6.2.1 PROTOCOL USING GO BACK N

In Go-Back-N ARQ, **N** is the sender's window size. Suppose we say that Go-Back-3, which means that the three frames can be sent at a time before expecting the acknowledgment from the receiver. It uses the principle of protocol pipelining in which the multiple frames can be sent before receiving the acknowledgment of the first frame. If we have five frames and the concept is Go-Back-3, which means that the three frames can be sent, i.e., frame no 1, frame no 2, frame no 3 can be sent before expecting the acknowledgment of frame no 1.

In Go-Back-N ARQ, the frames are numbered sequentially as Go-Back-N ARQ sends the multiple frames at a time that requires the numbering approach to distinguish the frame from another frame, and these numbers are known as the sequential numbers. The number of frames that can be sent at a time totally depends on the size of the sender's window. So, we can say that 'N' is the number of frames that can be sent at a time before receiving the acknowledgment from the receiver. If the acknowledgment of a frame is not received within an agreed-upon time period, then all the frames available in the current window will be retransmitted. Suppose we have sent the frame no 5, but we didn't receive the acknowledgment of frame no 5, and the current window is holding three frames, then these three frames will be retransmitted.

The sequence number of the outbound frames depends upon the size of the sender's window. Suppose the sender's window size is 2, and we have ten frames to send, then the sequence numbers will not be 1,2,3,4,5,6,7,8,9,10. Let's understand through an example.

- N is the sender's window size.
- If the size of the sender's window is 4 then the sequence number will be 0,1,2,3,0,1,2,3,0,1,2, and so on.

The number of bits in the sequence number is 2 to generate the binary sequence 00,01,10,11.

Example 3:

A 2 Mbps satellite link connects two ground stations. The altitude of the satellite is 36504 km and speed of the signal is 3 x 10^8 m/sec. What should be the packet size for a channel utilization of 50% for a satellite link using go back 127 sliding window protocol?

Solution: Given-

Bandwidth = 2 Mbps

Distance = 2 x 36504 km = 73008 km

Propagation speed = 3 x 10^8 m/sec

Efficiency = 50% = 1/2

Go back N is used where N = 127

Let the packet size be L bits.

Transmission delay (T_t) = Packet size / Bandwidth

= L bits / 2 Mbps

=0.5 L μsec

Propagation delay (T_p) = Distance / Speed

= (73008 x 10^3 m) / (3 x 10^8 m/sec)

= 24336 x 10^{-5} sec

= 243360 μsec

$a = T_p / T_t$

a = 243360 μsec / 0.5L μsec

a = 486720 / L

Efficiency (η) = N / (1+2a)

Substituting the values, we get-

1/2 = 127 / (1 + 2 x 243360 / L)

1/2 = 127 x L / (L + 486720)

L + 486720 = 254 x L

253 x L = 486720

L = 1924

From here, packet size = 1924 bits or 240 bytes.

Example 4:

A 20 Kbps satellite link has a propagation delay of 400 ms. The transmitter employs the "go back n ARQ" scheme with n set to 10. Assuming that each frame is 100 bytes long, what is the maximum data rate possible?

Solution: Given-

Bandwidth = 20 Kbps

Propagation delay (T_p) = 400 ms

Frame size = 100 bytes

Go back N is used where N = 10

Transmission delay (T_t) = Frame size / Bandwidth = 100 bytes / 20 Kbps

= (100 x 8 bits) / (20 x 10^3 bits per sec)

= 0.04 sec

= 40 msec

$a = T_p / T_t$

a = 400 msec / 40 msec

a = 10

Efficiency (η) = N / (1+2a) = 10 / (1 + 2 x 10)

= 10 / 21

= 0.476

= 47.6 %

Maximum data rate possible or Throughput

= Efficiency x Bandwidth

= 0.476 x 20 Kbps

= 9.52 Kbps

≅ 10 Kbps

2.6.2.1 PROTOCOL USING SELECTIVE REPEAT

Selective repeat protocol, also called Selective Repeat ARQ (Automatic Repeat Request), is a data link layer protocol that uses sliding window method for reliable delivery of data frames. Here, only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

It uses two windows of equal size: a sending window that stores the frames to be sent and a receiving window that stores the frames receive by the receiver. The size is half the maximum sequence number of the frame. For example, if the sequence number is from 0 – 15, the window size will be 8.

Working Principle:

Selective Repeat protocol provides for sending multiple frames depending upon the availability of frames in the sending window, even if it does not receive acknowledgement for any frame in the interim. The maximum number of frames that can be sent depends upon the size of the sending window.

The receiver records the sequence number of the earliest incorrect or un-received frame. It then fills the receiving window with the subsequent frames that it has received. It sends the sequence number of the missing frame along with every acknowledgement frame. The sender continues to send frames that are in its sending window. Once, it has sent all the frames in the window, it retransmits the frame whose sequence number is given by the acknowledgements. It then continues sending the other frames.

STOP TO CONSIDER

- In Stop-and-Wait ARQ, an improvisation was made to the simplex Stop-and-Wait by adding an error control mechanism.
- In Go-Back-N ARQ a number of frames are sent sequentially before receiving acknowledgement to improve transmission efficiency.
- In Selective Repeat only lost or erroneous frames are resent.

Check Your Progress-3

10. ARQ stands for _____.
11. The Stop-and-Wait protocol is inefficient if the channel is _____ and _____.
12. The purpose of the sliding window technique is to avoid _____ data, so it uses the _____ number.
13. State true or false
    a. In Stop-and-Wait ARQ the sender sends an acknowledgement on receiving acknowledgement from receiver.
    b. The concept of acknowledgement and timeout is introduced in Stop-and-Wait for noisy channels.
    c. TCP stands for Transportation Control Protocol.
    d. 'N' in Go-Back-N ARQ is the number of frames that can be sent at a time before receiving the acknowledgment from the receiver.

2.7 HDLC (HIGH-LEVEL DATA LINK CONTROL)

HDLC (High-level Data Link Control) is a group of protocols or rules for transmitting data between network points (sometimes called nodes).

In more technical terms, HDLC is a bit-oriented, synchronous data link layer protocol created by the International Organization for Standardization (ISO). The standard for HDLC is ISO/IEC 13239:2002. ECI stands for the International Electrotechnical Commission, an international electrical and electronic standards body that often works with the ISO.

Working Principle:

HDLC provides two common transmission modes namely normal response mode (NRM) and asynchronous balanced mode (ABM).

In normal response mode the station configuration is imbalanced. There exists one primary station and multiple secondary stations. While a primary station is used for sending instructions or commands, the secondary stations are only capable of responding. The NRM is applied at both point-to-point as well as multi-point links.

In asynchronous balanced mode as the name suggests, the station configuration is balanced. The link is point-to-point, and each station acts as both primary and secondary stations (act as peers).

To provide flexibility, HDLC basically uses and explains three different types of frames:

1. I-Frames (Information)
2. S-Frames (Supervisory)
3. U-Frames (Unnumbered)

Type of frame is basically determined by control field of frame. Each type of frame generally serves as an envelope for transmission of various types of messages.

I-frame stands for Information frames. This frame is generally used for transporting user data from network layer. These frames actually carry actual data or information of upper layer and some control information. This frame carries data along with both send sequence number and an acknowledgment number. It can also be used to piggyback acknowledgment information in case of ABM (Asynchronous Balanced Mode). The first bit of this frame of control filed is 0.

S-frame stands for Supervisory frames. These frames are basically required and essential for error control and flow control. They also provide control information. It contains or includes only an Acknowledgment number. First two bit of this frame of control filed is 10. S-frame does not have any information fields. This frame contains send and receives sequence numbers.

U-frame stands for Unnumbered frames. These frames are also required in various functions like link setup and disconnections. These frames basically support control purposes and are not sequenced. First two bit of this frame of control filed is 11. Some

U-frames contain an information field depending upon type. These frames are also used for different miscellaneous purposes along with link management. U-frame is required for managing link itself. This frame does not include any type of acknowledgment information i.e. in turn it includes or contained in sequence number. These frames are generally reserved for system management.

Each frame in the HDLC frame format consists up to six fields as shown in Fig 6.

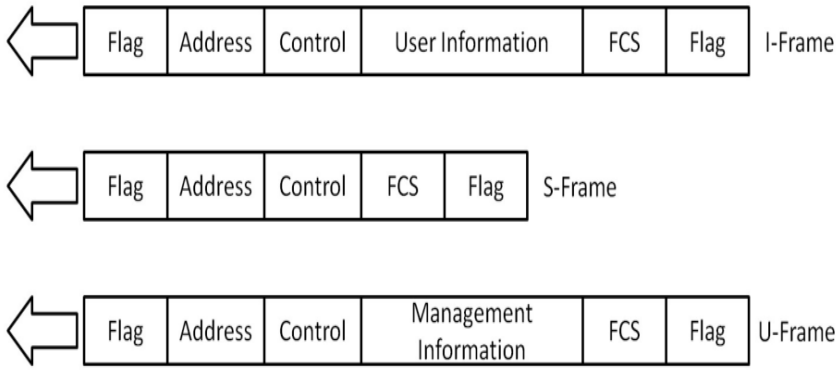


Fig 8: Frame format fields in HDLC

The functions of the different fields are as follows:

- Flag field: The flag field of an HDLC frame is an 8-bit sequence with the bit pattern 01111110 that identifies both the beginning and the end of a frame and serves as a synchronization pattern for the receiver.
- Address field: The second field of an HDLC frame contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary creates the frame, it contains a from address. An address field can be 1 byte or several bytes long depending on the needs of the network.
- Control field: The control field is a 1 or 2 byte segment of the frame used for flow and error control. The interpretation of bits in this field depends on the frame type.

- Information field: The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.
- FCS field: The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte ITU-T CRC.

Check Your Progress-4

14. The maximum window size for data transmission using the selective repeat protocol with n bit frame sequence numbers is _____.

15. In selective repeat only the _____or _____frames are retransmitted.

16. HDLC is a _____oriented protocol.

17. NRM is applied to both _____as well as _____links.

STOP TO CONSIDER

- HDLC protocol is a bit oriented protocol which is used for data transmission that classifies frames into I-Frame, S-Frame, and U-Frame.

2.8 SUMMING UP

- The second layer of the OSI model i.e. the Data Link Layer is responsible for data transmission between the Physical and Network Layers.
- For accomplishing various tasks on the network the DLL implements certain protocols specific to data transmission activities.

- Protocols can be categorized on the basis of type of channel: noiseless or noisy.
- Flow control is the task of controlling amount of data being sent or received in order to avoid unnecessary collisions and reduce network traffic or congestion.
- For noiseless channels we discussed Unrestricted Simplex protocol and Simplex Stop-and-Wait protocol which lack either flow control or error control activities or both.
- For noisy channels we discussed Stop-and-Wait ARQ, Go-Back-N ARQ and Selective Repeat protocols. In Stop-and-Wait ARQ, an improvisation was made to the simplex Stop-and-Wait by adding an error control mechanism. In Go-Back-N ARQ a number of frames are sent sequentially before receiving acknowledgement to improve transmission efficiency, and in Selective Repeat only lost or erroneous frames are resent.
- Both Go-Back-N ARQ and Selective Repeat use the concept of sliding window. If m is the number of bits for the sequence number, then the size of the send window must be less than 2^m, size of the receiver window must always be 1. In Selective repeat the size of sender and receiver window must be at most one half of 2^m.
- HDLC protocol is a bit oriented protocol used for data transmission which classifies frames into I-Frame, S-Frame, and U-Frame.

2.9 ANSWERS TO CHECK YOUR PROGRESS

1. Direction, Connected
2. Unidirectional
3. Walkie talkie
4. Full-duplex
5. Idealistic
6. Noisy
7. a.True, b.False, c.False
8. Noiseless
9. a.True, b.False
10. Automatic Repeat Request
11. Thick, Long

12. Duplicate, Sequence
13. a.False, b.True, c False, d.True
14. 2^{n-1}
15. Erroneous, Lost
16. Bit
17. Point-to-point, Multi-point

Multiple Choice Questions

1. Which of the following is a data link layer protocol?
   a) Ethernet
   b) Point to point protocol
   c) HDLC
   d) All of the mentioned

2. Which task is not performed by the data link layer?
   a) Framing
   b) Error control
   c) Flow control
   d) Channel coding

3. The DLL extracts packets from _____ and encapsulates them into frames for transmission.
   a. Network layer
   b. Physical layer
   c. Transport layer
   d. Application layer

4. The shortest frame in the HDLC protocol is the
   a. Information Frame
   b. Supervisory Frame
   c. Unnumbered Frame
   d. None of the above

5. When a NAK is received, all the frames since the last acknowledged frame are resent in the _____ protocol.
   a. Stop-and-Wait
   b. Go-Back-N ARQ

c. Selective Repeat ARQ
d. Both a and c

Answers: 1.d, 2.d, 3.a, 4.b, 5.b

State true or false

1. The second field of an HDLC frame is an 8-bit sequence with the bit pattern 01111110**.**
2. The Information field in the HDLC contains information from the network layer.
3. HDLC uses three frames to improve efficiency.
4. Selective Repeat protocol allows sending of multiple frames depending upon the availability of frames in the sending window.
5. The purpose of sliding window is to back up data by generating its duplicates.
6. In Go-Back-N ARQ, N is the receiver's window size.
7. In noisy channel frames are lost but not corrupted.
8. In Simplex Stop-and-Wait protocol there is no concept of Time Out.

1.False, 2.True, 3.True, 4.True, 5.False, 6.False, 7.False, 8.True

2.10 POSSIBLE QUESTIONS

Short answer type questions:

1. What is protocol?
2. State three examples of half-duplex transmission mode.
3. Define framing and the reason for its need.
4. Differentiate between noiseless and noisy channels.
5. What are the two sliding window protocols?
6. What is the size of the window for Go-Back-N ARQ Protocol?
7. What is the size of the window for Selective Repeat ARQ Protocol?
8. Give the full forms of: NRM, ABM
9. Differentiate between NRM and ABM.
10. What is bandwidth propagation delay?
11. Differentiate between I-Frame and S-Frame.
12. Why is the U-Frame used in HDLC?

13. What is frame check sequence?

Long answer type questions:

1. Discuss the functions of the Data Link Layer.
2. Distinguish between Simplex, Half-Duplex and Full-Duplex.
3. Describe the Unrestricted Simplex Protocol for Noiseless channel.
4. Differentiate between the Stop-and-Wait protocols for noiseless and noisy channels.
5. Explain with reasons why Go-Back-N ARQ was introduced and how it improved Stop-and-Wait protocol.
6. What are the advantages of Selective Repeat ARQ over other transmission protocols?
7. Compare and contrast the two sliding window protocols.
8. How is the HDLC Protocol different form the other data transmission protocols?
9. Elaborate the types of data frames used by the HDLC Protocol.
10. What are the fields used in the HDLC frame formats?

2.11 FURTHER READINGS

1. Computer Networks, Andrew S. Tanenbaum, David J. Wetherall.

2. Data Communications and Networking, Behrouz A. Forouzan

UNIT 3:

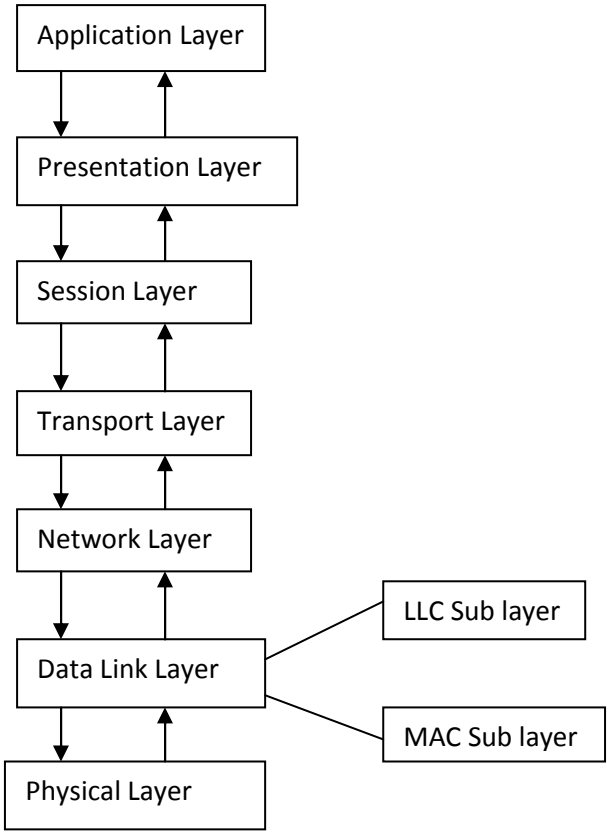
Unit Structure:

3.1 INTRODUCTION TO MAC SUBLAYER

SPACE FOR LEARNER NOTE

Network can be divided into two categories: 1) Point to point and 2) Broadcast Channels. MAC sub layer deals with broadcast networks and their protocols. It is also known as the Media Access Control is a sub layer of the data link layer. It shares a common communication medium and these are local area networks. This layer is the "low" part of the second OSI layer. The IEEE divided this layer into two layers "above" is the control layer the logical connection (Logical Link Control, LLC) and "down "the control layer the medium access (MAC).

The following diagram depicts the position of the MAC layer-



3.1.1. FUNCTIONS OF MAC SUB LAYER:

1) It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.

2) It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.

3) It resolves the addressing of source station as well as the destination station or groups of destination stations.

4) It performs multiple access resolutions when more than one data frame is to be transmitted.

5) MAC deals with broadcast channels and is especially important in LANs, many of which use a multi-access channel as the basis of communication.

3.2 THE CHANNEL ALLOCATION PROBLEM IN COMPUTER NETWORK

Channel allocation is a process in which a single channel is divided and allotted to multiple users for user specific tasks. User's quantity may vary every time the process takes place.
If there is M number of users and channel is divided into M equal-sized sub channels, each user is assigned one portion. If the number of users are small and don't vary at times, than Frequency Division Multiplexing can be used.
Channel allocation problem can be solved by two schemes:
1) Static channel allocation in LANs and MANs and
2) Dynamic channel allocation.

3.2.1. STATIC CHANNEL ALLOCATION IN LANs AND MANS

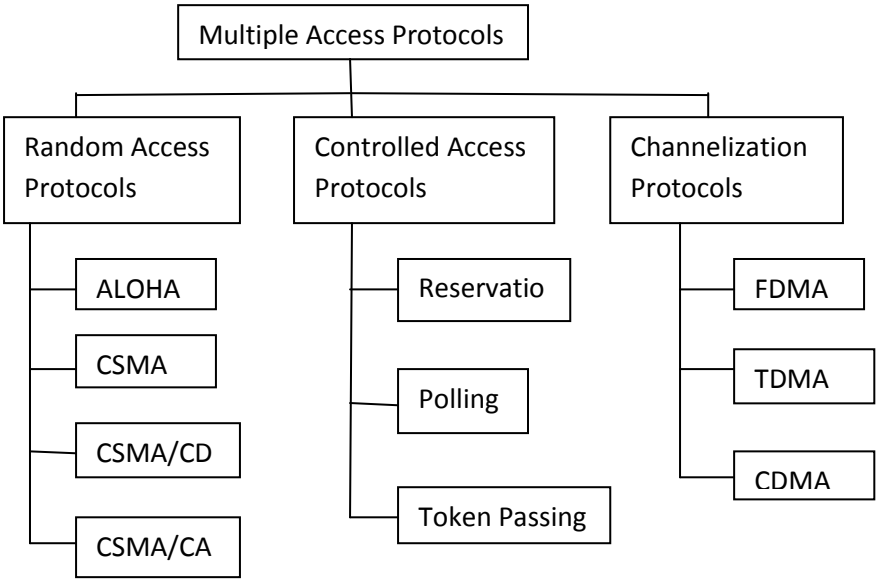
It is a approach of allocating a single channel among multiple competing users Frequency Division Multiplexing (FDM). If there are M users, the bandwidth is divided into M equal sized portions, each user being assigned one portion. Since, each user has a private frequency band, there is no interface between users.

STOP TO CONSIDER

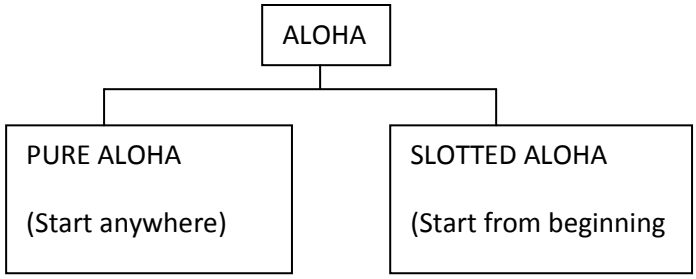
T=1/(U*C-L)
T(FDM)=N*T(1/U(C/N)-L/N)
Where T=mean time delay,
C=Capacity of channel,
L=arrival rate of frames,
1/U=bits/frame,
N=number of sub channels,
T(FDM)=Frequency Division Multiplexing Time.

3.2.2. DYNAMIC CHANNEL ALLOCATION

Possible assumptions include:
1) Station Model: Assumes that each of N stations independently produce frames.
2) Single Channel Assumption: Here all stations are equivalent and can send and receive on that channel.
3) Collision Assumption: If two frames overlap in time-wise, then collision occurs. Any collision is an error and both frames must be re-transmitted.
4(a) Continuous Time: Frame transmission can begin at any instant. There is no master clock dividing time into discrete intervals.
4(b) Slotted Time: Time is divided into discrete intervals (slots). Frame transmissions always begin at the start of a slot.
5(a) Carrier Sense: Stations can tell if the channel is in use before trying to use it. If the channel is sensed as busy, no station will attempt to use it until it goes idle.
5(b) No Carrier Sense: Stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later they determine whether the transmission was successful.



3.3. ALOHA

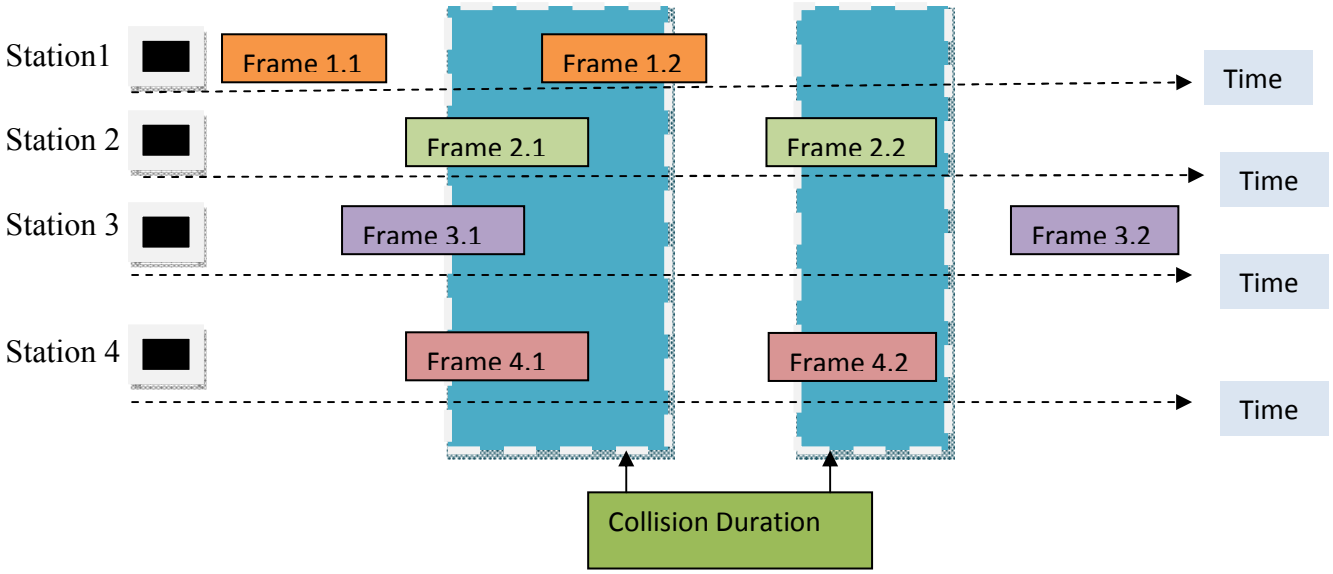


3.3.1. PURE ALOHA

The original ALOHA protocol is called pure ALOHA. This is simple but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is the possibility of collision between the frames from different stations. Figure below shows an example of frame collisions in pure ALOHA.

SPACE FOR LEARNER NOTE

Figure: Frames in a pure ALOHA network

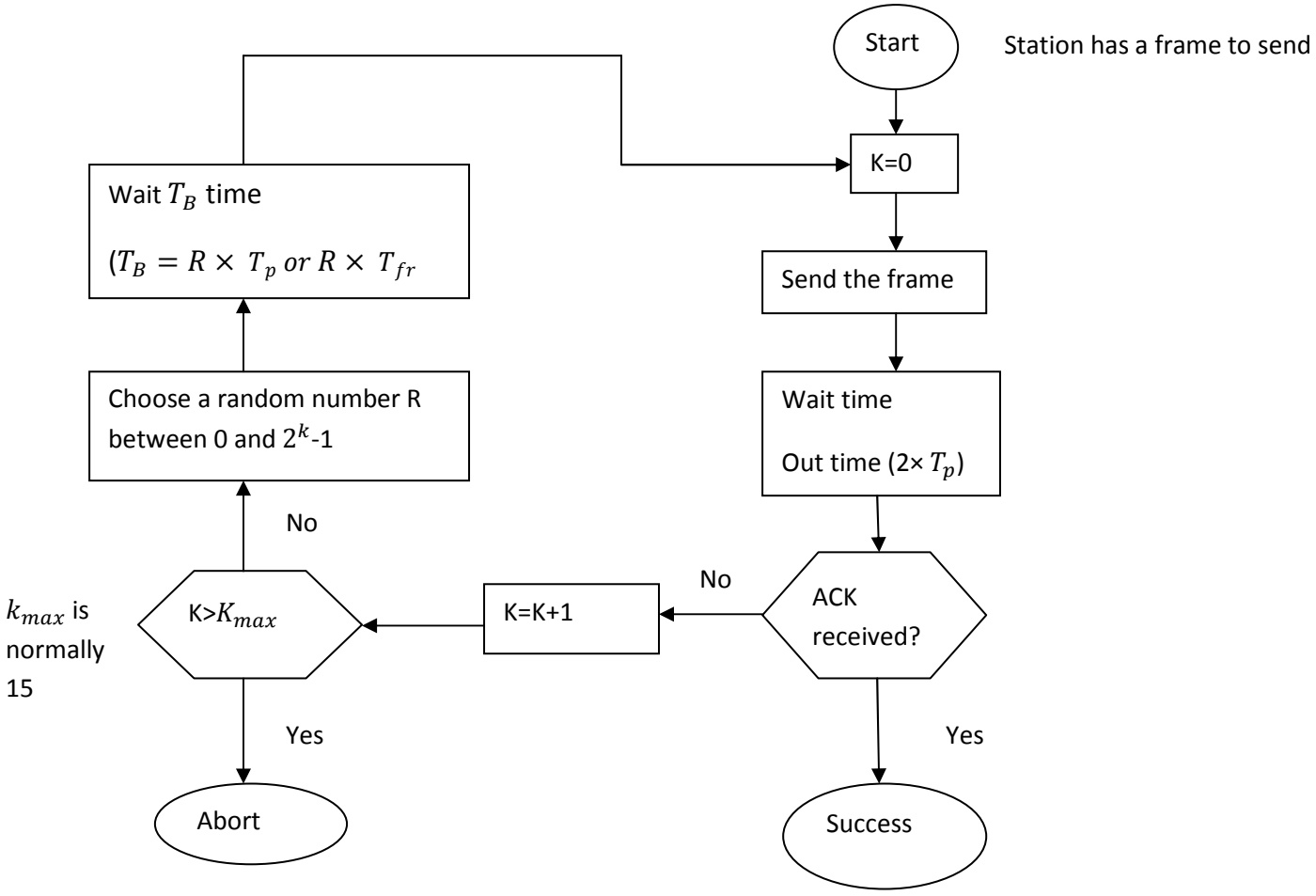


There are four stations that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. Figure shows that only two frames survive: frame 1.1 from station1 and frames 3.2 from station 3. Even if one bit of frame coexists on the channel with one bit from another frame, there is a collision and both will destroyed.

It is obvious that we need to resend the frames that have been destroyed during transmission. The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.

A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back-off timeT_B.

Figure: - Procedure pure ALOHA protocol



STOP TO CONSIDER

K: Number of attempts

T_p: Maximum propagation time

T_{fr}: Average transmission time for a frame

T_B : Back off time

Pure ALOHA vulnerable time=2× T_{fr}

The throughput for pure ALOHA is S=G×e^{-2G}

The maximum throughput S_{max}=0.184 when G= (1/2)

Problem 1: A pure ALOHA network transmits 200bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces?

a) 1000 frames per second.

b) 500 frames per second.

c) 250 frames per second.

Solution: The frame transmission time is 200/200 kbps or 1ms.

a) If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case, S=G×e^{-2G} or S=0.135, here G=1.

b) If the system creates 500 frames per second, this is (1/2) frames per millisecond. The load is (1/2). In this case, S=G×e^{-2G} or S=0.184 (18.4%). This means that the throughput is 500×0.184=92 and that only 92 frames out of 500 will probably survive.

c) If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case, S=G×e^{-2G} or S=0.152 (15.2%). This means that the throughput is 250×0.152=38. Only 38 frames out of 250 will probably survive.

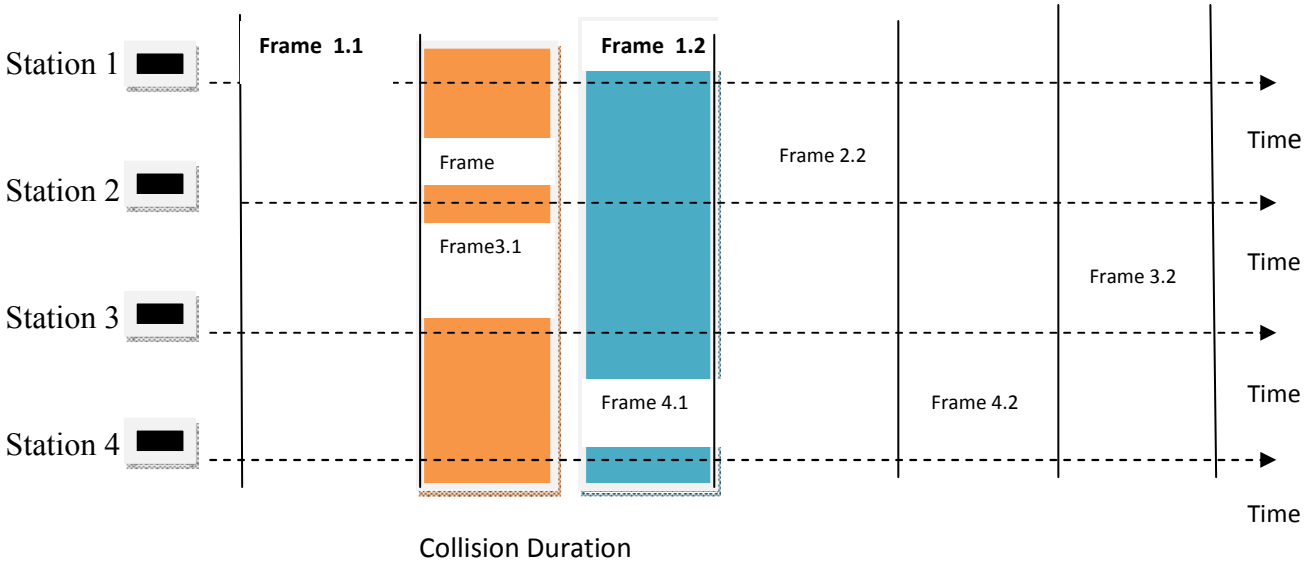
3.3.2. SLOTTED ALOHA

Pure ALOHA has a vulnerable time of $2\times T_{fr}$. This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.

In slotted ALOHA we divide the time into slots of T_{fr} and force the station to send only at the beginning of the time slot. Figure shows an example of frame collisions in slotted ALOHA.

SPACE FOR LEARNER NOTE

Figure: Frames in a slotted ALOHA network



Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame. But there is still the possibility of collisions if two stations try to send at the beginning of the same time slot. So, the vulnerable time is now reduced to one-half,

equal toT_{fr}. Figure shows the situation. Also show that the vulnerable time for slotted ALOHA is one-half that of pure ALOHA.

Slotted ALOHA vulnerable time= T_{fr}

The throughput for slotted ALOHA is S=G×e^{-G}

The maximum throughput S_{max}=0.368 when G=1.

Problem 2: A slotted ALOHA network transmits 200 bit frames using a shared channel with a 200 kbps bandwidth. Find the throughput if the system (all stations together) produces

a) 1000 frames per second.

b) 500 frames per second.

c) 250 frames per second.

Solution: The frame transmission time is 200/200 kbps or 1 ms.

a) In this case G is 1. So, S=G×e^{-G} $or\ S = 0.368\ (36.8\%)$. This means that the throughput is 1000×0.0368=368 frames. Only 368 out of 1000 frames will probably survive.

b) Here G is ½. In this case S=G×e^{-G} $or\ S = 0.303\ (30.3\%)$. This means that the throughput is 500×0.303= 151. Only 151 frames out of 500 will probably survive.

c) Now G is ¼. In this case S=G×e^{-G} $or\ S = 0.195\ (19.5\%)$. This means that the throughput is 250×0.195=49. Only 49 frames out of 250 will probably survive.

Check Your Progress 1

1. State whether true or false

   a) MAC sub layer using broadcast networks and their protocol.

   b) LLC is down layer of data link layer.

   c) MAC layer is responsible for encapsulating frames.

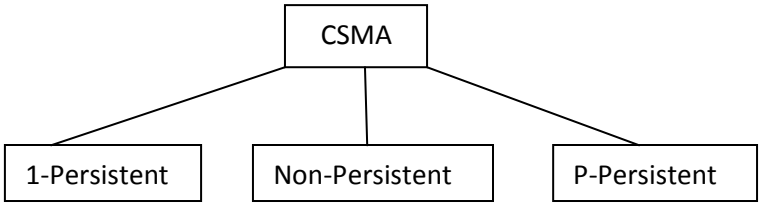
   d) ALOHA is a random access protocols.

2. Fill in the blanks:

   a) In …… ALOHA, it starts anywhere.

   b) ……. ALOHA improves the efficiency of ……. ALOHA

3.4. CARRIER SENSE MULTIPLE ACCESS (CSMA)



3.4.1. 1-Persistent

The 1-persistent method is simple and straight forward. In this method, after the station finds the line idle, its sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

3.4.2. Non-Persistent

In the non-persistent method, a station has a frame to send senses the line. If the line is idle, it waits a random amount of time and then senses the line again. The non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount and retry to send simultaneously. However, this method reduces the efficiency of network because the medium remains idle when there may be stations with frames to send.

3.4.3. P-Persistent

The p-persistent method is used if the channel has time slots with slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collisions and improves efficiency. In this method, after the station finds the line idle it follows these steps:

1. With probability p, the station sends its frame.
2. With probability q=1-p, the station waits for the beginning of the next time slot and checks the line again.

SPACE FOR LEARNER NOTE

Figure: Flow diagram for three persistence methods
Figure (a): 1-Persistant

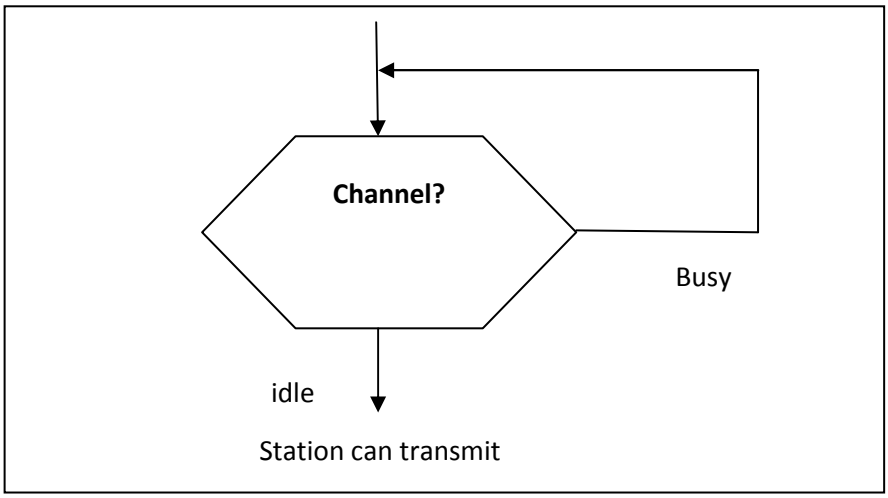
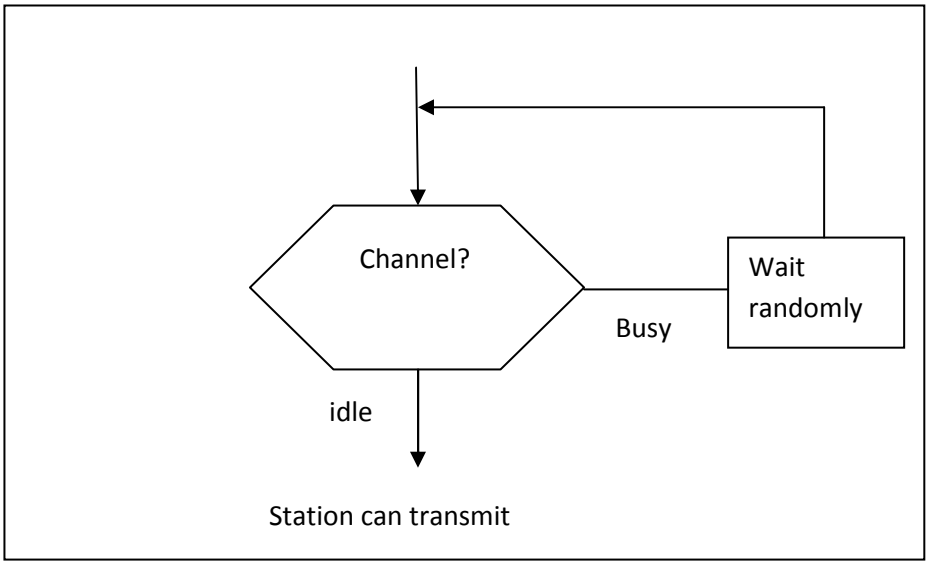
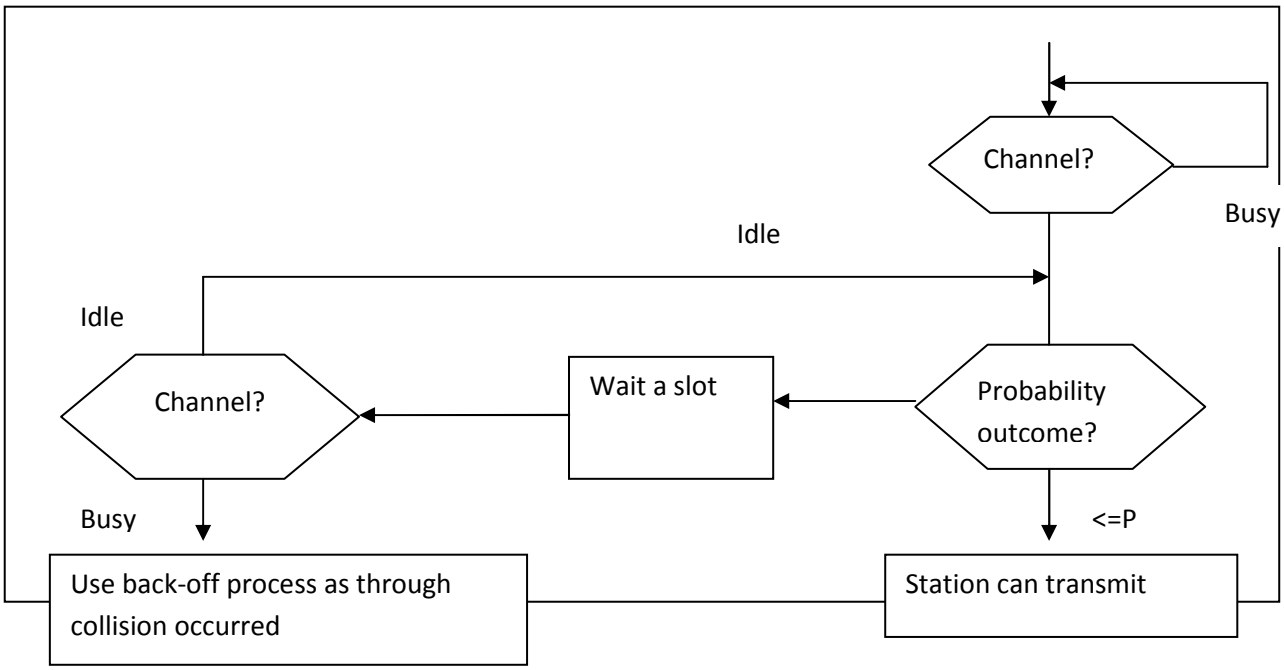


Figure (b): Non-Persistent



SPACE FOR LEARNER NOTE



3.5. CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION (CSMA/CD)

- CSMA/CD helps the CSMA algorithm to handle collision.
- In this method, a station monitors the medium after it sends a frame to see transmission was successful. If so, station is finished. If there is a collision, the frame is sent again.
- For CSMA/CD to work, we need a restriction on the frame size. Before sending last bit of frame, the sending station must detect collision, if any abort transmission.
- This is so because once the entire frame is sent, station does not keep copy of it. Therefore, transmission time must be at least twice of maximum propagation timeT_P.

Q) A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time is 25.6 μs. What is minimum size of frame?

Solution:

m/B ≥ $2T_P$

= m≥ $2\times25.6\times10^{-6}\times10\times10^{6}$

= m ≥512 bits or message size= 64 bytes

3.6. CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE (CSMA/CA)

Collision detection using energy level is possible in case of wired medium. But in case of wireless medium much of the sent energy is lost in transmission. Thus, energy level cannot be used for collision detection. So, we need to avoid collision on wireless because they cannot be detected.

CSMA avoids collision using three strategies:

1) Interface Space, 2) the contention window and 3) Acknowledgement.

Q) Consider a CSMA/CD network that transmits data at rate of 100 Mbps over a 1 km cable with no repeaters. If minimum frame size required for this network is 1250 bytes. What is signal speed (km/sec) is the cable?

Solution: $T_t \geq 2 \times T_P$

m/B $\geq$ 2d/V

$=1250/100 \times 10^6 \geq 2 \times 1 \times 10^3/V$

$=V \leq 2 \times 10^3 \times 10 \times 10^6 / 1250 \times 8$

$= V \leq 20000$

3.7. COLLISION FREE PROTOCOLS

Collisions can be avoided in CSMA/CD but they can still occur during the contention period. This affect the system performance, especially when the cable is long and the frames are short. Again, CSMA/CD is not universally applicable. Here, we shall discuss some protocols that resolve the collision during the contention period.

1) A Bit Map Protocol.
2) Binary Countdown.
3) Limited Contention Protocols.
4) Adaptive Tree Walk Protocol.

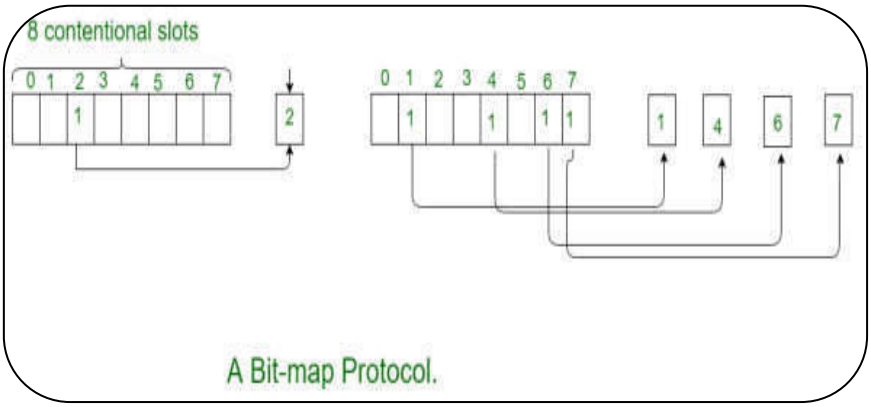
3.7.1. A BIT MAP PROTOCOL

It is our first collision free protocol; each contention period consists of exactly N slots. If station 0 has a frame to send, it transmits a 1bit during the zeroth slot. No other station is allowed

SPACE FOR LEARNER NOTE

to transmit during this slot. In this way, each station has complete knowledge of which station wishes to transmit. There will never be any collisions because everyone agrees on who goes next. Protocols like this in which the desire to transmit is broadcasting for the actual transmission are called Reservation Protocols.

Figure: A Bit Map Protocol



For analysing the performance, we will measure time in units of the contention bit slot, with a data frame of d time units. Under low load conditions, this will simply repeated over and over for lack of data frames.

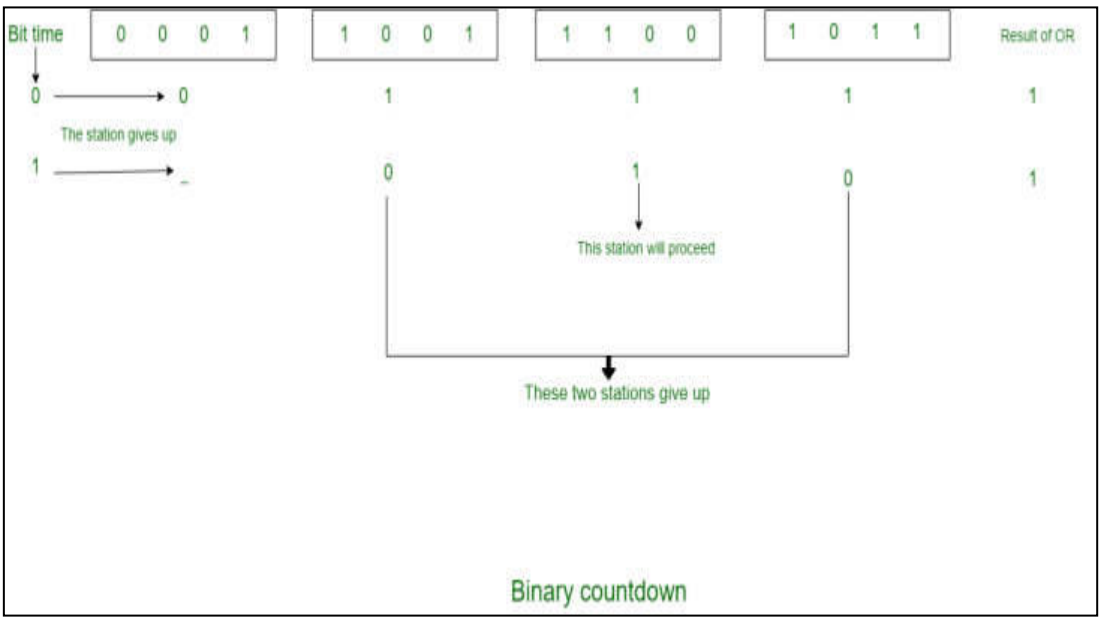
3.7.2 Binary Countdown

This protocol is used to overcome the overhead 1 bit per binary station. Here, binary station addresses are used. All addresses are assumed of the same length. All the station at first broadcast their most significant address bit that I 0,1,1,1 respectively. The most significant bits are ORed together.

Station 0001 sees the 1 MSB in another station addresses. Other three stations 1001, 1100, 1011 continue. The next bit is at station 1100; swiss station 1011 and 1001 give up. Then station 110 starts transmitting a frame, after which bidding cycle starts.

SPACE FOR LEARNER NOTE

Figure: Binary Countdown



3.7.3. LIMITED CONTENTION PROTOCOLS

- Collision based protocols (pure and slotted ALOHA, CSMA/CD) are good when the network load is low.
- Collision free protocols (bitmap, binary countdown) are good when load is high.
- When combining their advantages
    1. Behave like the ALOHA scheme under light load.
    2. Behave like the bitmap scheme under heavy load.

3.7.4. ADAPTIVE TREE WALK PROTOCOL

- Partition the group of station and limit the contention for each slot.
- Under light load, everyone can try for each slot like ALOHA.
- Under heavy load, only a group can try for each slot.
- How do we do it:
    1. Treat every station as the leaf of a binary tree.

2. First slot (after successful transmission), all station can try to get the slot (under the root node).
3. If no conflict, fine.
4. In case of conflict, only nodes under a sub tree get to try for the next one (depth first search).

3.8. WAVELENGTH DIVISION MULTIPLE ACCESS PROTOCOLS

It is a technique of multiplexing multiple optical carrier signals through a single optical fiber channel by varying the wavelengths. It allows communication in both the directions in the fiber cable.
Here, the optical signals from different sources are combined so that their wavelengths are different.
The combined signal is transmitted via a single optical fiber strand. At the receiving end, a demultiplexer splits the incoming beam into its components and each of the beams is send to the corresponding receivers.
Based upon the wavelength, it can be divided into two categories-

1. Course WDM (CWDM) and
2. Dense WDM (DWDM)

Check Your Progress-2

1. **Choose the correct one:**
   a) **1-Persistent/ Non-Persistent/ P-Persistent method has the highest chance of collisions.**
   b) **1-Persistent/ Non-Persistent/ P-Persistent method has the lowest chance of collisions.**
   c) **CSMA avoids collision using two/three/four strategies.**
   d) **A bit map/ Limited Contention Protocols behave like the ALOHA Scheme under light load and bitmap scheme under heavy load.**

3.9. SUMMING UP

- MAC sub layer deals with broadcast networks and their protocols. It is also known as **Media Access Control Protocol.**
- In channel allocation, single channel is divided and allotted to multiple users. It can be solved by two schemes- **static** and **dynamic** channel allocation.
- ALOHA is divided into two parts- **Pure ALOHA** and **Slotted ALOHA.** In pure ALOHA, we can start anywhere but in case of slotted ALOHA, we can start from beginning.
- Carrier sense multiple access protocol is divided into three parts- **1-persistent**, **non-persistent** and **p-persistent.**
- CSMA/CD helps the CSMA algorithm to **handle collision**.
- CSMA/CA avoids collisions using **three** strategies: **interface space**, **the contention window** and **acknowledgement**.
- Some protocols resolve collisions during the contention period. They are a **bit map protocol, binary countdown, limited contention protocols** and **adaptive tree walk protocol.**

3.10. ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress 1:

1) a) True, b) False, c) True, d) True

2) a) Pure ALOHA, b) Slotted ALOHA, Pure ALOHA

Check Your Progress 2:

1) a) 1-Persistent, b) P-Persistent, c) two, d) Limited Contention Protocols

3.11. POSSIBLE QUESTIONS

Short Answer Type Questions:

1. **What is MAC Sub Layer?**
2. **What is ALOHA?**
3. **What are the types of ALOHA?**
4. **What is CSMA?**
5. **What are the different types of CSMA?**
6. **What are the collision free protocols?**

Long Answer Type Questions:

1. **Define MAC Sub Layer. What are the various functions of MAC Sub Layer?**
2. **What are the difference between the MAC sub layer and LLC sub layer?**
3. **What is the channel allocation problem? How can we solve this problem?**
4. **What are the basic assumptions in dynamic channel allocation?**
5. **Define ALOHA. What is its type? Differentiate between pure and slotted ALOHA.**
6. **Discuss pure ALOHA with example.**
7. **Define slotted ALOHA with example.**
8. **Define different types of CSMA.**
9. **What are the different types of collision free protocols? Briefly explain.**
10. **Write short notes on**

    a) CSMA/CD b) CSMA/CA c) Wavelength Division Multiple Access Protocols.

3.12. FURTHER READINGS

- Computer Network, Fourth Edition, Andrew S. Tanenbaum

UNIT 4 : LOCAL AREA NETWORK (LAN)

CONTENTS

4.0 INTRODUCTION TO LAN

A ***l**ocal-**a**rea **n**etwork **(LAN)*** is a computer network that covers a relatively small geographical area, typically confined to a single building premises. Most of the LANs connect Workstations and Personal Computers where each station has its own CPU and programs for sharing of resources. LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line.

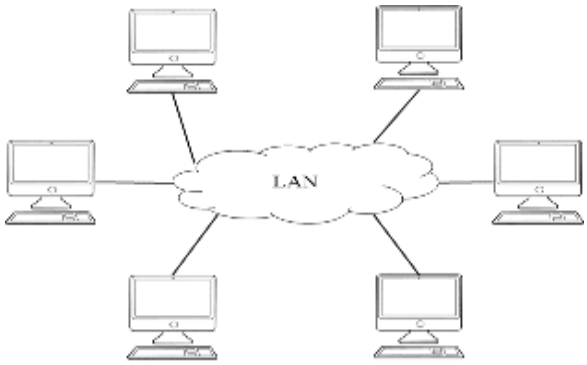


Figure 4.1: Local Area Network

LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN). The difference between a LAN and WAN is that the wide-area network spans a relatively large geographical area. LAN requires Ethernet cables and Layer 2 switches.

4.1 OBJECTIVES

After going through this unit you will be able to -

- understand the basic concepts of LAN
- Know different types of Ethernet Cablings and frame format
- working mechanism of Hubs and switches
- designing wiring closets and patch panels
- Data encoding Techniques
- understanding Fast and gigabit Ethernet

4.2ETHERNET CABLING

IEEE has standardized a number of local area networks under the name project IEEE 802. The most important LAN standards are IEEE 802.3 Ethernet and IEEE 802.11 (wireless LAN) where both the standards have different physical layers and different MAC sub-layers.

The name "Ethernet" is meaning cables. There is wide variety of options available for the physical medium to be used in 10 Mbps specification for IEEE 802.3 (Ethernet).

There is a concise notation:
<Data rate in Mbps><signaling method><maximum segment length in hundreds>

The standard specifications are
10 BASE 5
10 BASE 2
10 BASE-T
10 BASE-F

4.2.1 10 BASE 5

10Base5 cabling, popularly called thick Ethernet, came first. Connections to it are generally made using vampire taps, in which a pin is very carefully forced halfway into the coaxial (RG-58) cable'score. The notation 10Base5 means that it operates at 10 Mbps, uses baseband signaling, and can support segments of up to 500 meters.

4.2.2 10 BASE 2

The second cable type was 10Base2, or thin Ethernet. Connections to it are made using industry-standard BNC connectors to form T junctions, rather than using vampire taps. BNC connectors are easier to use and more reliable. Thin Ethernet is much cheaper and easier to install, but it can run for only 185 meters per segment, each of which can handle only 30 machines

4.2.3 10 BASE-T

10BASE-T has a maximum segment length of 100m and has a 10Mbps data transmission speed. 10BASE-T can use Category 3, 4, or 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cables for connectivity. Computers are connected through these cable to a central hub. With 10Base-T, there is no shared cable at all. Adding or removing a station is simpler in this configuration, and cable breaks can be detected easily. The disadvantage of 10Base-T is that the maximum cable run from the hub is only 100 meters, maybe 200 meters if very high quality category 5 twisted pairs are used.

4.2.4 10BASE-F

10BASE-F uses fiber optics. This alternative is expensive due to the cost of the connectors and terminators, but it has excellent noise immunity and is the method of choice when running between buildings or widely-separated hubs. Runs of up to km are allowed. It also offers good security since wiretapping fiber is much more difficult than wiretapping copper wire.

Summary of IEEE 802.3 10 Mbps Ethernet Characteristics

Standard	Cable	Maximum Distance	Connector Used
10BASE-2	Thin Coax	185m	BNC
10BASE-5	Thick Coax	500m	BNC
10BASE-T	Twisted Pair	100m	RJ-45
10BASE-FL	Fiber optics	Up to 2km	SC or ST

4.3 HUBS

An Ethernet hub or simply a hub is a network device for connecting Ethernet devices together to act as a single network segment. Hub comprises of multiple input/output (I/O) ports. A device which has to be connected to the LAN is plugged in to one of these ports. When a data frame arrives at one port it is relayed to every other port, without considering whether it is destined for a particular destination or not. If two frames arrive at the same time, they will collide, just as on a coaxial cable. In other words, the entire hub forms a single collision domain.. Hub is just a central meeting point of all devices present in the network. Hub does not have any intelligence i.e.it does not examine the 802 addresses or use them in any way.

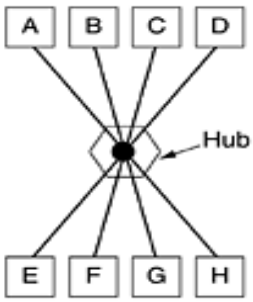


Figure 4.2: Hub

There are three types of network hubs: passive, active, and intelligent.

Passive Hubs do not amplify o regenerate any incoming signals before sending them tothe the LAN. Passive hubs are connected to other devices in a star configuration.

Active Hubs amplify the incoming electrical signals. Ifthe signal is too weak for rebroadcasting, Active hubs apply retiming and resynchronization techniques.

Intelligent Hubs work like active hubs and include have the facility of remote management. They also provide flexible data rates to network devices.

A hub works at the physical layer (layer 1) of the OSI model. Hubs are now largely obsolete, having been replaced by network switches.

4.4 PATCH PANELS

A patch panel is hardware unit with multiple ports that helps organize a group of cables. A patch panel in a local area network (LAN) is a mounted hardware assembly that contains ports used to connect and manage incoming and outgoing LAN cables. Each of these ports contains a wire that goes to a different location. Patch panels can be smallhaving just a few ports, or very largewith many hundreds of ports. They can also be set up for, cat5 cables, RJ45 cables, fiber optic cables and many types.

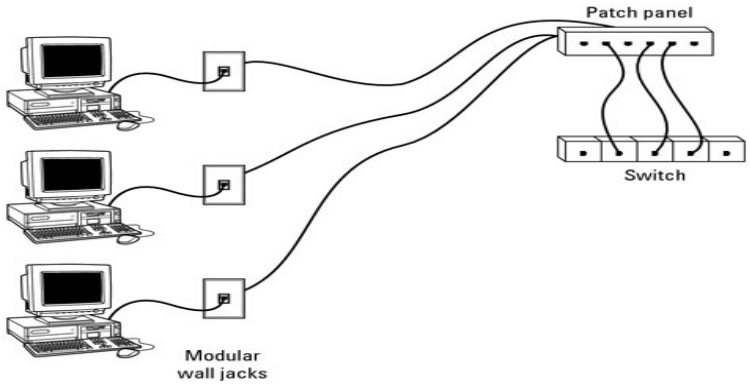


Figure 4.3: Patch Panel

The idea of Patch panels is to connect various IT devices together in an organized manner. They are in many different environments including communications closets, telephone company central offices, and data centers. Each port in a patch panel goes to a different device somewhere in the installation.

4.5 WIRING CLOSEST

Wiring closet is also known as an equipment room or server room. It is a dedicated room on the floor of a building that contains hubs, switches, and any other network components. While they are used for many purposes, their primary use is for computer networking where it may be called a premises wire distribution room (PWD room). Equipment that may be found in a wiring closet includes: Alarm systems, Circuit breaker panels, Video systems, such as cable TV and closed-circuit television systems, Ethernet routers, Network switches, Firewalls, Fiber optic terminations, Patch panels, Wireless access points etc..

While planning a wiring closet it is important that the control panel fronts are kept safely which is within easy reach and if necessary the panels should be mounted on the walls. It is to be ensured that adequate ventilation facilities are provisioned in the wiring closets. it should be designed in such a way that the operators have easy access to both front and rear of all equipment.

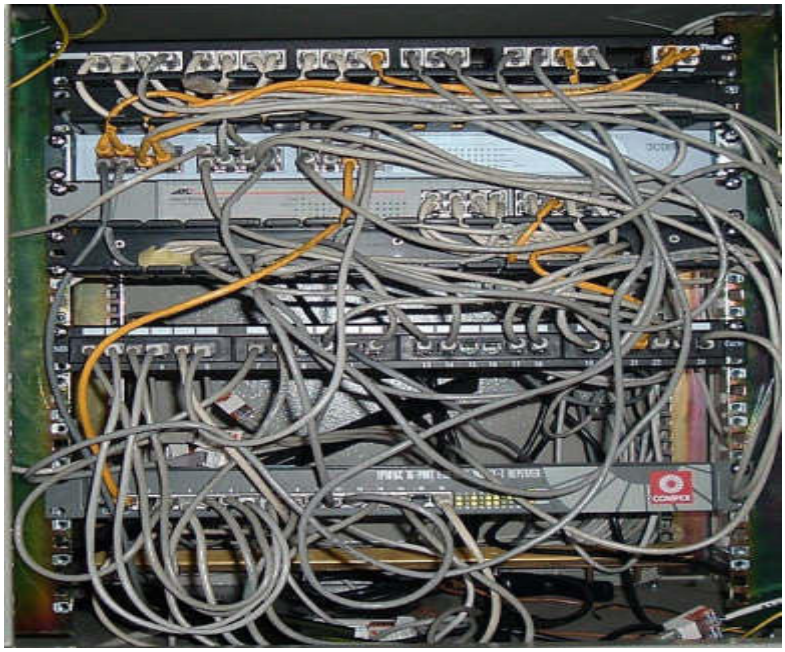


Figure 4.4: Wiring Closet

4.6 MANCHESTER ENCODING

Manchester encoding is a synchronous clock-encoding technique used by the physical layer to encode the clock and data of a synchronous bit stream. In this technique, the actual binary data to be transmitted over the physical media are not sent as a sequence of logic 1s and 0s (known as Non Return to Zero (NRZ)). Instead, the bits are converted into a slightly different format.

In Manchester encoding a binary 0 (zero) is indicated by a 1 to 0 transition in the middle of the bit and a binary 1 is indicated by a 0 to 1 transition in the middle of the bit. The signal transitions do not always occur at the *bit boundaries* (the division between one bit and another), but that there is *always* a transition in the middle of each bit.

The following diagram shows a typical Manchester encoded signal with the corresponding binary representation of the data (0100110100) being sent.

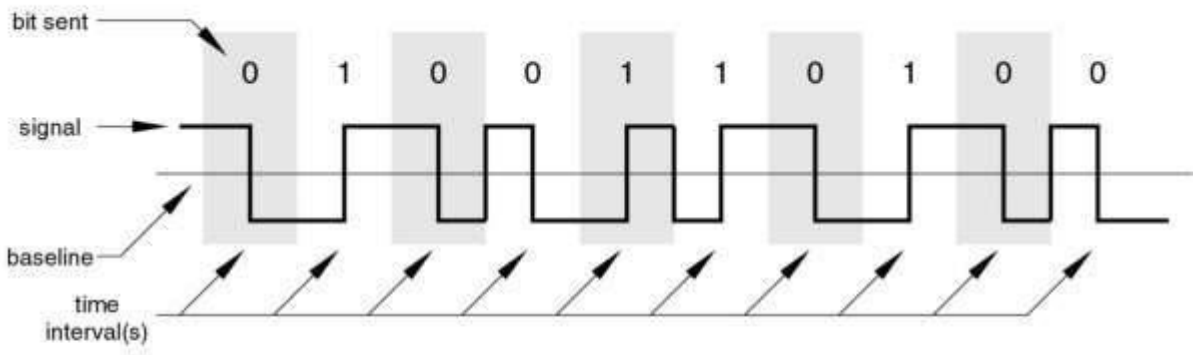


Figure 4.5: Encoding of Signal in Manchester Encoding

Advantage :DC component of the signal carries no information. which makes it possible that standards that usually do not carry power can transmit this information.

Drawback: it requires needs more bandwidth than other encoding techniques

4.7 MAC SUB-LAYER PROTOCOL

Media access control (MAC) protocols specifies how multiple devices access to a shared media network. The protocols used to determine who goes next on a multi access channel belong to a sub layer of the data link layer called the MAC (Medium Access Control) sublayer. Carrier sense multiple access/collision detection (CSMA/CD) is the most used contention-based MAC protocol, used in Ethernet networks. The channel access protocols are discussed in details in another part of the Syllabus.

4.7.1 IEEE 802.3 (ETHERNET) FRAME FORMAT

TotaBasic frame format which is required for all MAC implementation is defined in **IEEE 802.3 standard**. The Ethernet frame contains seven fields: preamble, SFD, DA, SA, Length or Type field, upper-layer data, and the CRC. The format of the MAC frame is shown in figure

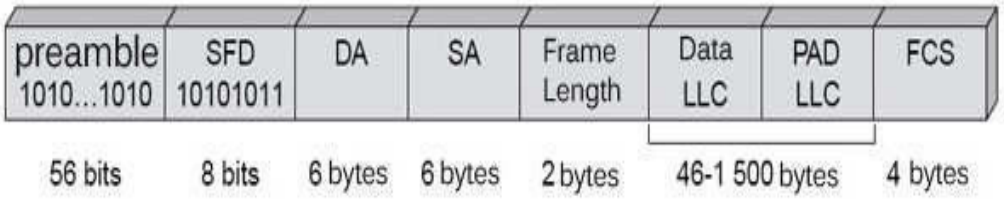


Figure 4.6: Ethernet Frame format

The frame starts with Preamble and SFD which are added by the Physical layer.

- **Preamble**: The first field of the 802.3frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. PRE (Preamble) was introduced to allow for the loss of a few bits due to signal delays
- **Start Frame Delimiter (SFD)**: The second field (1 byte: 10101011) signals the beginning of the frame. The last 2 bits is 11 and alerts the receiver that the next field is the destination address. The SFD warns station or stations that this is the last chance for synchronization.
- **Destination address (DA):** The DA field is 6 byte contains the physical address of the destination station or stations to receive the packets.
- **Source address (SA):** The SA field is also 6 byte and contains the physical of the sender of the packet.
- **Length or Type:** This field is defined as a type field or length field. This is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet.

- **Data:** This is the place where actual data is inserted, also known as **Payload**. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e. 46 bytes, then padding 0's is added to meet the minimum possible length.

- **CRC:**CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted

KEY NOTE:

The maximum data limit was chosen somewhat arbitrarily at the time the DIX standard was cast in stone, mostly based on the fact that a transceiver needs enough RAM to hold an entire frame and RAM was expensive in 1978. A larger upper limit would have meant more RAM, hence a more expensive transceiver.

In addition to there being a maximum frame length, there is also a minimum frame length. While a data field of 0 bytes is sometimes useful, it causes a problem. When a transceiver detects a collision, it truncates the current frame, which means that stray bits and pieces of frames appear on the cable all the time. Ethernet requires that valid frames must be at least 64 bytes.

STOP TO CONSIDER

- Preamble and SFD are not part of Ethernet Frame; but added by the Physical Layer.
- Maximum Frame Length is 1500+18 =1518 Bytes
- Minimum Frame Length is 46 + 18=64 Bytes
  where 18Bytes are calculated as :
  DA (6 Bytes)+SA(6 Bytes) +Frame Length(2 Bytes)+FCS/CRC(4 Bytes)=18 Bytes

4.8 Ethernet Performance

Now let us analyze the performance of Ethernet under conditions of heavy and constant load. Assumek stations are always ready to transmit with probability p during each contention slot. Let A be the probability that some station acquires the channel. A is calculated as −

$A = kp\ (1-p)^{kp}$

The value of A is maximized at p = 1/k. If there can be innumerable stations connected to the Ethernet network, i.e. k → ∞, the maximum value of A will be 1/e.

Let Q be the probability that the contention period has exactly j slots. Q is calculated as −

$Q = A\ (1-A)^{j-1}$

Let M be the mean number of slots per contention. So, the value of M will be −

$$M = \sum_{j=0}^{\infty} jA\ (1-A)^{j-1} = \frac{1}{A}$$

Given that τ is the propagation time, each slot has duration 2τ. Hence the mean contention interval, *w* will be 2τ/A.

Let P be the time is seconds for a frame to propagate.

The channel efficiency, when a number of stations want to send frame, can be calculated as −

$$Channel\ Efficiency = \frac{P}{P + 2\tau/A}$$

Let F be the length of frame, B be the cable length, L be the cable length, c be the speed of signal propagation and e be the contention slots per frame.

The channel efficiency in terms of these parameters is −

$$Channel\ Efficiency = \frac{1}{1 + 2BLe/cF}$$

4.9 SWITCHED ETHERNET

Ethernet is classified into two categories: classic Ethernet and switched Ethernet. Where legacy Ethernet networks transmitted data at 10 megabits per second (Mbps), modern Ethernet networks can operate at 100Mbps, 1,000 Mbps or even more due to the use of **switched Ethernet**. The first Ethernet cross-connecting devices were "hubs" that share the total bandwidth. However, the switch treats each send-receive pair at full speed, and most all hubs have been replaced with switches.Switched networks replace the shared medium of legacy Ethernet with a dedicated segment for each station. These segments connect to a switch, which acts much like an Ethernet bridge, but can connect many of these single station segments.

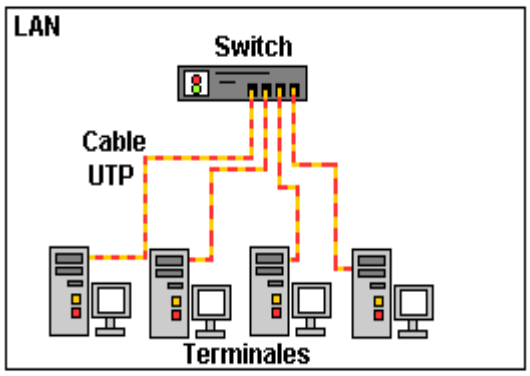


Figure 4.7: Switched Ethernet

The switch connects the high-speed backplane bus to all the stations in the LAN. The switch-box contains a number of ports, typically within the range of 4 – 48. Connections from a backbone Ethernet switch can go to computers, peripherals or other Ethernet switches and Ethernet hubs.

4.10 FDDI

Fiber Distributed Data Interface, or FDDI, is a high-speed network technology developed in the early 1980s by the American National Standards Institute (ANSI) for operating at speeds up to 100 Mbps over fiber-optic cabling that is often used for network backbones in a local area network (LAN) or Metropolitan Area Network (MAN). The FDDI network is set up in a ring topology fashion having two rings: a primary ring and a secondary ring, each able to carry 100Mbps. FDDI makes use of the same token-passing scheme as the IEEE 802.5 Token Ring network to control transmission around the loop. Following are the two types of devices used in FDDI standard: one is end user stations and the second one is concentrators which connects the Single Attached Systems (SAS) to the FDDI ring.

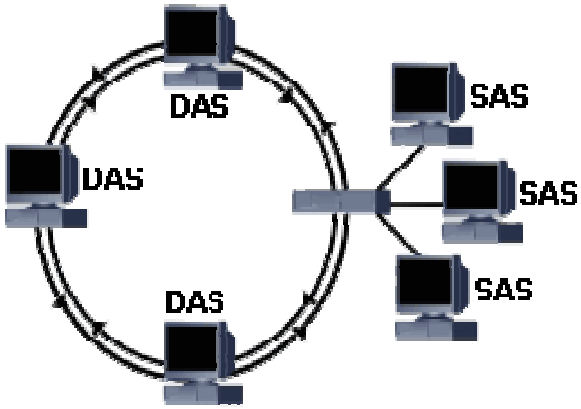


Figure: 4.8 FDDI LAN

The FDDI standard defines three ways of connecting devices to the ring

- **Single Attached Systems (SAS):** These devices cannot connect directly to FDDI dual ring since they have a single port, to connect theses device to the FDDI network a concentrator is used.
- **Dual Attached Systems (DAS):** All stations connected to the FDDI dual ring must be dual attached and always be up and running. For stations that cannot be connected using DAS methodology can use a SAS which uses a concentrator.
- **Dual Homing:** Some devices may connect to two concentrators using a DAS card for redundancy purposes. One link will be active and the other link will take the active role if the active links fails.

FDDI can handle data rates upto 100 mbps and provides good security because of Fiber Technology as eavesdrop on fiber optic link is quite difficult and the cable is not breakable like any other media types. Fiber optic Cable can transmit signal to long distances upto 200 kms and it is immune to the Electro Magnetic Interfaces. FDDI can isolate faulty nodes with use of wiring concentrators for instantaneous re-routing. Wiring concentrators function as centralized cabling connection devices for workstations. FDDI is relatively more complex system than other systems because of its installation and maintenance issues which requires great deal of expertize.

4.11 FIBER CHANNEL

Fiber Channel (FC) is a high-speed data transfer protocol providing in-order, lossless delivery of raw block data**.** It is a serial I/O interconnect network technology capable of supporting multiple protocols. It is used primarily for storage area networks (SANs). Fiber Channel technology handles high-performance disk storage for applications on many corporate networks, and it supports data backups, clustering, and replication. The original version of Fibre Channel operated at a maximum data rate of 1 Gbps. Newer versions of the standard increased this rate up to 128 Gbps, with 8, 16, and 32 Gbps versions also in use. The FC SAN physical components such as network cables network adapters and hubs or

switches can be used to design a Fibre channel Storage Area Network. The different types of FC architecture which can be designed are

- Point-to-point
- Fibre channel arbitrated loop (FC-AL)
- Fibre channel switched fabric (FC-SW).

4.11.1 PORT TYPES IN FC

The ports in a switched fabric can be one of the following types

- **N_Port:** It is an end point in the fabric. It is a computer system port (FC HBA port) or a storage system port that is connected to a switch in a switched fabric.

- **E_Port:** It is a port that forms the connection between two FibreChannel switches. The E_Port on an FC switch connects to the E_Port of another FC switch in the fabric ISLs.

- **F_Port:** It is a port on a switch that connects an N_Port.
- **G_Port:** It is a generic port on a switch that can operate as an E_Port or an F_Port and determines its functionality automatically during initialization.

Three are various topologies defined for fiber channel with regard to application and installation requirements. Each of these topologies exhibit different performance characteristics.

4.11.2 POINT-TO-POINT

Point-to-Point topology is the most basic and simple Fiber Channel topology amongst all. Here two devices are directly connected by a Fiber Channel cable. In general, it has been used to connect RAID (Redundant Array of Independent Disks) and other storage subsystems to servers in server-centric computing environments.

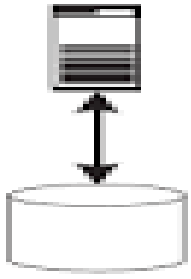


Figure 4.9 :Point-to point

4.11.3 ARBITRATED LOOP

The arbitrated loop, also known as FC-AL, is a Fiber Channel topology in which devices are connected in a one-way loop fashion in a ring topology. It was cost effective alternative to a fabric topology. FC-AL uses fiber optic cabling and copper wires to produce a maximum (burst) data transfer rate of more than 100 MB/sec. FC-AL is capable of supporting up to 127 devices as far as 10 kilometers away, thus opening a new perspective for remote data storage (web storage and storage networking).

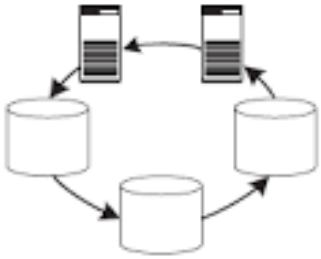


Figure 4.10: Arbitrated Loop

This topology is usually used to connect disk drives to RAID controllers or host bus adapters (HBA).

4.11.3 SWITCHED FABRIC

Switched fabric or switching fabric is a network topology in which network nodes interconnect via one or more network switches (particularly crossbar switches). Because a switched fabric network spreads network traffic across multiple physical links, it yields higher total throughput than broadcast networks, such as the early 10BASE5 version of Ethernet and most wireless networks such as Wi-Fi. It essentially consists of one or more switches, controlling a large amount of port-to-port transfers of data and commands between nodes.

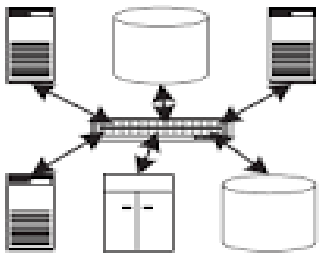


Figure 4.11: Switched Fabric

Fiber Channel networks have a historical reputation for being expensive to build, difficult to manage, and inflexible to upgrade due to incompatibilities between vendor products.

4.12 FAST ETHERNET

It is the Successor of 10-Base-T Ethernet. It is more popular than Gigabit Ethernet because its configuration and implementation is simple. There are several versions of 100 Mbps Ethernet and these are designated using the 100BASE-xx configuration where 100 indicates the speed in Mbps, Base indicates it is BASE band and the suffix indicates the medium either fibre cable or copper. It is faster than its successors. Its variants are:

4.12.1100 BASE-T4

This is the early implementation of Fast Ethernet over twisted pair cables, carrying data traffic at 100 Mbps.It uses four pairs of category-3 UTP cable. Two of the four pairs are bi-directional, the other two are unidirectional. In each direction, three pairs are used at the same time to carry data.Encoding/decoding in 100Base-T4 is more complicated.As it uses category 3 UTP, each twisted pair cannot easily handle more than 25 Mbaud data.

4.12.2 100BASE-TX

100BASE-TX is the technical name of Fast Ethernet over twisted pair cables. This has either two pairs of unshielded twisted pairs (UTP) category 5 wires or two shielded twisted pairs (STP) type 1 wires to connect a station to the hub. Each network segment can have maximum length of 100m .Straight binary coding is not used; instead a scheme called used4B/5B is used. The 100Base-TX system is full duplex; stations can transmit at 100 Mbps and receive at 100 Mbps at the same time.

4.12.3 100BASE-FX

100BASE-FX is the technical name of Fast Ethernet over fiber optic cables. It is a version of Fast Ethernet carrying data traffic at 100 Mbps. This has two pairs of optical fibers. One pair transmits frames from hub to the device and the other from device to hub. Maximum distance between hub and station is 2000m. It has a data rate of 125 Mbps. In most Fast Ethernet applications, fiber optics is used for the long haul transmissions.In addition, the distance between a station and the hub can be up to 2 km.

Summary of IEEE 802.3 100 Mbps Ethernet Characteristics

Standard	Cable Type	Maximum Distance	Connector Used
100BaseT4	Category 3, 4, or 5 UTP or STP	100m	RJ-45
100BaseTX	Category 5 UTP or STP	100m	RJ-45
100BaseFX	Fiber-optic	412m with half-duplex 10,000m with full-duplex fiber	SC or ST

4.13 GIGABIT ETHERNET

The emergence of Gigabit Ethernet has been purely to increase the Ethernet performance while maintaining all Ethernet standards. Gigabit Ethernet supports two different modes of operation: full-duplex mode and half-duplex mode. Full-duplex mode allows traffic in two directions at the same time. When a central switch connected to computers on the periphery; this mode is used.A half-duplex mode is used when computers are connected to a hub rather than a switch. A hub does not buffer incoming frames. All the lines are electrically connected internally, simulating the multi-drop cable used in classic Ethernet. Standard CSMA/CD protocol is required in this mode because collisions are possible. Because a 64-byte frame can now be transmitted 100 times faster than in classic Ethernet, the maximum cable length must be 100 times less or 25 meters.

Gigabit Ethernet supports both copper and fiber cabling. Signaling at or near 1 Gbps over fiber means that the light source has to be turned on and off in under 1 nsec. LEDs simply cannot operate this fast, so lasers are required. Two wavelengths are permitted: 0.85 microns (Short) and 1.3 microns (Long). Lasers at 0.85 microns are cheaper but do not work on single-mode fiber.

Summary of IEEE 802.3 1000 Mbps Ethernet Characteristics

Standard	Cable Type	Maximum Distance	Connector Used
1000BaseSX	MM fiber-optic	550m	SC or ST
1000BaseLX	Fiber cable	5000m	SC or ST
1000BaseCX	Shielded copper wire	25m	9-pin shielded connector

CHECK YOUR PROGRESS

1. IEEE 802.3 standard is known as ----------
2. IEEE 802.11 standard is known as ----------
3. What is Thick and thin Ethernet?
4. What type of Cabling is used in 10Base F
5. State whether True or False

a. 10Base 2 uses BNC Connectors.
b. 10Base T uses Coaxial Cables .

6. What are the port Types in Fiber Channel
7. What are the key differences between Switched fabric and Arbitrated Loop?
8. Why Preamble and SFD fields are added to the Ethernet Frame?
9. Define Passive and intelligent hubs.
10. Discuss the summarized characteristics of 10, 100 Mbps Ethernet.
11. What are the significances of a well plannedwiring closest?

4.14 SUMMING UP

- IEEE has standardized a number of local area networks under the name project IEEE 802. The most important LAN standards are IEEE 802.3 Ethernet (Wired Network) and IEEE 802.11 (wireless LAN).
- An Ethernet hub or simply a hub is a network device for connecting **Ethernet** devices together to act as a single network segment. Hub comprises of multiple **input/output** (I/O) ports There are three types of network hubs: passive, active, and intelligent.

- A patch panel is hardware unit with multiple ports that helps organize a group of cables. A patch panel in a local area network (**LAN**) is a mounted hardware assembly that contains **ports** used to connect and manage incoming and outgoing LAN cables.

- In Manchester encoding a binary 0 (zero) is indicated by a 1 to 0 transition in the middle of the bit and a binary 1 is indicated by a 0 to 1 transition in the middle of the bit. it requires needs more bandwidth than other encoding techniques
- Ethernet Frame has minimum size of 64 bytes and maximum of 1500 bytes.
- Ethernet is classified into two categories: classic Ethernet and switched Ethernet. Where legacy Ethernet networks transmitted data at 10 **megabits** per second (Mbps), modern Ethernet networks can operate at 100Mbps, 1,000 Mbps or even more due to use of switched Ethernet
- The FDDI network is set up in a ring topology fashion. FDDI can handle data rates upto 100 mbps

- Fiber Channel (FC) is a high-speed data transfer protocol capable of supporting multiple protocols. It is used primarily for storage area networks (SANs). The different types of FC architecture which can be designed are -Point-to-point Fibre channel arbitrated loop (FC-AL) and Fiber channel switched fabric (FC-SW)
- Gigabit Ethernet supports both copper and fiber cabling. Signaling at or near 1 Gbps over fiber.

4.15 KEY TERMS

Ethernet: The IEEE 802.3 standard is meant for wired Local Area Networks which is popularly termed as Ethernet

Thick Ethernet: The 10Base5 standard of IEEE 802.3 10Mbps specification is known as Thick Ethernet

Thin Ethernet: The 10Base2 standard of IEEE 802.3 10Mbps specification is known as Thick Ethernet

Fast Ethernet:The IEEE 802.3 Ethernet operating at the sped of 100Mbps is also known as Fast Ethernet

Gigabit Ethernet:The IEEE 802.3 Ethernet operating at the sped of 1000Mbps is also known as Fast Ethernet

Fiber Channel Fiber Channel (FC) is a high-speed data transfer protocol providing in-order, lossless delivery of raw block data**.**It is used primarily for storage area networks (SANs)

FDDI: FDDI is a high-speed network technology for operating at speeds up to 100 Mbps over fiber-optic cabling that is often used for network backbones in a local area network (LAN) or Metropolitan Area Network (MAN).

Hub: An Ethernet hub is a network device for connecting Ethernet devices together to act as a single network segment. It is just a central meeting point of all devices which are electrically joined**.**

Switched Ethernet: The legacyEthernet networks transmitted data at 10 megabits per second (Mbps), modern Ethernet networks can operate at 100Mbps, 1,000 Mbps or even more due to use of switches in the LAN treating each send-receive pair at full speed.

4.16 QUESTIONS AND ANSWERS

Fill in the Blanks

1. The Full form of MAN is ----------.....

2. The maximum length of a cable segment in 100BaseTX standard is ----------meter.

3. The maximum and minimum size of data in IEEE 802.3 Ether Frame is---------- bytes and ----------bytes respectively.

4. The Full form of NRZ is----------

5. The maximum length of a cable segment in 10Base5 standard is ----------meter

Answers :

1. Metropolitan Area Network **2**. 100 **3**. 46 1500 **4.**Non Return To Zero**5.**550

Short Answer Type Questions

1. What is LAN and MAN?

2. What is Ethernet? What is Fast and Gigabit Ethernet?

2**.** Explain the IEEE 802.3 100 Mbps Ethernet standards

3.Explain the IEEE 802.3 1000 Mbps Ethernet standards

4.. What is Fiber Channel?

5. What is Patch Panel?

6. what is Thick and thin Ethernet?

7. What is Preamble and SFD in Ethernet Frame?

8. What is Switched network and its Advantages?

9. What is MAC?

10. What is the major Drawback of Manchestar Encoding Technique?

Long Answer type Questions

1. What is FDDI? Explain SAS and DAS.

2. Explain the Frame format of IEEE 802.3 Ethernet standard.

3. Explain the Manchester Encoding of a signal with a suitable representation of binary data. What are the advantages and disadvantages of Manchester Encoding technique?

4. What is Fiber channel? Explain various types of ports in FC.

5. What is Hub? what are the various types of Hubs? what is the advantage of network Switch over network Hubs

2.17: SUGGESTED READINGS

Computer Networks: 4th edition Author: Andrew S Tanenbaum

Online Reference Sources

https://en.wikipedia.org/
https://www.lifewire.com/
https://www.geeksforgeeks.org/
https://www.certificationkits.com/
https://www.mycloudwiki.com/
https://www.tutorialspoint.com

UNIT 5: The Wireless LAN

Unit Structure:

5.1 INTRODUCTION

In this unit, you will learn about Wireless LAN (WLAN). You will be able to know how a mobile user can connect to a Local Area Network (LAN) through wireless connection. WLAN use high frequency radio wave and allow using the internet, checking e-mail and receiving instant messages while user is moving. You will get an idea about station and its categories, services, types of WLAN. You will also learn about wireless LAN protocol MACA and MACAW and the problem related to this protocol. You will be able to understand the hidden station and the exposed station problem. In this unit, you will study about IEEE standard for WLAN. This unit gives you an idea about IEEE protocol and protocol stack. A protocol is a set of rules for data communication. You will learn about the two 802.11 MAC sublayer function DCF and PCF. You will also learn about the different techniques that are used for data transmission in physical layer of WLAN. You will know about the different types of frame in 802.11. You can understand the data frame structure of 802.11standard and its field. You will get an idea about the distribution service and the station service that are provided by 802.11 standard.

5.2 UNIT OBJECTIVES

After going through this unit, you will be able to—

- Know about the Wireless LAN, its uses, advantages and disadvantages.
- Understand station, service and types of Wireless LAN.
- Know about wireless protocol MACA and MACAW.
- Describe the IEEE 802.11 standard and its different variant.
- Understand the IEEE 802.11 sublayer protocol.
- Know how the IEEE 802.11 protocol stack is designed.
- Understand the data frame structure of 802.11.
- Describe the distribution service and the station service.

5.3 Wireless LAN

Wireless LAN stands for Wireless Local Area Network. It is also called LAWN (Local Area Wireless Network).WLAN is a local area network. It uses radio communication to provide mobility. In WLAN, a mobile user can connect to a Local Area Network (LAN) through a wireless connection that means a WLAN extends wired local area network. Users connected by wireless LANs can move around within a limited area such as home, school, campus, office building, railway platform, etc. The performance of WLAN is high as compared to other wireless networks. The IEEE 802.11 group of standards defines the technologies for wireless LANs. Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name

The workstations and the servers of a wired LAN are fixed in their native locations. For users who are highly mobile and if there is no possibility to install and lay down the cables of a wired LAN, a good solution is to install a wireless LAN. Wireless LANs transmit and receive data over the atmosphere, using radio frequency (RF) or infrared optical technology by eliminating the need for fixed wired connections. Wireless LANs provides dual advantage of connectivity and mobility. Wireless LANs have gained strong popularity in applications like health-care, retail, manufacturing, warehousing, and academic. A Wi-Fi network is a type of WLAN.

5.3.1 Uses of WLAN

Wireless LAN has many important uses. Some uses of WLANs are—

- Users would be able to surf the Internet, check e-mail, and receive Instant Messages while they are moving.
- WLANs are easy to set up networks in the areas that are affected by earthquakes or other such disasters where no suitable infrastructure may be available on the site.
- In historic buildings, WLANs are very good to set up networks where wiring may not be permitted or the building design may not be conducive to efficient wiring.

5.3.2 Advantages of WLAN

- **Flexibility:** A user can communicate without further restriction within radio coverage. Wireless network is suitable for any kind of geographical conditions. Installation requires to properly setup the transmitter and the receiver antenna (RF) or infrared system. This is much easier than cable installation of a wired LAN. Radio waves can penetrate walls. Senders and receivers can be placed anywhere.
- **Planning**: Wireless LAN allows communication without previous planning.
- **Design:** Wireless LAN allows the independent design. For example small devices which can be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.
- **Robustness:** Wireless LAN can handle disasters, e.g., earthquakes, flood etc. But a LAN which requires a wired infrastructure will usually break down completely in disasters.
- **Cost:** The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN. This is because adding additional users to a Wireless LAN will not increase the cost. Wireless LAN eliminates the direct costs of cabling.
- **Ease to Use:** Wireless LAN is easy to use and the users need very little new information to take advantage of WLAN.

5.3.3 Disadvantages of WLAN

- Wireless LAN is very prone to interference and noise.
- It has limited coverage area.
- Communication is not very secure and unauthorized access is common.
- License is required. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.
- If wireless LAN uses radio transmission, many other electrical devices can interfere with them.

- Several govt. and non-govt. institutions regulate the operation in world-wide and restrict frequencies to minimize interference.

5.3.4 Working of WLAN

Wireless LANs use radio or infrared technology to communicate information from one point to another without relying on any physical connection. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. It is the modulation of the carrier by which the information being transmitted. Multiple radio carriers can exist in the same space at the same time. This carrier does not interfere with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver tunes in one radio frequency while rejecting all other frequencies. In a typical wireless LAN configuration, an access point connects to the wired network from a fixed location using standard cabling. The access point receives buffers and retransmits data between the wireless LAN and the wired network infrastructure. A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet.

Wireless LAN adapters provide an interface between the client network operating system (NOS) and the air waves via an antenna. The nature of the wireless connection is transparent to the NOS.

5.4 Architecture

In this section, we will discuss the components used in WLAN. We will learn about the purpose of these components.

5.4.1 Station

A Station refers to all components that can connect into a wireless medium in a network. All stations are equipped with wireless network interface controllers.

Wireless stations are of two categories

- Wireless access point
- Client.

Access points are normally wireless routers. These access points are base stations for the wireless network. They transmit and

receive radio frequencies for wireless enabled devices to communicate. Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones and other smart phones, or non-portable devices such as desktop computers, printers, and workstations that are equipped with a wireless network interface.

5.4.2 Service

There are two types of services in WLAN

- Basic services set
- Extended Service Set

5.4.2.1 Basic Services Set

The basic services set (BSS) contain stationary or mobile wireless stations and a central base station called access point (AP). All station in basic service set can communicate with each other at Physical Layer. A Basic Service Set has an identification number known as BSSID. BSSID is the MAC address of the access point servicing the BSS.

There are two types of BSS---

- Independent BSS
- Infrastructure BSS

An independent BSS (IBSS) is an ad hoc network that contains no access points. They cannot send data to any other basic service set.

In Infrastructure BSS, the BSS contain an access point.

5.4.2.2 Extend Service Set

An extended service set (ESS) is created by joining two or more basic service sets (BSS) having access points (APs). Access points in an ESS are connected by a distribution system. Each ESS can be identified by an ID called the SSID which is a 32-byte (maximum) character string.

ESS has two types of station---

- **Mobile station**: These are the normal stations inside a BSS.
- **Stationary station**: These are AP stations that are part of a wired LAN.

Two stations in two different BSS can communicate using their AP.

5.4.3 Types of WLAN

WLAN has two basic modes of operation

- Infrastructure
- Ad hoc mode.

5.4.3.1 Infrastructure mode

In this mode, mobile units communicate through an access point that serves as a bridge to other networks (such as Internet or LAN). Wi-Fi networks are employed in infrastructure mode. A base station can work as a wireless access point hub through which nodes can communicate. The hub usually has a wired or fiber network connection and may have permanent wireless connections to other nodes. Wireless access points are usually fixed and provide service to their client nodes within range.

5.4.3.2 Ad hoc mode

In this mode, mobile units transmit directly peer-to-peer.
There is no base station and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).
A peer-to-peer network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network. This can basically occur in devices within a closed range.

CHECK YOUR PROGRESS

1. A WLAN uses ———— for communication.
2. WLAN can be configured in ———— ways.
3. A Basic Service Set has an identification number known as ————. .
4. Access points are normally wireless ———— .
5. State true or false
   a. Wi-Fi allows only laptops in its range.

b. In Wireless ad-hoc network, access point is not required.
c. The cost of installing and maintaining a wireless LAN is higher than the cost of installing and maintaining a traditional wired LAN

5.5 Wireless LAN Protocol

Wireless LAN is an extension of LAN. So, it have some different properties than the conventional LAN. A special MAC sublayer is needed for wireless LAN.

In a simple approach of Wireless LAN, CSMA protocol can be used. But Wireless stations have transmission ranges and all stations are not within radio range of each other. So simple CSMA will lead to Hidden station problem and Exposed station problem.

Let us consider the situation given in the following figure.

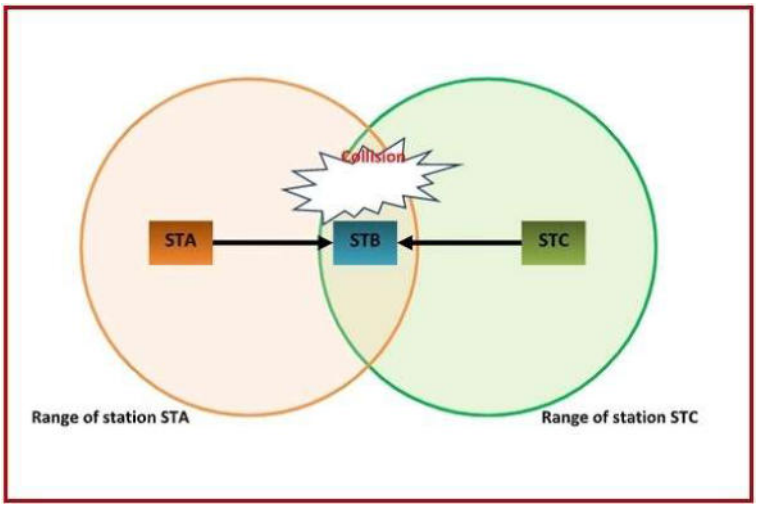


Fig: 5.1 The hidden station problem

There are three stations labelled STA, STB, and STC. The two stations STA and STC are not in the radio range of each other. The station STA and STC both covers station STB in their radio range STA starts transmitting to station STB. Since station STC is out of radio range of STA, it concludes that the channel is free and starts transmitting to STB. The frames received by STC are garbled and collision occurs. The problem is a transmission problem that arises when two or more stations that are out of range of each other

transmits simultaneously to a common recipient. This situation is known as the hidden station problem.

Let us consider another situation following in the figure.

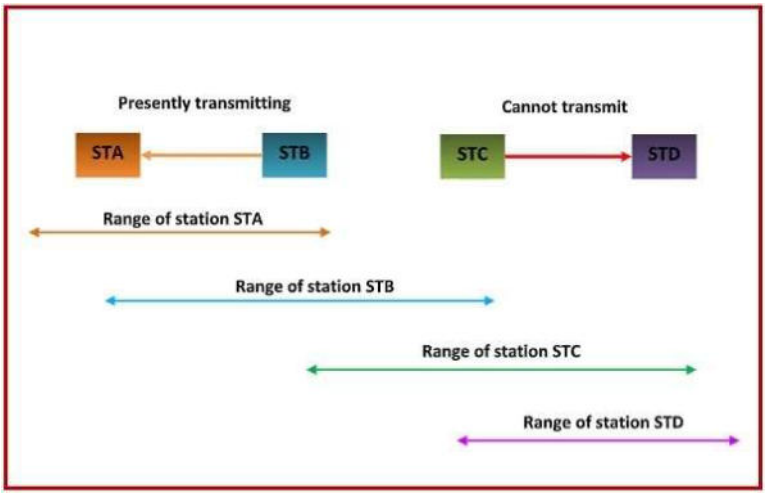


Fig: 5.2 The exposed station problem

The two receivers STA and STD are out of radio range of each other, but the station STB and STC are in radio range of each other in the above figure. When STB is transmitting to STA, STC falsely concludes that the transmission will cause collision and so stops its transmission to STD. But, the collision would not have occurred because the transmission from STC to STD is out of range of STB. The problem is that a transmitting station is prevented from transmitting frames because of interference with another transmitting station. This problem is known as exposed station problem.

STOP TO CONSIDER
CSMA is a carrier sense multiple access based on media access protocol to sense the traffic on a channel before transmitting the data. The main idea is that if the channel is idle, the station can send data to the channel otherwise it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

5.5.1 MACA

MACA (Multiple Access with Collision Avoidance) is a protocol designed for Wireless LAN. MACA was proposed to overcome the shortcomings of CSMA protocols when used for wireless networks. The hidden station problem and exposed station problem in CSMA can be solved using this protocol.

The main idea behind MACA is that the stations have to be synchronized with frame sizes and data speed. Before starting transmission of data frames between two stations, the sender transmits a frame called RTS (Request to Send) and the receiver responds with a frame called CTS (Clear to Send).

Let us take a station A has data frame to send to a station B. A will send RTS frame to the B. Then B will send CTS frame to A.

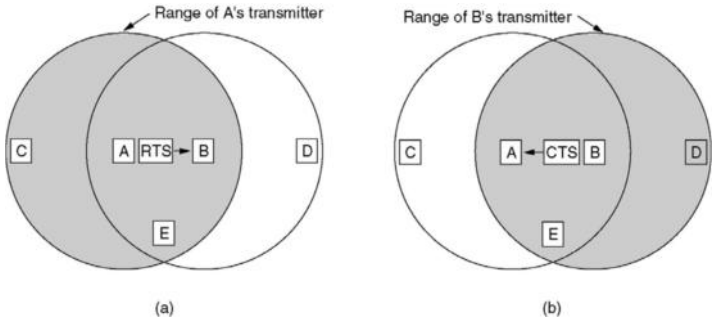


Fig: 5.3 The MACA protocol. (a). A send an RTS to B. (b). B responds to A with a CTS

When A gets CTS frame from B, it starts to send data to station B. After getting an RTS from a nearby transmitting station A, a station keeps silent until the CTS transmitted back to station A without conflict. Stations which get the CTS are near to the receiving station and keep silent during the data transmission.

Let us see how MACA solves the hidden and exposed station problem.

Station C gets RTS from station A. But the CTS from station B does not reach station C because C is not within the range of B. So, C is free to transmit while the data frame is being sent as it does not interfere with the CTS. In other hand, Station D does not get RTS from station A but it gets CTS frame from B. This is because D is in the range of B but not in range of A. So, it realizes that B is busy and defers its transmission to avoid collision. Thus MACA resolves the hidden station problem and the exposed station problem with the help of RTS and CTS frame.

But collision can still occur in spite of all these provision. In fig: 5.3 both station B and C can send RTS to station A simultaneously. These will cause collision and RTS will be lost.

SAQ

1. Do you think WLAN has many benefits over LAN? Justify your answer.
2. How can the shortcoming of CSMA be eliminated using MACA?

5.5.2 MACAW

MACAW is an improved version of MACA protocol which is designed for Wireless LAN. It makes use of RTS and CTS from MACA protocol and employ RTS-CTS-DS-DATA-ACK frame sequence to transmit data.

MACAW initiates an ACK frame after each successful transmission of data frame. It also adds carrier sensing. The backoff algorithm is chosen to run individually for each data stream not per station. This changes leads to a fair protocol. In this protocol, the backoff algorithm responds less violently to temporary problem by using a mechanism to improve system performance.

A successful data transfer (A to B) consists of the following sequence of frames:

1. A send RTS to B
2. B send CTS A
3. A send "Data Sending" frame (DS) to B
4. A send DATA fragment frame from to B
5. B Acknowledges A by sending Acknowledgement frame (ACK).

CHECK YOUR PROGRESS

6. ———— sublayer is needed for WLAN.
7. ———— lead to hidden station and exposed station problem.
8. RTS stands for ————.
9. The improved version of MACA designed for WLAN is ————.

10. State true or false
    a. MACAW uses an ACK frame.
    b. Collision can not occur in MACA.
    c. The backoff algorithm run individually for each data stream in MACW.

5.6 The IEEE Standard

IEEE formed a working group to develop a Medium Access Control (MAC) and Physical Layer standard for wireless connectivity for stationary, portable, and mobile computers within a local area. This working group is IEEE 802.11. IEEE 802.11 is the standard for WLAN. There are some standard of IEEE 802.11. The important among them are —

1. **802.11**
   IEEE 802.11 was the original version. It gives 1 Mbps or 2 Mbps data rate in the 2.4 GHz band but it is outdated now. Either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS) is used by this standard.

2. **802.11a**
   This standard achieves data transfer speeds as high as 54Mbps within a 5GHz frequency range. It employs Orthogonal Frequency Division Multiplexing (OFDM). Due to its high frequency, it has difficulty in penetrating walls and other obstructions. Signal coverage is comparatively less than other standards but expensive to implement.

3. **802.11b**
   It operates within the 2.4GHz range and supports 11Mbps bandwidth speed. It uses the multiple access method known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). It is less vulnerable to obstructive interferences such as walls. It has low implementation cost with a good data transmission signal. It facilitates path sharing through its supported bandwidth.
4. **802.11g**

This standard combines the features of 802.11a and 802.11b protocols. 802.11g supports both the 5GHz (802.11a standard) and 2.4GHz (802.11b standard) frequencies, which allows it to operate at wider ranges. It uses OFDM technique. 802.11g is backward compatible with 802.11b devices that means their access points and network adaptors can work interchangeably. It is more expensive for implementation but provides high speeds, varying signal range, and flexibility to obstruction.

5. **802.11n**

This standard is an upgraded version of 802.11g. 802.11n operates on variable data rate ranging from 54 Mbps to 600 Mbps which produces better signal coverage with wider radio frequency. It is an improvement over previous standards 802.11 by incorporating multiple-input multiple-output (MIMO). MIMO implements multiple antennas at both the transmitter end and receiver ends.

5.6.1 protocol

The IEEE 802.11 protocol is specified in terms of coordination function. This function determines when a station is allowed to transmit and when it may be able to receive data over the wireless medium. The IEEE 802.11 MAC sublayer protocol is the standard for wireless LAN. IEEE 802.11 MAC sublayer uses two co-ordination functions for collision avoidance before transmission −

1. **Distributed Coordination Function**
2. **Point Coordination Function**

5.6.1.1 Distributed coordination function

The Distributed coordination function (DCF) is an improved version of Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).The DCF is used in BSS having no access point. It provides support for asynchronous data transfer. In this function, CSMA/CA uses both physical channel sensing and virtual channel sensing.

In physical channel sensing, a station senses the channel when it has to send data. If the channel is idle, the station sends the entire frame. During the transmission, it does not sense the channel so

collision may occur. If the channel is busy, the station waits for it to be idle and then send. A colliding station waits for a random time using the binary exponential backoff algorithm after a collision occurs and try again.
The virual channel sensing in CSMA/CA is based on MACW. This works as follows—

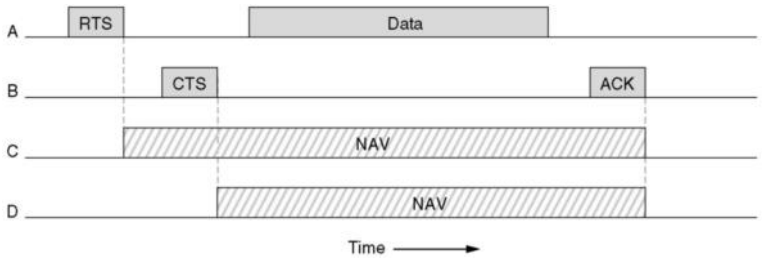


Fig: 5.4 The virtual channel sensing using CSMA/CA

In the above figure, A sends an RTS frame to B when it has data to send. After receiving the request, B responds with CTS if it decides to give permission. A sends its data and starts an ACK timer when it get the CTS from B. B sends an ACK frame after receiving the correct data. If the ACK reach A after the ACK timer of A expire, the whole protocol is run again.
C receives the RTS as it is in the range of A. Then C generates a virtual channel busy NAV (Network Allocation Vector) for itself. D is in the range of B so it gets the CTS. After getting the CTS, it creates a shorter NAV for itself. NAV is adjusted from the duration field in the data frame or in RTS and CTS frames. The stations which asserts NAV are not allowed to transmit data to avoid collisions

STOP TO CONSIDER
NAV is a virtual carrier sensing mechanism with collision avoidance (CSMA/CA). This signal is not transmitted. It is only an internal reminder to remain quiet for certain amount of time. The NAV can be considered as a counter which counts down to zero. When the counter is zero, the virtual carrier-sensing indicates that the channel is idle. When it is nonzero, the channel is busy.

For noisy channel, long packets have less probability of being successfully transmitted. It will results high error rates. To solve

this problem, 802.11 allow fragmentation with stop-and-wait protocol on the fragments.

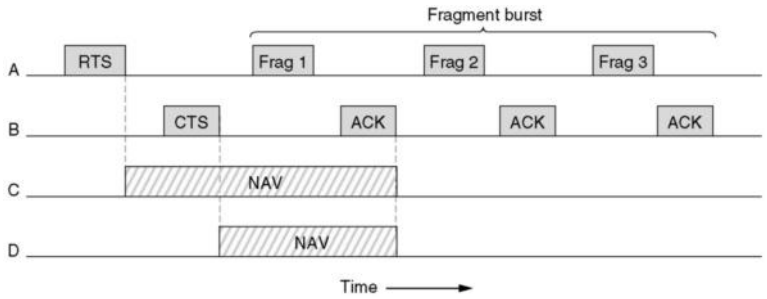


Fig:5.5 Data fragmentation

Multiple fragment can be transmitted in a row after getting the channel. It will increases the throughput because the bad fragment is only transmitted rather than the entire frame.

5.6.1.2 Point Coordination Function

It is an optional function used by 802.11 MAC Sublayer. The point coordination function (PCF) is a polling-based access scheme with no contention. The base station performs polling for stations that wants to transmit data. Base station sends beacon frame periodically.The various stations are polled one after the other. In PCF, the base station takes control of the transmission. So no collision occurs.

STOP TO CONSIDER
Beacon frame contains network information needed by a station before it can transmit a frame. They are used for announcing the presence of devices in a WLAN as well as synchronization of the devices and services. It is a management frame.

5.6.1.3 Co-existence of PCF and DCF

In 802.11, point and distribution control function can co-exist using interframe Spacing. The Inter Frame Spaces define the minimum time that a station needs to wait after it senses the channel free. Shorter IFS denotes a higher priority to access the medium. Four different intervals are defined for their specific purpose.

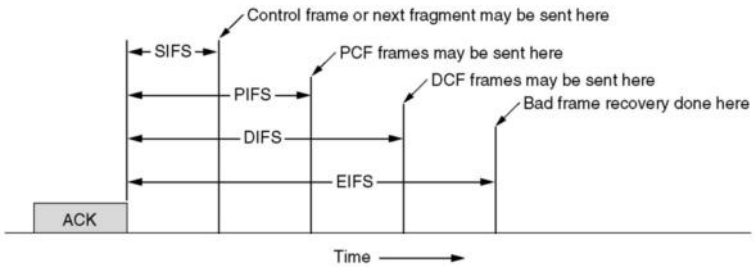


Fig:5.6 Interframe spacing in 802.11

1. **SIFS**
   SIFS (Short Interframe Spacing) is the shortest IFS used for the high priority frames like acknowledgement frames, CTS frames, poll response etc. The transmission of fragment should begin only after the channel is sensed to be idle for a minimum time period of at least SIFS.

2. **PIFS**
   when no station responds to SIFS and a time PIFS (PCF Interframe Spacing) time out, then the base station can issue beacon or poll which allow a station to send data frame.

3. **DIFS**
   When there is no PIFS and a time DIFS (DCF interframe Spacing) expire, any station can attempt to acquire the channel to transmit data frame. It is equal to SIFS plus two time slots and is the longest inter frame gap.

4. **EIFS**
   Extended IFS is the lowest priority interval used to report bad or unknown frame.

CHECK YOUR PROGRESS

11. ———— is the standard for WLAN.
12. The original standard of WLAN uses ———— and ———— transmission technique.
13. The throughput of IEEE standard 802.11b is less than equal to ————.
14. CSMA/CA uses both ———— and ———— in DCF.
15. State true or false

a. 802.11 allow fragmentation of data using sliding window protocol.

b. DCF performs polling for station.
c. When PIFS time out, base station can send beacon frame.

5.7 Protocol stack

A protocol stack refers to a group of protocols that are runnning concurrently. The interconnectivity rules for a layered network model are determined by the protocol stack. To become a stack, the protocols must be interoperable to being able to connect both vertically between the layers of the network and horizontally between the end-points of each transmission segment. A certain similarity of structure is used by the all the 802 variant. A partial view of 802.11 protocol stack is given in the following figure---

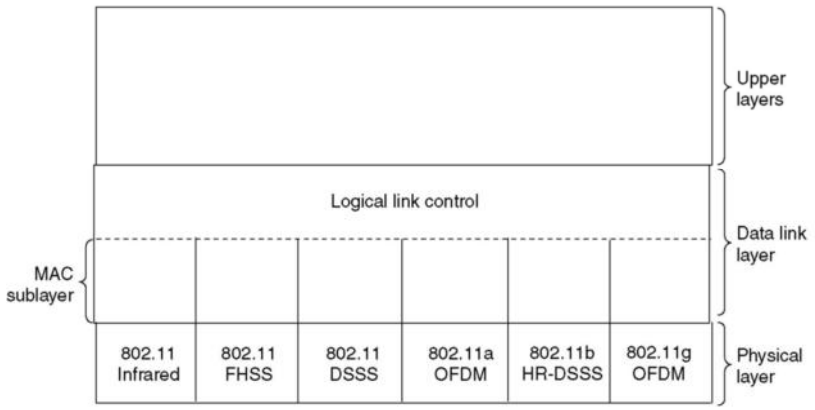


Fig:5.7 Part of 802.11 protocol stack

5.7.1 Data link layer

The data link layer is split into two sub layer

- Logical Link Control
- MAC sublayer

The dissimilarity between the different standard of 802 are hidden by the logical Link Control (LLC). Thus LLC makes 802 standards identical for the network layer. MAC sublayer determines who acquire the channel to transmit next.

5.7.2 Physical layer

The physical layer resembles to the OSI layer. It is responsible for converting data stream into signals. The bits of 802.11 networks can be converted to radio waves or infrared waves.

5.8 Physical layer transmission technique

There are five transmission techniques allowed in the physical layer. The techniques are Infrared, FHSS, DSSS, OFDM and HR-DSSS. We will discuss it briefly in next section. It is possible to send data from one station to another using the transmission technique.

5.8.1 Infrared

It uses diffused infrared light in the range of 800 to 950 nm. It allows two different speeds that are 1 Mbps and 2Mbps. For converting digital signal to analog, pulse position modulation (PPM) is used. Infrared method uses the same technology as television remote controls.

5.8.2 FHSS

Frequency Hopping spread spectrum (FHSS) spreads the signal over a wider frequency to minimize the interference from other devices. This method uses 2.4 GHz ISM band. This band is divided into 79 subbands of 1MHz with some guard bands. A pseudo random number generator selects the hopping sequence. The allowed data rates are 1 or 2 Mbps. This method uses frequency shift keying for modulation.

5.8.3 DSSS

Direct Sequence Spread Spectrum spreads signal over entire spectrum using pseudo-random sequence as CDMA. Each bit is transmitted in an 11-bit chipping Barker sequence. It uses phase shift keying (PSK) technique at 1 M baud. This technique operates on1 or 2 Mbps.

5.8.4 OFDM

Orthogonal Frequency Division Multiplexing (OFDM) uses for signal generation. This method is capable of delivering data upto 18 or 54 Mbps. It uses 5 GHz ISM band. The data rate is 18 Mbps if phase shift keying (PSK) is used for modulation. If quadrature amplitude modulation (QAM) is used, the data rate can be 54

Mbps. It uses 5 GHz ISM band. This band is divided into 52 subbands. 48 sub bands are used for data and 4 sub bands are used for control information.

5.8.5.1.1 HR-DSSS

High Rate Direct Sequence Spread Spectrum(HR-DSSS) uses 11 million chips/sec. It achieves 11 Mbps in 2.4 GHz band. It supports four data rates: 1,2,5.5 and 11 Mbps. 1 Mbps and 2 Mbps data rates uses phase shift modulation.

5.9 Frame structure

The 802.11 framing is complex because the wireless medium requires several management features and frame types that are not required in wired networks. It defines three types of frames that are data, control and management.
Data frame are used for carrying data and control information. Control frame are used for accessing the channel and acknowledging frames. The control frames are RTS and CTS. Management frame are used for initial communication between stations and access points.

The 802.11 frames consist of 9 fields. The following figure shows the basic structure of an IEEE 802.11 data frame along with the content of the frame control field.

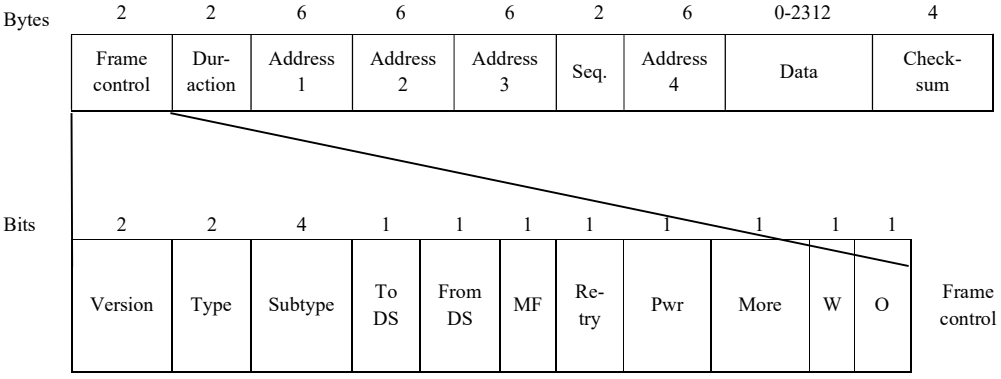


Fig:5.8 The data frame structure of 802.11

Frame Control is a 2 bytes starting field composed of 11 subfields. It defines type of frame and some control information. The 11 subfields are –

1. **Version** − It is a two bit long field which indicates the current protocol version which is fixed to be 0 for now. It has been included to allow future versions of IEE 802.11 to operate simultaneously.
2. Type − It is a two-bit subfield that specifies whether the frame is a data frame, control frame or a management frame.

3. Subtype − It is a four bit long field which indicates sub-type of the frame. It states whether the field is a Request to Send (RTS) or a Clear to Send (CTS) control frame. For a regular data frame, the value is set to 0000.

4. To DS – It is a single bit subfield indicating whether the frame is going to a distributed system. This bit is set to 1 if the frame was sent to the DS.
5. From DS – It is a single bit subfield and set to 1 if the frame is coming from the distributed system.

6. MF – It is a single bit subfield which is set to 1 to indicate that the fragments is followed by more fragment.

7. Retry −It is single bit long field and set to 1 if the current frame is a retransmission of an earlier frame.

8. Pwr − It is 1 bit long field which indicates the mode of a station after successful transmission of a frame. It is set to 1 to indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.

9. More Data – It is a single bit subfield to indicate that sender has further data frames for the receiver.

10. W ─ It is 1 bit long field which indicates that the frame body has been encrypted using WEP algorithm.
11. Order ─ It is 1 bit long field. It is set to 1 to inform the receiver that the frames should be in an ordered sequence.

Duration is a 2-byte field that specifies the time period for which the frame and its acknowledgement occupy the channel.

Address fields are 6-byte address fields which contain standard IEEE 802 MAC addresses (48 bit each). Two addresses contain

the addresses of source and destination. And the other two are source and destination base station respectively.

Seq is a 2 bytes field that stores the frame numbers. Among the 16 bits, the 4 bits identifies the fragment and the rest 12 bits identifies the frame.

Data is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver. The maximum size of data field is 2312 bytes.

Checksum is 4 bytes long and contains a 32 bit CRC error detection sequence to ensure error free frame.

5.10 Services

The 802.11 standard services provide the functions that requires for sending data between two entities on the network. These services fall into two categories

- Distribution Service
- Station Service

5.10.1 Distribution Service

Access points provide distribution services that deal with station mobility. The distribution service is used to manage cell membership and to interact with stations outside the cell. Distribution system services provide functionality across a distribution system. The function are--

5.10.1.1 Association

Each station use the association service to connect an access point before it can send information through a distribution system. The association maps a station to the distribution system via an access point. A station moves within the radio range of base station and use this service. It declares its identity and capabilities after arrival. Each station can associate with only a single access point, but each access point can associate with multiple stations. The base station may accept or reject the mobile station.

5.10.1.2 Disassociation

A station or access point can invoke the disassociation service to break an existing association. Stations should use disassociation before leaving the network. An access point may disassociate all its stations before removed for maintenance.

5.10.1.3 Distribution

A station uses this service for sending frames to the base station. The distribution service provides information about how to route frames sent to base station. A frame can be sent over air directly when the destination is local for base station. If not, the frame has to be sent over wired network.

5.10.1.4 Reassociation

The reassociation service enables a station to change its current state of association. A station can change its association from one access point to another by this service. The mobile station always initiates the reassociation service. No data will be lost due to handover if the service is properly used.

5.10.1.5 Integration

The integration service enables the delivery of a frame through a non-802.11 network. The integration function performs all required translations from the 802.11 format to the required format of destination network.

5.10.2 Station Service

The 802.11 standard defines services for providing functions among stations. All access points implement station services. This service is used after a station connects to base station. To provide necessary functionality, these stations need to implement adequate levels of security.

5.10.2.1 Authentication

Every 802.11 station must use the authentication service before establishing a connection with another station with which it will communicate. Stations performing authentication send a unicast management authentication frame to the corresponding station. This type of authentication assumes that each station has received a secret shared key through a secure channel independent from the 802.11 network. Stations authenticate through shared knowledge of the secret key. 802.11 requires mutually acceptable, successful authentication before association

5.10.2.2 Deauthentication

A station invokes the deauthentication service when it wants to disassociate from another station. Deauthentication is a notification and cannot be refused.

5.10.2.3 Privacy

All stations and other devices can hear data traffic taking place within range on the network. It affect the security level of a wireless link. So data sent over the Wireless network must be encrypted. The encryption and decryption are managed by this service.

5.10.2.4 Data Delivery

This service determines how data are transmitted and received. Detecting and correcting errors must be handled by the higher layers.

CHECK YOUR PROGRESS

16. The data link layer in 802.11 protocol stack is divided into ———— and ————.
17. DSSS uses ———— modulation technique.
18. ———— frames are used for accessing the channel and to acknowledge frames.
19. Source and destination address are stored in ———— fields of data frames.
20. state true or false

a. The maximum size of data field in 802.11 data frame structure is 2312 bytes.

b. In association, an access point can associate with a single station.

c. Privacy service in 802.11 manages encryption and decryption.

5.11 SUMMING UP

- A Wireless LAN connects computers without using network cables. Computer uses radio frequency to send data between each other.
- You can communicate directly with other wireless computer or connect to an existing network through an access point.
- User can use Internet, check mail while they are moving. WLAN are flexible with independent design. It eliminates the direct cost of cabling. But it is prone to interference and noise.
- Wireless station has two types of station that are Wireless access point and clients.
- WLAN has two types of service that are Basic service set (BSS) and Extended service set (ESS).
- WLAN has two modes of operation that are infrastructure and Ad hoc mode. In infrastructure mode, communication uses an access point and in Ad hoc mode, there is no access point.
- CSMA protocol lead to hidden station and exposed station problem. MACA is used to solve these problem using RTS and CTS frame but it may also lead to collision.
- MACAW is an improved version of MACA designed for WLAN. It uses ACK frame after each data frame.
- The IEEE 802.11 is a standard for WLAN. 802.11a, 802.11b, 802.11g and 802.11n are some important standard of IEEE 802.11.
- The IEEE 802.11 sublayer protocol uses two functions DCF and PCF. DCF uses physical channel sensing and virtual channel sensing with CSMA/CA. 802.11 allows data fragmentation for noisy channel which increase throughput. PCF performs polling for station and use beacon frame periodically.
- DCF and PCF can co-exist using interframe spacing.

- In 802.11 protocol stack, the data link layer is subdivided into two sublayer that are logical link control and MAC sublayer. The physical layer uses five different data transmission technique Infrared, FHSS, DSSS, OFDM and HR-DSSS.
- 802.11 support three types of frames that are data, control and management frames.
- Access point provides distribution service for station mobility and station service relate to activity within in a single station.

5.12 ANSWERS TO CHECK YOUR PROGRESS

1. Radio frequency
2. Two
3. BSSID
4. Routers
5. a. F b. T c. F
6. 802.11 MAC
7. CSMA
8. Request to Send
9. MACW
10. a. T b. F c. T
11. IEEE 802.11
12. FHSS and DSSS
13. 11 Mbps
14. Physical channel sensing and virtual channel sensing
15. a. F b. F c. T
16. Logical link control and MAC sublayer
17. Phase shift keying
18. Control
19. Address
20. a. T b. F c. T

5.13 POSSIBLE QUESTIONS

Short answer type questions:

1. Why do you need WLAN?
2. What are the uses of WLAN?
3. What do you mean by station in WLAN?

4. What is the Extended Service set?
5. What do you mean by Ad hoc mode in WLAN?
6. What is the hidden station problem?
7. What do you mean by exposed station problem?
8. What is the main idea behind MACA?
9. What is IEEE 802.11?
10. What is the principle behind point Coordination Function?
11. What is the principle behind FHSS?
12. What is infrared transmission?
13. What are the main types of frame in 802.11 frame structure?
14. Explain the importance of version field in 802.11 frame structure.
15. What are the main types of service present in 802.11 standard?
16. Define the authentication service in IEEE 802.11.

Long answer type questions:

1. What is WLAN? Discuss its advantages and disadvantages.
2. What are the types of WLAN? Explain.
3. How can MACA protocol be used to solve hidden and exposed station problem? Explain.
4. Explain the DCF mechanism used in IEEE 802.11 WLAN.
5. Explain the advantages of MACAW over MACA.
6. Explain some important standard of IEEE 802.11.
7. What do you understand by inter frame spacing. Explain briefly its type.
8. Explain the 802.11 protocol stack.
9. Describe the different transmission technique used in the physical layer of 802.11.

10. Explain briefly the different field present in 802.11 data frame structure.
11. What are the 802.11 standard distribution services? Explain.

5.14 FURTHER READINGS

1. Tanenbaum, Andrew S. Computer Network. Pearson.
2. https://ecomputernotes.com/computernetworkingnotes/communication-networks/wireless-lan.
3. https://www.tutorialspoint.com/what-are-wireless-lans.

UNIT 2 THE NETWORK LAYER: ROUTING

CONTENTS

2.0 INTRODUCTION

The main responsibility of the network layer is the source-to-destination delivery of a packet via multiple networks or links unlike the data link layer which is responsible for delivery of a packet on the same network or links. The network layer focuses on that each packet which origins from its source must reach its final destination host. When a device finds that there are multiple paths to reach a destination, it selects a path (preferably the best one) over others. This mechanism of selecting the possible best path is termed as *routing*, one of the functions of the network layer. The routing process is performed by network layer (layer 3) devices such as a router or a layer 3 switch.

2.1 UNIT OBJECTIVES

After completing this unit, you will be able to learn:

- Why routing is needed?
- Goals of routing
- Basic concepts of congestion
- Adaptive and Non-adaptive Algorithms used for Routing
- The concept of the optimality principle
- Various widely used shortest path routing algorithms and their working rules.
- Unicast, broadcast, multicast and hierarchical routing
- Applications of queuing theory in computer networks

2.2 CONCEPTS OF ROUTING & CONGESTION

In case, all hosts (systems) are attached to a same single physical segment then there is no need of routers or any routing protocols to communicate within them. See *fig 4.1* where all the hosts are present on the same segment and they can communicate among them without any router or any routing algorithm.

Routing involves the delivery of packets or datagrams between end systems situated on different networks. It is a process or

mechanism to choose an optimal path between the source and destination which is performed by a device which works on network layer (layer 3). *Fig 2.2* depicts how a router provides physical connection between different subnets or different networks to communicate from one end to the other end. Routers are configured with some type of routing algorithm to enable communication between hosts when they are situated outside the local segment.

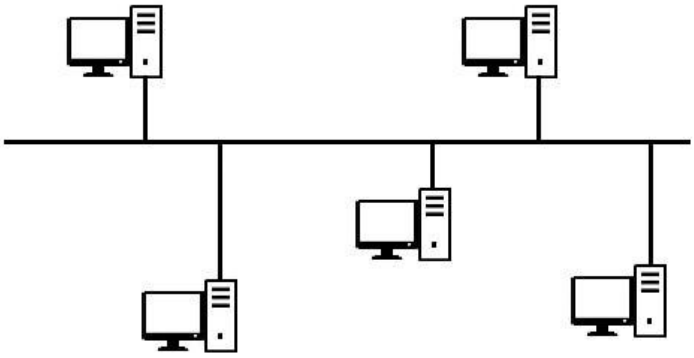


Fig 2.1: All systems located on a single segment

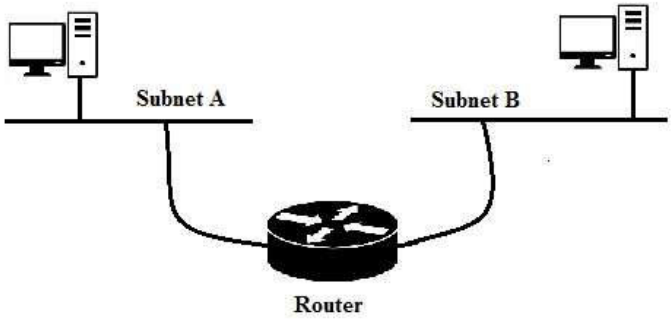


Fig 2.2: Different subnets connected by Router

There are some major goals of routing, which are:

- **Correctness:** Routing should be done properly and accurately so that the packets may reach their destination correctly.
- **Simplicity:** The network overhead increases with increasing the complexity of the routing algorithms. That is why Routing should be done in a simple manner to keep the overhead as low as possible.

- **Robustness:** The routing algorithms should be robust enough to handle the changes in the network topology and should be able to handle any failures in software or hardware without the need to abort all the jobs in all hosts and without rebooting the network whenever a router goes down.
- **Stability:** Under all possible conditions the routing algorithms should be stable.
- **Fairness:** Each and every node present in the network should get a fair chance of transferring its packets; which is usually done on a first come first serve basis.
- **Optimality:** Routing algorithms should be optimal in terms of increasing the throughput and minimizing the mean packet delays. There is a trade-off here and one has to choose which one is more suitable as per need.

On the other hand, congestion is a state of the network which deteriorates the network service because of carrying high amount of data which may lead to packet loss or frame loss. When congestion occurs in a network the throughput of the network decreases along with the response time. In a network, congestion may occur when the allotted bandwidth becomes insufficient as the data traffic exceeds the capacity of the network bandwidth.

Congestion in a network may lead to *congestion collapse*- a condition in which the useful communication gets limited or prevented. Network congestion and collapse can be avoided by these two major components:

- When the routers detects that critical level (exceeding the handling capacity) is reached while receiving the data packets, the router should be capable of dropping or reordering the packets.

- Use of any flow control mechanisms to respond efficiently whenever data flow rates reach the critical level or exceeds the handling capacity.

Check Your Progress

1. This mechanism of selecting the best possible path is termed as _____.

   a) Congestion b) Routing

   c) Path finding d) None of these

2. Which one is **not** a goal of routing?

   a) Correctness b) Optimality
   c) Robustness d) Complexity

3. Router is a _____ device.

   a) layer 1 b) layer 2

   c) Layer 3 d) Layer 7

4. *State TRUE or FALSE:*

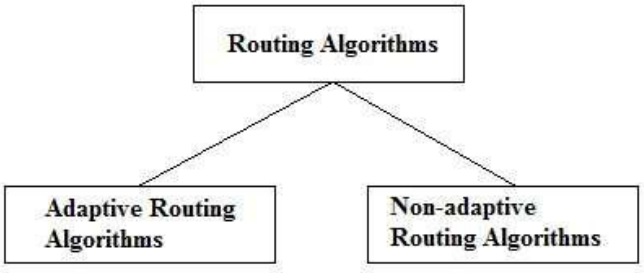
   a) Congestion in a network may lead to congestion collapse.

   b) Routing deteriorates the network service.

   c) Congestion increases- throughput increases.

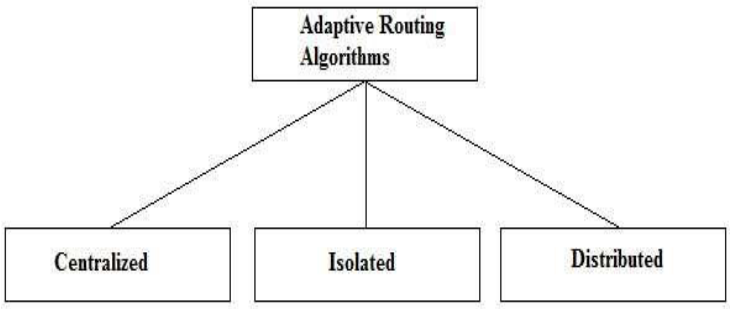
2.3 ROUTING ALGORITHMS

So far, we have learnt that Routing is the mechanism to forward the data packets from source to destination. But in order to find the best route or path from source to destination the network layer uses various routing algorithms or routing protocols through which the data packets can be transmitted. The routing algorithms can be classified as:



Adaptive Routing Algorithms:

Whenever there is a change in the network topology or the network traffic load these algorithms changes their routing decisions. That is why these algorithms are also known as dynamic routing algorithms. The main parameters considered by these algorithms while updating the routing table are hop count, distance measure, estimated transmit time and delay etc. Furthermore, the adaptive algorithms can be classified into three categories such as:



Centralized algorithms:

In centralized algorithm, there is centralized node which has all the necessary global information related to the network and based on that it takes all the routing decisions to find the best route or optimal path. So, it is also termed as global routing algorithm. As the involvement of other nodes is very less, the resource requirement becomes very less too as all information are stored in the centralized node only. However, if only the central node goes down then the whole routing fails as the performance is too much dependant on the central node only. Centralized algorithms need to aware the cost of the links prior to performing any calculations. *Link State Routing* is one example of such algorithm which is aware of the costs of the paths or links present in the network.

Isolated algorithms:

In isolated routing, the routing decisions are made based on the local information available to them instead of seeking those from other nodes. Here, any information regarding the status of the links or paths is not known. Though this helps in making the routing decision faster but these algorithms may result in delay as the nodes may transmit data through a congested network. Some

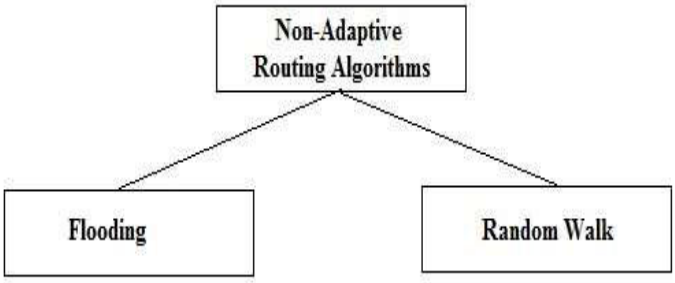
examples of this type of algorithm for routing are: *Hot Potato* and *Backward Learning*. In hot potato algorithm, when a packet arrives to a node, it tries to get rid of that packet as fast as it can, by sending it on the shortest output queue without considering where that link leads. In backward learning algorithm, the routing table at each node is updated by the information it receives from the incoming packets. Backward learning can be implemented by including the identity of the source node in each packet with a hop counter that is incremented with each hop. When a node receives a packet, it counts the number of hops it has passed through from the source node to reach it. If the previous hop count value is found better than the current value then it does nothing but if the current value is found better than the previous one then the value is updated for future use.

Distributed Algorithms:

In distributed routing algorithms, the nodes gathers the information form their neighbours and based on that the decision is taken which way to transmit the packet. It is also called as decentralized algorithm as no node has all the information related to cost of all the paths from source to destination. A node has the information of its directly connected nodes only and the complete least-cost path to the destination is calculated in an iterative and distributed manner. *Distance Vector Routing* is an example of this category where it never knows the complete path from source to destination. So, it forwards the packet to the direction through which the packet to be transmitted finding the least-cost path.

Non-adaptive Routing Algorithms:

The non-adaptive routing algorithms are also termed as static routing algorithms as they do not change their routing decisions based on the variations on the network traffic and topology. In fact, the route to be chosen to transmit packets from one node to another is determined in advance. The static routing table is formulated depending on the routing information stored in the routers when the network is booted. Once the static paths are computed and made available to all the routers, they start transmitting the packets through these paths. The routing decisions remain unaffected to any changes in the network. Non-adaptive routing algorithms can further be categorized as:



Flooding uses the technique in which a node forwards every incoming packet to every outgoing line except the one through which it arrived. Flooding in more detail will be discussed later on this unit.

Random Walk is a highly robust algorithm in which a node forwards a packet to one of its neighbours randomly. This is a probabilistic protocol to select the next random node to forward the data packet, so it does not have the need of any global information.

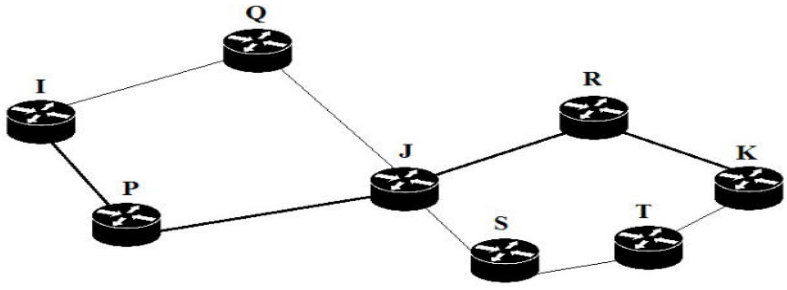
2.4 THE OPTIMALITY PRINCIPLE

A routing algorithm enables a router to find the output path through which an incoming packet can be forwarded. The path should be a least cost or optimal path. The optimality principle states that:

Given a network of routers, if a router 'J' lies on the optimal path from router 'I' to router 'K', then the optimal path to router 'J' to router 'K' also lies on the same route.

The optimality principle logically implies that:

If a better route between router J and router K is obtained and updated then the path from router I to router K is also updated via the same route. To understand this, let's consider an example:



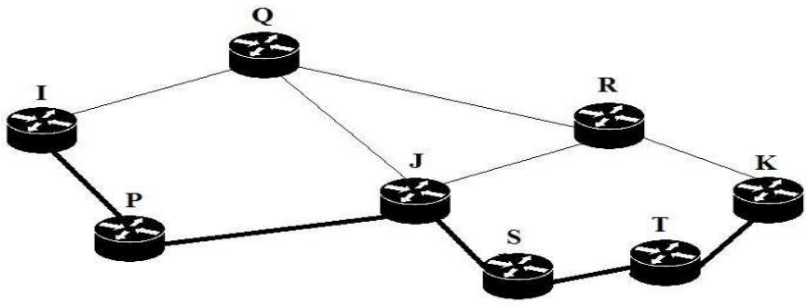


Fig 2.3 a (above) & 2.3 b (below): Optimal paths

Let's consider a network of routers I-P-Q-J-R-S-T-K shown in *fig 2.3 a & b.* In case of *fig 2.3 a,* let's consider the optimal path from router I to router K be via I-P-J-R-K which is shown in bold line. Here, according to optimality principle the optimal path from router J to router K will also fall on the same route which is J-R-K. Now, suppose a better route from router J to router K is found via J-S-T-K and updated as optimal route to router J to router K, then the optimal route from router I to router K is also updated via that route which becomes I-P- J-S-T-K.

Check Your Progress

5. Adaptive routing algorithms are also termed as _____ algorithms.

   a) Static Routing b) Dynamic Routing
   c) Fixed Routing d) None of these

6. Link State Routing is an example of _____ algorithms.

   a) Distributed adaptive routing
   b) Non- adaptive routing
   c) Centralized adaptive routing
   d) Isolated adaptive routing

7. *State TRUE or FALSE:*

   a) Non-Adaptive routing algorithms are also termed as dynamic routing algorithms.

   b) Flooding is an example of adaptive routing algorithms.

   c) Optimality principle helps to find and update least cost path.

2.5 SHORTEST PATH ROUTING

The goal of the shortest path routing is to minimize the routing cost by obtaining the shortest path between the nodes by applying some graph theory approaches. Some of the shortest path routing algorithms are:

- Dijkstra's Algorithm
- Bellman Ford's Algorithm
- Floyd Warshall's Algorithm

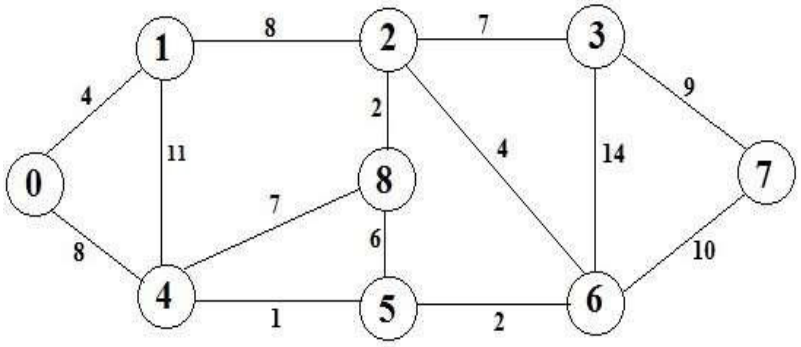
2.5.1 DIJKSTRA'S ALGORITHM

This algorithm finds the shortest path from a single node (source) to all other nodes (vertices) in a weighted graph. Let's understand the working of Dijkstra's algorithm with an example.

The Algorithm:

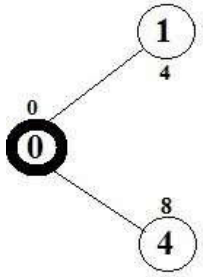
1. Find a shortest-path tree set (*SPT*) that keeps track of vertices included in the shortest-path tree, Initially, this set is empty.
2. The distances from the Source Node to all other vertices are set to ∞.
3. While *SPT* doesn't include all vertices
    a) Pick a vertex u which is not there in *SPT* and has a minimum distance value.
    b) Include u to *SPT.*
    c) Update distance value of all adjacent vertices of u. To update the distance values, iterate through all adjacent vertices. For every adjacent vertex v, if the sum of distance value of u (from source) and weight of edge u - v which is given by $c(u, v)$, is less than the distance value of v , then update the distance value of v. That means If $d(u) + c(u, v) < d(v)$ then $d(v) = d(u) + c(u, v)$ [*principle of relaxation*].

Consider the following graph:

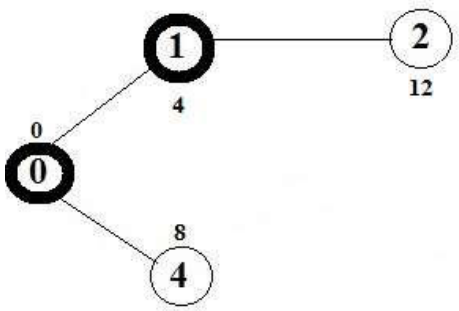


For the above weighted graph let's consider the Node 0 be the source node from which the shortest paths to all other vertices are to be found using Dijkstra's algorithm.

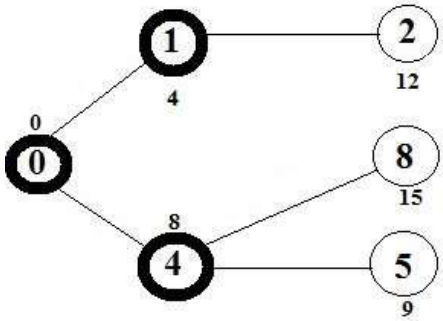
Initially *SPT* is kept empty and distances assigned to vertices are $[0,\infty,\infty,\infty,\infty,\infty,\infty,\infty]$. The vertex 0 is picked as source node, included it to the *SPT*. So *SPT* becomes [0]. After inserting node 0 to *SPT*, the distances of its adjacent vertices are updated. The adjacent vertices of node 0 are node 1 and node 4. The distance values of node 1 is updated as 4 as $d(u) + c(u, v) = 0 + 4 = 4$ which is less than $d(v) = \infty$. Similarly the distance value of node 4 is also updated as 8. The following sub graph shows the vertices and their distance values. Bold vertices are added to the SPT.



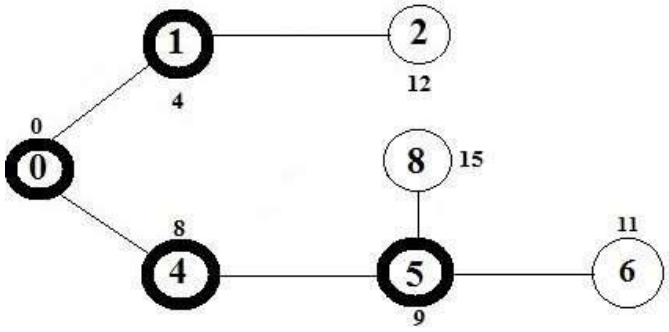
Next, select the vertex with minimum distance value which is not already included in the SPT. The vertex 1 is selected and inserted into SPT. Now the SPT becomes [0, 1]. The distance values of the adjacent vertices of node 1 are updated, so the distance value of node 2 becomes 12.



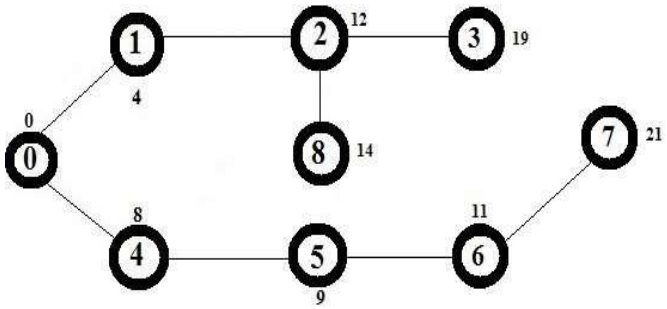
Next, select the vertex with minimum distance value which is not already included in the SPT. The vertex 4 is selected and inserted into SPT. Now the SPT becomes [0, 1, 4]. The distance values of the adjacent vertices of node 4 are updated. So, the distance values of node 5 and node 8 are updated as 9 and 15 respectively.



Next, select the vertex with minimum distance value which is not already included in the SPT. The vertex 5 is selected and inserted into SPT. Now the SPT becomes [0, 1, 4, 5]. The distance values of the adjacent vertices of node 5 are updated. So, the distance value of node 6 is updated as 11 and the distance value of node 8 is remained unaffected.



The steps are repeated iteratively until we get all the vertices inserted in the SPT. Finally the following SPT is found:



The weights written outside the nodes indicate the shortest distance from the source node which is node 0 in the above example.

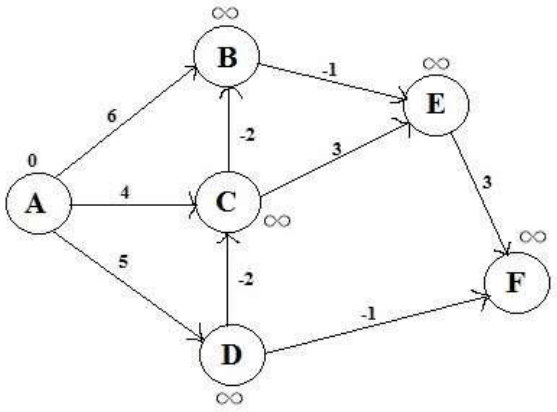
2.5.2 BELLMAN FORD'S ALGORITHM

Dijkstra algorithm finds the shortest paths from the source node to all other target nodes but it may fail to find the shortest paths in the graphs having negative weights. Bellman Ford's algorithm works correctly for such graphs. But it it is also noteworthy that Bellman Ford's algorithm is slower than Dijkstra's algorithm. The working principle of the Bellman Ford's algorithm is based on the *principle of relaxation* which states that if $d(u) + c(u,v) < d(v)$ then $d(v) = d(u) + c(u,v)$ for every adjacent vertex v from source u.

Algorithm

1. Initialize distances from the source node to all other vertices as ∞ and distance from the source to itself as 0. Create and initialize array dist[ ] of size |V| with all values as ∞ except dist[src] where src is source vertex and |V| is the number of vertices in given graph.
2. Calculate shortest distances for |V|-1 times where
   a) Do the followings for each edge $u - v$
      if $dist(u) + cost(u,v) < dist(v)$
      then $dist(v) = dist(u) + cost(u,v)$
3. This step ensures if there is any negative weight cycle in graph. To, find that we iterate through all edges and calculate the shortest path once again and if we get a shorter path for any node, then there is a negative weight cycle.

Let's understand this algorithm with the help of an example:
Consider the following graph:



Initially,

A	B	C	D	E	F
0	∞	∞	∞	∞	∞

The graph has |V|=6, so there will be 5 (|V|-1) iterations.

For the iteration 1,
The edges (A,B), (A,C), (A,D), (B,E), (C,E), (D,C), (D,F), (E,F), (C,B) are processed. The order can be as per your choice.
For edge (A,B):
u = A and v = B
$dist(u) + cost(u, v) = 0 + 6 = 6$ which is $< \infty$
So, $dist(v)$ is updated. Hence B = 6
Similarly, if we process other edges the updates will be
For (A,C), C = 4,
For (A,D), D = 5,
For (B,E), E = 5,
For (C,E), E is not updated,
For (D,C), C = 2 (updated again),
For (D,F), F = 4,
For (E,F), F is not updated,
For (C,B), B = 1 (updated once again).
After the completion of *iteration 1*:

A	B	C	D	E	F
0	1	3	5	5	4

For the iteration 2,

The edges (A,B), (A,C), (A,D), (B,E), (C,E), (D,C), (D,F), (E,F), (C,B) are processed again. The updated costs are:

A	B	C	D	E	F
0	1	3	5	0	3

For the iteration 3,

The edges (A,B), (A,C), (A,D), (B,E), (C,E), (D,C), (D,F), (E,F), (C,B) are processed again. The updated costs are:

A	B	C	D	E	F
0	1	3	5	0	3

For the iteration 4,

The edges (A,B), (A,C), (A,D), (B,E), (C,E), (D,C), (D,F), (E,F), (C,B) are processed again. The updated costs are:

A	B	C	D	E	F
0	1	3	5	0	3

For the iteration 5,

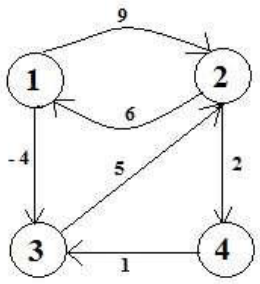
The edges (A,B), (A,C), (A,D), (B,E), (C,E), (D,C), (D,F), (E,F), (C,B) are processed again. The updated costs are:

A	B	C	D	E	F
0	1	3	5	0	3

As you can see after iteration 3 the updating is not performed. But as per algorithm the iterations to be performed is |V|-1 times that is why we performed 5 iterations. There is a drawback of the algorithm that it may produce negative weight cycle in some of the cases.

2.5.3 FLOYD WARSHALL'S ALGORITHM

This algorithm is used to find all pair shortest paths. Unlike Dijkstra where shortest paths are found from just a single source, *Floyd Warshall's Algorithm* finds shortest paths from each of the vertices to all other vertices in just a single run. Let's understand the working of the algorithm with the help of an example.



Considering the above directed weighted graph and let's apply the *Floyd Warshall's Algorithm* to find all pair shortest paths.
Initially a D^0 distance matrix is formed which includes distances to and from all the vertices.

	1	2	3	4
1	0	9	-4	∞
2	6	0	∞	2
3	∞	5	0	∞
4	∞	∞	1	0

Here, distance from node 1 to 1 is 0 and if there is no direct link to other nodes or vertex then that distance is considered as ∞. Using this D^0 matrix, another distance matrix D^1 is formed, using D^1, D^2 matrix is formed and like way depending on the number of total vertices available in the graph other matrices are formed. In this case there will be four distance matrices (D^1, D^2, D^3 and D^4).

D^1 Matrix:
The matrix D^1 is calculated using the matrix D^0. While calculating matrix D^1 , node 1 is considered as an intermediate node to reach other vertices.

	1	2	3	4
1	0	9	-4	∞
2	6	0	**2**	2
3	∞	5	0	∞
4	∞	∞	1	0

As you can see the distance from 2 to 3 which is indicated by $D^1(2,3)$ is updated to 2 (earlier it was ∞).
As node 2 to node 3 can be reached via the intermediate node 1, so
$D^1(2,3)$ $D^0(2,1) + D^0(1,3)$ [*node 1 is intermediate*]

$\infty > 6 + (-4)$ [Values are put using D^0 matrix]

$\infty > 2$

As we have found a lesser value than∞, so it is updated.

Let's find $D^1(2,4)$, which means finding path from node 2 to node 4 keeping node 1 as intermediate node.

$D^1(2,4)$ $D^0(2,1) + D^0(1,4)$

$2 < 6 + \infty$

$2 < \infty$

As there is no direct path from node 1 to node 4, so the value $D^0(1,4)$ becomes ∞ and this results that the previous value of $D^1(2,4)$ will not be updates. And similarly rest other values are also not updated in the matrix D^1.

D^2 Matrix

	1	2	3	4
1	0	9	-4	11
2	6	0	2	2
3	11	5	0	7
4	∞	∞	1	0

As we can see matrix D^2 is updated with a lot of changes keeping node 2 as intermediate node, let's evaluate one value, say $D^2(3,1)$.

$D^2(3,1)$ $D^1(3,2) + D^1(2,1)$

$\infty > 5 + 6$

$\infty > 11$

So, $D^2(3,1)$ is updated to 11.

D^3 Matrix:

Matrix D^3 is updated keeping node 3 as intermediate node.

The resultant D^3 is:

	1	2	3	4
1	0	1	-4	3
2	6	0	2	2
3	11	5	0	7
4	12	6	1	0

D^4 Matrix:

Matrix D^4 is updated keeping node 4 as intermediate node.

The resultant D^4 is:

	1	2	3	4
1	0	1	-4	3
2	6	0	2	2
3	11	5	0	7
4	12	6	1	0

As we have four vertices in the graph, we have to find 4 distance matrices. And this D^4 matrix will give us all pairs of shortest paths from any vertex as source vertex.
Suppose we take vertex 3 as source vertex then the shortest paths to all other vertices can be found using D^4, and these are:

3 → 1 = 11
3 → 2 = 5
3 → 4 = 7

Check Your Progress

8. Principle of relaxation is:

a) If $d(u) + c(u,v) < d(v)$ then $d(v) = d(u) + c(u,v)$
b) If $d(u) + c(u,v) > d(v)$ then $d(v) = d(u) + c(u,v)$
c) If $d(u) + c(u,v) > c(u,v)$ then $d(v) = d(u) + c(u,v)$
d) None of these

9. Single Source shortest path algorithms

a) Find shortest path to all vertices from many sources
b) Find shortest path to all vertices from single source
c) Find all pair shortest paths from all vertices
d) None of these

10. State TRUE or FALSE:

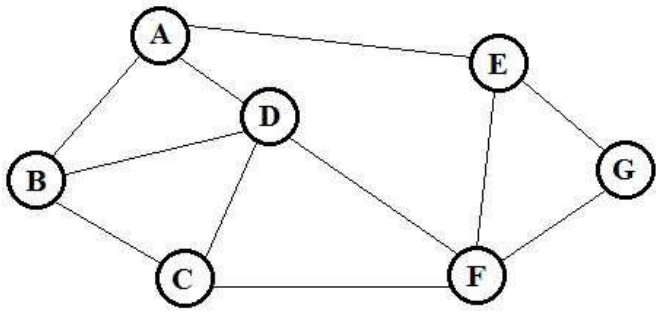
a) Bellman Ford's algorithm is faster than Dijkstra's algorithm.

b) Dijkstra's algorithm works well with graphs having negative weights.

c) Floyd Warshall's Algorithm finds all pair shortest paths.

2.6 FLOODING

Flooding is a non-adaptive routing algorithm which states that whenever a packet arrives at a router, it is forwarded to all the outgoing links of the router except the link through which the packet arrived. Let's consider the following network of 7 routers:



If flooding is applied to the above network then,

- An incoming packet to router A will be forwarded to router B, D and E.
- B again will forward the packet to C and D
- D will forward the packet to C and F
- C will forward the packet to F
- F will forward the packet to E and G
- E will forward the packet to G

Though flooding is a very simple and robust algorithm, here, we can see that a router may receive duplicate packets from other routers which is a disadvantage of flooding. Using a technique called *Hop Count* this can be solved. The *Hop Count* is a counter attached with the packet which is decremented each time the packet passes through a router. Whenever it reaches Zero, the packet is discarded.

Types of Flooding:

Three types of flooding techniques are there.

- Uncontrolled Flooding: an incoming packet to a router is transmitted unconditionally to all the neighbours.
- Controlled Flooding: here, some methods are used to control the forwarding of the packets to its neighbours. Sequence Number Controlled Flooding (SNCF) and

Reverse Path Forwarding (RPF) are two popular controlled flooding algorithms.

- Selective flooding**:** This variant of flooding does not directly forward the packets to all the neighbors; instead, it only uses those lines which are linked to the routers that are approximately in the same direction as the recipient node.

2.7 DISTANCE VECTOR ROUTING

Distance vector routing algorithm is an asynchronous dynamic algorithm in which a node or a router 'X' sends the copy of its distance vector to all its neighbours. Node 'X' also receives the new distance vector from one of its neighbouring nodes, saves the distance vector and uses the Bellman-Ford's equation to find the shortest paths and update its own distance vector. When router X updates its own routing table then it also sends the distance vector to all of its neighbours to update their routing tables. Like this the routing tables of all the nodes are updated. The working of this algorithm is based on exchange of the distance vectors among the nodes that is why this algorithm is called Distance Vector Routing algorithm.

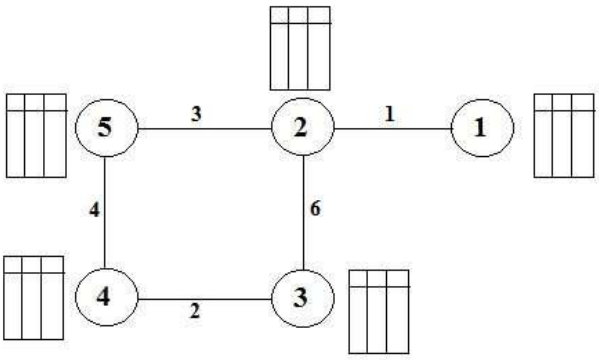
Important Steps of the algorithm:

1. A router exchanges its distance vector (included in a routing packet) to each of its direct neighbors.
2. Each router saves the most recently received distance vector from each of the neighbors.
3. Any router present in the network recalculates its distance vector when:
    - The distance vector received from a neighbor contains different information than before.
    - It discovers a link failure in the network.

When a router x receives new Distance Vector estimate from any neighbor v, it saves v's distance vector and updates its own Distance Vector using the Bellman-Ford's equation mentioned below:

$$Dx(y) = \min\{ C(x,v) + Dv(y), Dx(y) \} \text{ for each node } y \in N$$

Let's understand the working of this algorithm with the help of an example.



The above network has 5 routers and each router has its own routing table. A routing table at least has these three entries as shown below.

Destination	Cost	Next Hop
Node 1	-	-
Node 2	-	-
.	-	-
.	-	-
Node N	-	-

Here, Destination field refers to the destination from the source router, Cost refers to the distance or cost of the path upto that destination and Next Hop signifies the next node or next router through which the destination is reached.

First of all, each router or node creates its own routing table locally.

Routing table of node 1:

Destination	Distance	Next Hop
Node 1	0	Node 1
Node 2	1	Node 2
Node 3	∞	-
Node 4	∞	-
Node 5	∞	-

In this routing table of node 1, the distance from node 1 to itself is 0 and distance from node 1 to node 2 is 1 where the next hop is node 2. But other nodes like node 3, node 4 and node 5 are not reachable directly from node 1, so the cost is kept as ∞ and the

next hop are unknown. Like this, other nodes also create their own routing tables.

Routing table of node 2:

Destination	Distance	Next Hop
Node 1	1	Node 1
Node 2	0	Node 2
Node 3	6	Node 3
Node 4	∞	-
Node 5	3	Node 3

Routing table of node 3:

Destination	Distance	Next Hop
Node 1	∞	-
Node 2	6	Node 2
Node 3	0	Node 3
Node 4	2	Node 4
Node 5	∞	-

Routing table of node 4:

Destination	Distance	Next Hop
Node 1	∞	-
Node 2	∞	-
Node 3	2	Node 3
Node 4	0	Node 4
Node 5	4	Node 5

Routing table of node 5:

Destination	Distance	Next Hop
Node 1	∞	-
Node 2	3	Node 2
Node 3	∞	-
Node 4	4	Node 4
Node 5	0	Node 5

Now, keep it in mind that only the distance column (not the whole routing table) of the routing tables is shared with the adjacent neighbours, which is known as the *Distance Vector*. After receiving these distance vectors from their neighbours, routers update their routing tables and again share the distance vectors

with its neighbours and this process goes on until there is no change in the distance vector.

Let's consider some scenarios while sharing the distance vector

- Router 1 will receive the distance vector from router 2 only, as it is the only adjacent neighbour.
- Router 2 will receive the distance vectors from router 2, router 3 and router 5.
- Router 3 will receive the distance vectors from router 4 and router 5.
- Router 4 will receive the distance vectors from router 3 and router 5.
- Router 5 will receive the distance vectors from router 2 and router 4.

After getting all the distance vectors all nodes updates their routing tables and again the updated distance vectors are shared with the neighbours.

Let's look at the update process of router 1.

The Distance vector received from router 2 is:

Distance
1
0
6
∞
3

This will be used to update the routing table of router 1. And the updated table is:

Destination	**Distance**	**Next Hop**
Node 1	0	Node 1
Node 2	1	Node 2
Node 3	7	Node 2
Node 4	∞	-
Node 5	4	Node 2

We can see that the routing table is updated. Let' see how it's done.

Node 1	0	Node 1

As we know that the distance from node 1 to node 1 the distance is 0, so it is not updated.

Node 2	1	Node 2

Node 2 can be reached via Node 1 → Node 2 and Node 2 → Node 2 path.
Distance of Node 1 → Node 2 = 1 and
distance of Node 2 → Node 2 = 0
So, total distance = 1 + 0 = 1.

Node 3	7	Node 2

Node 3 can be reached via Node 1 → Node 2 and Node 2 → Node 3 path.
Distance of Node 1 → Node 2 = 1 and
Distance of Node 2 → Node 3 = 6 [found form the received Distance vector]
So, total distance = 1 + 6 = 7.

Node 4	∞	-

Node 4 can be reached via Node 1 → Node 2 and Node 2 → Node 4 path.
Distance of Node 1 → Node 2 = 1 and
Distance of Node 2 → Node 4 = ∞ [found form the received Distance vector]
So, total distance = 1 + ∞ = ∞.
This specifies that Node 4 is actually not reachable from Node 1.

Node 5	4	Node 2

Node 5 can be reached via Node 1 → Node 2 and Node 2 → Node 5 path.
Distance of Node 1 → Node 2 = 1 and
Distance of Node 2 → Node 5 = 3 [found form the received Distance vector]
So, total distance = 1 + 3 = 4

Thus, the routing table is updated in router 1.

Let's take one more case how the routing table of router 5 will be updated.
The Router 5 will receive two distance vectors each from Router 2 and Router 4. These are:

Node 2	**Node 4**
Distance	**Distance**
1	∞
0	∞

6	2
∞	0
3	4

The updated routing table will be:

Destination	**Distance**	**Next Hop**
Node 1	4	Node 2
Node 2	3	Node 2
Node 3	6	Node 4
Node 4	4	Node 4
Node 5	0	Node 5

Let's find out how it's updated:

Node 1	4	Node 2

Node 5 to Node 1 can be reached via

Path 1: Node 5 → Node 2 and Node 2 → Node 1.
Path 2: Node 5 → Node 4 and Node 4 → Node 1.

Path 1:
Distance of Node 5 → Node 2 = 3 [known already from its RT]
Distance of Node 2 → Node 1 = 1 [found form the received Distance vector from Node 2]
So, total distance = 3 + 1 = 4

Path 2:
Distance of Node 5 → Node 4 = 4 [known already from its RT]
Distance of Node 4 → Node 1 = ∞ [found form the received Distance vector from Node 4]
So, total distance = 4 + ∞ = ∞

From the two possible cases the least distance is kept, and it is 4.
So, the updated distance becomes 4.

Like this all other entries of the routing table are updated.

This process of updating the routing table goes on each node unless there are no more modifications in the shared distance vectors.

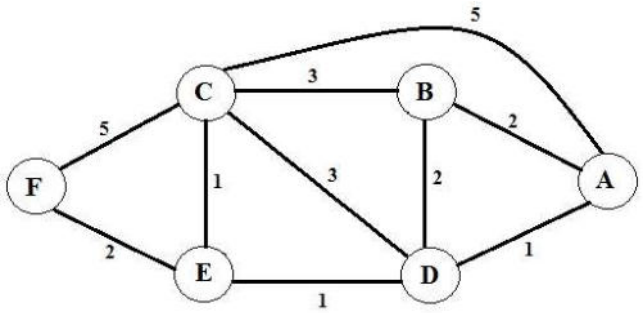
2.8 LINK STATE ROUTING

Link state routing is another routing protocol that has a different philosophy than the distance vector routing. Here, instead of sending a routing table, a node or a router sends some information which is called a *Link State Packet* (LSP) to its neighbourhood using *flooding* and for updating the routing table a router can use Dijkstra's algorithm to find the shortest paths. The Link State Packet carries information about the node identity, sequence number, age and the list of links. So, every node has global knowledge about the network because of the sharing of this LSP packet which is not there in distance vector routing.

Four sets of actions are performed to create the routing table at each node showing the least-cost node to every other node.

1. Creation of the Link State Packet (LSP)
2. Using Flooding in an efficient way distribution of LSPs to every other node.
3. Calculation of shortest path tree at each node (using Dijkstra's algorithm)
4. Formation of Routing Table based on the shortest path tree.

Let's understand the working of this algorithm with the help of an example:
Consider the following network of 6 routers:



Considering the router A as the source router let's proceed step by step:

STEP 1:
This is initialization step. Source **A** has direct neighbours **B, D,** and **C** and the least cost path to reach them are 2, 1 and 5 respectively. Step 1 produces the following:

N	D(B), P(B)	D(C), P(C)	D(D), P(D)	D(E), P(E)	D(F), P(F)
A	2, A	5, A	1, A	∞	∞

Here,
N represents the node processed.
D(v) represents the distance/ cost from the source node to node v,
P(v) represents the previous node (neighbour of v) from the source node along the least cost path.

STEP 2:
We can see in the above table from step 1 that node **D** has the shortest path, there for it is added in N. Now, the shortest path to other nodes will be calculated trough node **D**.

Calculating shortest path from **A to B**:

$D(B) = \min(D(B), D(D) + \text{cost}(D,B))$

$D(B) = \min(2, 1 + 3)$ [Values can be obtained from step 1 table]

$D(B) = \min(2,4) = 2$

Therefore, currently the shortest path becomes 2.

Calculating shortest path from **A to C**:

$D(C) = \min(D(C), D(D) + \text{cost}(D,C))$

$D(B) = \min(5, 1 + 3)$

$D(B) = \min(5,4) = 4$

Therefore, currently the shortest path becomes 4.

Calculating shortest path from **A to E**:

$D(E) = \min(D(E), D(D) + \text{cost}(D,E))$

$D(E) = \min(\infty, 1 + 1)$

$D(E) = \min(\infty, 2) = 2$

Therefore, currently the shortest path becomes 2.

We don't need to find the shortest path from **A** to **F** as there is no direct link to node **F** via node **D**, it will be ∞.

N	D(B), P(B)	D(C), P(C)	D(D), P(D)	D(E), P(E)	D(F), P(F)
A	2, A	5, A	1, A	∞	∞
A,D	2, A	4, D	-	2, D	∞

STEP 3:

We can see in the above table from step 2 that node **B** and **E** both have the shortest paths. Let's take node E and it is added in N. Now, the shortest path to other nodes will be calculated trough node **E**.

Calculating shortest path from **A to B**:

$D(B) = \min(D(B), D(E) + \text{cost}(E, B))$

$D(B) = \min(2, 2 + \infty)$ [Values can be obtained from step 2 table]

$D(B) = \min(2, \infty) = 2$

Therefore, currently the shortest path becomes 2.

Calculating shortest path from **A to C**:

$D(C) = \min(D(C), D(E) + \text{cost}(E, C))$

$D(C) = \min(4, 2 + 1)$

$D(C) = \min(4, 3) = 3$

Therefore, currently the shortest path becomes 3.

Calculating shortest path from **A to F**:

$D(F) = \min(D(F), D(F) + \text{cost}(D, F))$

$D(F) = \min(\infty, 2 + 2)$

$D(F) = \min(\infty, 4) = 4$

Therefore, currently the shortest path becomes 4.

N	D(B), P(B)	D(C), P(C)	D(D), P(D)	D(E), P(E)	D(F), P(F)
A	2, A	5, A	1, A	∞	∞
A,D	2, A	4, D		2, D	∞
A, D, E	2,A	3, E			4, E

STEP 4:

We can see in the above table from step 3 that node **B** has the shortest path. So, it is added in N. Now, the shortest path to other nodes will be calculated trough node **B**.

Calculating shortest path from **A to C**:

$$D(C) = \min(\, D(C)\,,\, D(B) + \text{cost}(B,C)\,)$$

$$D(C) = \min(\, 3,\, 2 + 3\,)$$

$$D(C) = \min(\, 3, 5\,) = 3$$

Therefore, currently the shortest path becomes 3.

Calculating shortest path from **A to F**:

$$D(F) = \min(\, D(F)\,,\, D(B) + \text{cost}(B,F)\,)$$

$$D(F) = \min(4,\, 2 + \infty\,)$$

$$D(F) = \min(4,\, \infty\,) = 4$$

Therefore, currently the shortest path becomes 4.

N	D(B), P(B)	D(C), P(C)	D(D), P(D)	D(E), P(E)	D(F), P(F)
A	2, A	5, A	1, A	∞	∞
A,D	2, A	4, D		2, D	∞
A,D,E	2,A	3, E			4, E
A,D,E,B		3, E			4, E

STEP 5:

From step 4 table we can see that node **C** has the shortest path. So, it is added in N. Now, the shortest path to other nodes will be calculated trough node **C**.

Calculating shortest path from **A to F**:

$$D(F) = \min(\, D(F)\,,\, D(C) + \text{cost}(C,F)\,)$$

$$D(F) = \min(4,\, 3 + 5\,)$$

$$D(F) = \min(4,\, 8\,) = 4$$

Therefore, currently the shortest path becomes 4.

N	D(B), P(B)	D(C), P(C)	D(D), P(D)	D(E), P(E)	D(F), P(F)
A	2, A	5, A	1, A	∞	∞
A,D	2, A	4, D		2, D	∞
A,D,E	2,A	3, E			4, E
A,D,E,B		3, E			4, E
A,D,E,B,C					4, E

STEP 6:

From step 4 table we can see that node **F** has the shortest path. So, it is added in N. The Final routing table is found having the shortest distances to all nodes from source **A.**

.N	D(B), P(B)	D(C), P(C)	D(D), P(D)	D(E), P(E)	D(F), P(F)
A	2, A	5, A	1, A	∞	∞
A,D	2, A	4, D		2, D	∞
A,D,E	2,A	3, E			4, E
A,D,E,B		3, E			4, E
A,D,E,B,C					4, E
A,D,E,B,C,F					

2.9 HIERARCHICAL ROUTING

Hierarchical routing is the arrangement of organizing the routers in a hierarchical way and based on hierarchical addressing. Here the network is divided into different regions or groups are connected in a hierarchical fashion and a router from a particular region knows only about its own domain and other routers. So, the network can be viewed in two levels.

- The sub-network level
- The network level.

In the sub-network level, each node in a region or domain has knowledge about the region's interface with other domains and its peers in the same domain. A region may have different local routing mechanism to handle traffic within the same region and send outgoing packets to the appropriate interface.

In the network level, each region can be considered as a single node connected to its interface nodes. The routing mechanisms at the network level handle the routing of packets between two interface nodes only, with no relation to intra-regional transfer.

Advantages of hierarchical routing are the sizes of the routing tables are smaller which reduces the calculations in updating the tables. But the disadvantage of hierarchical routing is once it is imposed on a network, it is followed and possibility of finding the direct paths is ignored, which may lead to sub optimal routing.

Check Your Progress

11. Bellman Ford's algorithm is used by

a) Links State Routing b) Distance Vector Routing
c) Flooding d) None of these

12. Dijkstra's algorithm is used by

a) Links State Routing b) Distance Vector Routing
c) Flooding d) None of these

13. Which one of the followings is a level in hierarchical routing?

a) Data Link level b) Sub-network level
c) Transport level d) Application level

14. State TRUE or FALSE:

a) Flooding forwards the packets to all the links including the incoming one.
b) Routing tables are comparatively smaller in Hierarchical routing which enhances its performance.

2.10 UNICAST, BROADCAST AND MULTICAST ROUTING

In *unicast routing*, there is one source and one destination which is called one-to-one relationship. A unicast packet sent from one source passes through routers to reach its destination. The routers forward the received unicast packets through only one of its interfaces.

In *multicast routing*, there is only one source and multiple numbers of destinations which is called one-to-many relationship. Here, the source address is a unicast address but the destination address is a group address defining one or more destinations. A multicast packet sent from the source node goes to all destinations belonging to a group. The routers may forward the multicast packets through several of its available interface.

In *broadcast routing*, the source transmits the packet to all the nodes as destinations even if they don't want it. The relationship between the source and destination is called one-to-all. Broadcasting is not usually supported as it creates a huge amount of traffic.

2.11 QUEUING THEORY

Queuing theory is the study of formation, function and congestion of queues or waiting lines with the help of mathematics. A model is constructed for predicting the queue length and waiting time and is known as a queuing model.

A queuing situation involves two parts.

1. Someone or something that requests for a service which is usually referred to as a customer or job or request.

2. Someone or something that completes or delivers the services and is usually referred to as server.

Queuing theory inspects the whole system of waiting in line, including elements like the customer arrival rate, number of servers and customers, waiting area capacity, average service completion time and queuing discipline. Queuing discipline refers to the rules of formation of the queue, for example whether the queue is being formed based on a principle of first-in-first-out, last-in-first-out, prioritized or serve-in-random-order.

Applications of queuing theory includes management of single-server queues, retrial/balking queues, finite-buffer queues, multiple queues and optimization in queues as well. Queuing theory is also applied in performance analysis, various network model constructions and in performance enhancement of routing algorithms.

Check Your Progress

15. Multicast routing is

a) One-to-one relationship

b) many-to-one relationship

c) One-to-many relationship

d) Many-to-many relationship

16. If there is one source and one destination then it is

a) Unicasting b) Multicasting
c) Broadcasting d) Supercasting

17. Mathematical study of queues or waiting lines is known as?

a) Waiting Theory b) Relaxing Theory

c) Queen Theory d) Queuing theory

18. State TRUE or FALSE:

a) In *broadcast routing*, source transmits the packet to all the nodes as destinations even if they don't want it.

b) In Queuing theory, someone that completes or delivers the services is usually referred to as server.

. c) In Multicast routing, a router forwards the packets only via one interface.

2.12 SUMMING UP

- The network layer is responsible for the delivery of individual packets from source to destination host.
- Routing is one of the services provided by the network layer. Routing involves the delivery of packets or datagrams between end systems situated on different networks
- When congestion occurs in a network the throughput of the network decreases along with the response time.
- Adaptive routing algorithms change their routing decisions and also known as dynamic routing algorithms whereas

static algorithms or Non-adaptive routing algorithms don't change their decisions.

- The goal of routing is to find and transmit through the optimal path.
- Dijkstra's Algorithm, Bellman Ford's Algorithm, Floyd Warshall's Algorithms are examples of some shortest path routing algorithms
- Some other dynamic routing algorithms are link state routing and distance vector routing.
- Queuing theory is the study of formation, function and congestion of queues or waiting lines with the help of mathematics. It helps in optimization in network models.

2.13 ANSWERS TO CHECK YOUR PROGRESS

1. (b), 2 (d), 3 (c), 4.a True, 4.b False, 4.c False, 5. (b), 6. (c), 7.a False, 7.b False, 7.c True 8. (a), 9. (b) , 10.a False, 10.b False, 10.c True, 11. (b), 12. (a), 13. (b), 14.a False, 14.b True, 15. (c), 16. (a), 17. (d), 18.a True, 18.b True, 18.c False.

2.14 POSSIBLE QUESTIONS

Short answer type questions:

- What is need of routing? Explain.
- What do you mean by congestion in a network?
- What are the two types of routing algorithms?
- What do you mean by adaptive routing algorithms?
- What do you mean by non-adaptive routing algorithms?
- Give one examples of each adaptive routing algorithms and non-adaptive routing algorithms.
- What do you mean by flooding?
- What do you mean by random walk?
- What is a routing table?
- What do you mean by a distance vector?

- What do you mean by hierarchical routing?
- Explain the terms unicast, multicast and broadcast routing?
- What do you mean by queuing theory?

Long answer type questions:

- Explain the Dijkstra's algorithm to find a single source shortest path in a network.
- Explain the Bellman Ford's algorithm with an example.
- Explain the Floyd Warshall's algorithm with an example.
- Explain the Distance Vector Routing in details with a suitable example.
- Explain the working of Link State Routing in details with a suitable example.
- What is flooding? Explain various types of flooding techniques available.

2.15 FURTHER READINGS

- Behrouz A Forouzan, *Data Communications and Networking,* The McGraw-Hill Companies, Latest edition.

UNIT 4: The Transport Layer: The Services

Unit Structure:

4.1 INTRODUCTION

In this unit, you will learn the delivery of an entire message from an application program on the source device to a similar application program on the destination device.you will learn the all modules and procedures pertaining to transportation of data or data stream. You also learn about the categorization of all modules and procedure needed for the transportation of data in this layer.This layer gives the idea about the peer-to-peer and end-to-end connection between two processes on remote hosts. Transport layer takes data from upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to lower layer (Network Layer) for delivery.This layer ensures that the data must be received in the same sequence in which it was sent. You will study the two main Transport layer protocols Transmission Control Protocol and User Datagram Protocol. You will learn about the different types of transport service primitives, quality of services, connection management, transport control mechanism, flow control.

4.2 UNIT OBJECTIVES

After going through this unit, you will able to:

- Understand the services provided by the transport layer to the session layer.
- Know peer-to-peer and end-to-end connection.
- Know the different types of transport service primitives.
- Describe the connection establishment between processes on remote machine.
- Describe transmission control protocol and user datagram protocol.
- Understand flow control.

4.3 Services for upper layer

The main objective of the transport layer is to provide efficient, reliable and cost-effective service to its users generally processes in the application layer.The main role of the transport layer is to

provide the communication services directly to the application processes running on different hosts.

The basic function of the Transport layer is to accept data from the layer above, split it up into smaller units, pass these data units to the Network layer. This layer ensure that all the pieces arrive correctly at the other end.Transport layers work transparently within the layers to deliver and receive data without errors. The send side breaks application messages into segments (packets) and passes them on to the network layer.The receiving side then reassembles segments into messages and passes them to the application layer. All this must be done efficiently in a way that isolates the upper layers from the inevitable changes in the hardware technology.The Transport layer also determines what type of service to provide to the Session layer, and ultimately to the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent.

4.4 Transport service primitives

A Service is specified by set of primitives. These service are used by user or other various entities to access the service. All these primitives simply tell the service to perform some action or to report on action that is taken by peer entity

The transport layer must provide some operations to application programs, that is, a transport service interface. These interface allow users to access the transport service. Each transport service has its own interface.

The network service is intended to model the service offered by real networks. Real networks can lose packets, so the network service is generally unreliable. The (connection-oriented) transport service, in contrast, is reliable. Real networks are not error-free, but that is precisely the purpose of the transport layer to provide a reliable service on unreliable network**.**

The primitives for simple transport service are

1. **LISTEN:** When the server is ready to accept request of incoming connection, it simply put this primitive into action. LISTEN primitive simply waits for incoming connection request.

2. **CONNECT:** This primitive is used to connect the server by creating or establishing connection with waiting peer.
3. **SEND:** SEND primitive is put into action by the client to transmit it's request that is followed by receive primitive. This primitive send or transfer the message to the peer.
4. **RECEIVE:** This primitive blocks the server. RECEIVE primitive waits for a DATA packet to arrive.
5. **DISCONNECT:** This primitive is used to terminate the connection after which no sender will be able to send any message.

The TPDU (Transport Protocol Data Unit) is used for messages sent from transport entity to transport entity. The TPDUs is exchanged by the transport layer and contained in Packets exchanged by the network layer. And packets are contained in Frames.

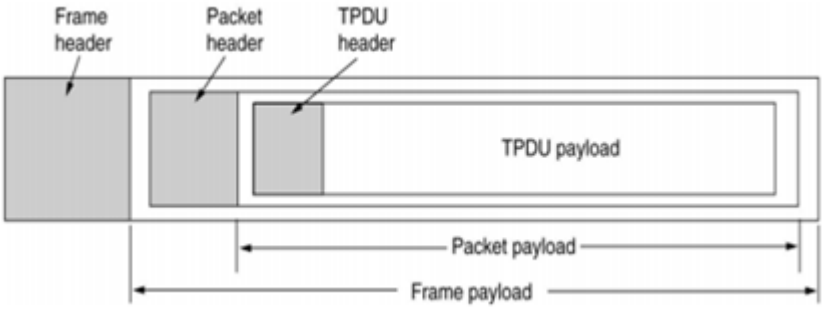


Figure: The nesting of TPDU, Packet and Frame

When a client wishes to talk to the server it issues a CONNECT primitive. Transport entity now blocks the client and sends a packet to the server CONNECTION REQ containing a transport layer message for the server's transport layer. When the CONNECTION REQ arrives at the server, the server's transport entity checks to see if the server is blocked on a LISTEN and can therefore handle server requests. Server is unblocked and a CONNECTION ACCEPTED TPDU is sent back to the client. This unblocks the client and the connection is established
Data is exchanged using SEND and RECEIVE primitives. When the TPDU arrives, the receiver is unblocked. Then the receiver process the TPDU and send a reply. When a connection is no

longer needed, it must be released to free up table space within the two transport entities.
A state diagram for a simple connection management scheme is. shown in figure below

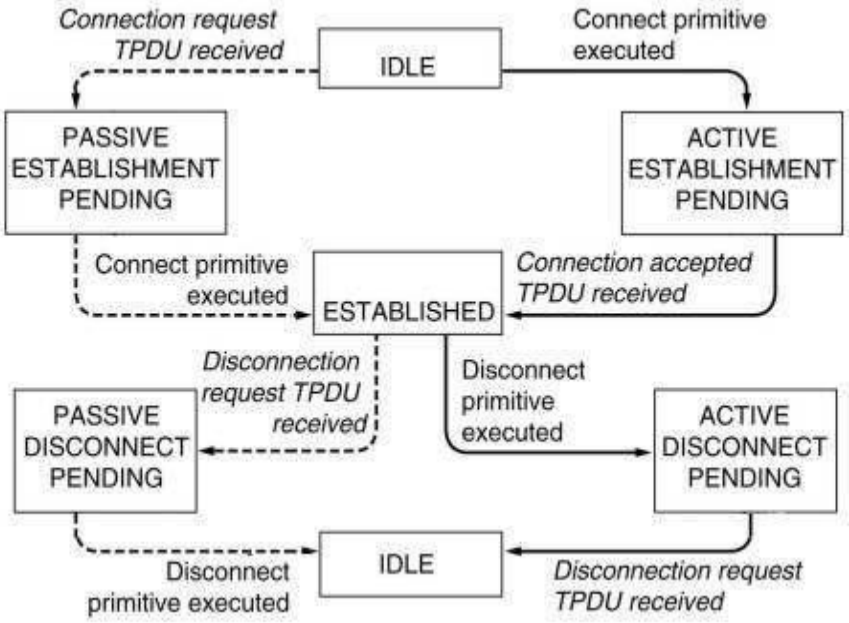


Figure:simple connection management scheme

Transitions labeled in italics are caused by packet arrivals. The solid lines show the client's state sequence. The dashed lines show the server's state sequence.

CHECK YOUR PROGRESS

1. Transport layer is the _____th layer of OSI Model.
2. The _____ is responsible for end to end delivery, segmentation, and concatenation.
3. Transport layer aggregates data from different applications into a single data unit before passing it to _____.
4. The message sent from transport entity to transport entity is called as_____.
5. State true or False

a. RECEIVE primitive waits for a DATA packet to arrive.
b. Each transport service has its own interface.
c. Client issue a SEND primitive When it wants to talk to the server

4.5 Types of service

The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer and the transport layer controls all the lower layers.The services provided by the transport layer protocol are

4.5.1 End-to-end delivery

The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

4.5.2 Addressing

The system can run various programs at the equivalent time. For this reason, the header must contain a type of address known as service point address or port.The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.The transport layer protocols need to know which upper-layer protocols are communicating.The transport layer receives the entire message to restore the process on that computer.

4.5.3 Segmentation and reassembly

The message is split into several packets. Each packet has its sequence number. The transport layer reassembles the message correctly according to the order number and identifies the lost message.

4.5.4 Connection Control

This layer can be connection-oriented or connectionless. The connectionless transport layer treats each packet as independent and produces it to the destination. But, the connection-oriented transport layer first makes the connection and then provides the respective data.

4.5.5 Multiplexing

The transport layer uses the multiplexing to improve transmission efficiency.Multiplexing can occur in two ways.

4.5.5.1 Upward Multiplexing

Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.

4.5.5.2 Downward Multiplexing

Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.

4.5.6 Flow Control

It is also responsible for flow control implemented end to end instead of across an individual link. Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed.

4.5.7 Error Control

The transport layer can support error control. The error control at the transport layer is implemented end to end instead of across an individual link. Error correction is frequently completed by

retransmission. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.

SAQ

1. What do you understand by downward and upward multiplexing?
2. What do you mean by Flow Control in transport layer?

STOP TO CONSIDER

When the size of the data units received from the upper layer istoo long to handle, the transport layer divides it into smaller usable blocks. This dividing process is called segmentation.
When the sizes of the data units belonging to a single sessionare so small that the several data unit can fit together into a single data unit, the transport protocol combines them into a single data unit. This combining process is called concatenation.

4.6 Quality of service

Quality of service (QOS) is the measurement of the overall performance of a service particularly the performance seen by the users of the network. It is particularly important for the transport of traffic with special requirements. For achieving the quality of service, it is indeed imperative to maintain the traffic at different nodes in the network.

4.6.1 Requirements

The QOS parameters can be negotiated during connection establishment. The requirements of each flow can be characterized by some parameter.These parameters jointly determine the QOS that the flow requires.The transport layer quality of service are-

4.6.1.1 Connection Establishment Delay

Source-to-destination delay is a flow characteristic. In this case, telephony, audio conferencing, video conferencing, and remote

login basically need a minimum delay, while delay in file transfer or e-mail is less important.

The time difference mainly between the instant at which a transport connection is requested and the instant at which it is confirmed is called connection establishment delay. The shorter the delay is the better the quality of service (QOS).

4.6.1.2 Connection Establishment Failure Probability

It is the probability that a connection is not established even after the maximum connection establishment delay. This can be due to network congestion, lack of table space, or some other problems.

4.6.1.3 Throughput

It mainly measures the number of bytes of user data transferred per second, measured over some time interval. It is measured separately for each direction.

Different applications need different bandwidths. In video conferencing, we need to send millions of bits per second to refresh a color screen while the total number of bits in an e-mail may not reach even a million.

4.6.1.4 Transit Delay

It is the time between a message being sent by the transport user on the source machine and its being received by the transport user in the destination machine.

4.6.1.5 Residual Error Ratio

It measures the number of lost or distorted messages as a fraction of the total messages sent. Ideally, the value of this ratio should be zero and practically it should be as small as possible.

4.6.1.6 Priority

This parameter provides a way for the user to show that some of its connections are more important (have higher priority) than the other ones. This is important while handling congestion. Because the higher priority connections should get service before the low priority connections.

4.6.1.7 Resilience

Due to internal problems or congestion, the transport layer spontaneously terminates a connection. The resilience parameter gives the probability of such a termination.

4.6.1.8 Reliability

Lack of reliability means losing a packet or acknowledgmentwhich entails retransmission.However, the sensitivity of any application programs to reliability is not the same. For e.g file transfer and email service require reliable service unlike telephone or audio conferencing.

4.6.1.9Jitter

Jitter is the variation in delay for packets associated with the same flow. For applications such as audio and video applications, it does not matter if the packets arrive with a short or long delay as long as the delay is the same for all packets.High jitter means the difference between delays is large, low jitter means the variation is small.

4.6.2Techniques for Achieving Good QOS

Now we will discuss some of the techniques that can play important role to reduce the effect of congestion at any node of a networking device, and thus improving the QoS.

4.6.2.1Over Provisioning

It is aneasy technique. It provides so much router capacity, buffer space and bandwidth that the packets can move through easily.

4.6.2.2 Buffering

The receiving side can buffer the packets before being delivered.Buffering increases the delay and smoothes out the jitter without affecting the reliability or bandwidth.

4.6.2.3 PacketScheduling

Packets from different flows arrive at a switch or router for Processing. A good scheduling technique treats the different flows in a fair andappropriate manner. Some scheduling techniques to improve the quality of service are

1. FIFO Queuing

In FIFO Queuing, packets wait in a Queue until the node is ready to process them. If the average rate is higher than the average processing rate, thequeue will fill up and new packets will be discarded.

2. Priority Queuing

In this queuing, packets are first assigned to **priority class**. Each priority class has itsown Queue. The packets in the highest priority Queue are processed first. But ifthere is a continuous flow in high-priority Queue, the packets in the low priorityQueues will never have a chance to be processes.

3. Weighted Fair Queuing

In this method, the packets are still assigned to different classes and admitted todifferent queues. The queues are weighted based on the priority of the queues. The higher priority means a higher weight.The system processes packets in each queue in a round-robin fashion with thenumber of packets selected from each queue based on the corresponding weight.

For example: If the weights are 3, 2 and 1, three packets are processed from thefirst queue, two from the second queue and one from the third queue.If the system does not impose priority on the classes, all weights can be equal.

4.6.2.4 Leaky Bucket

This technique is used fortraffic shaping to control the amount and the rate of the traffic sent to the network.This is implemented using a buffer at the interface level. If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket.The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty. Buffer stores the data and forwards it in regular 'T' intervals.

The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.

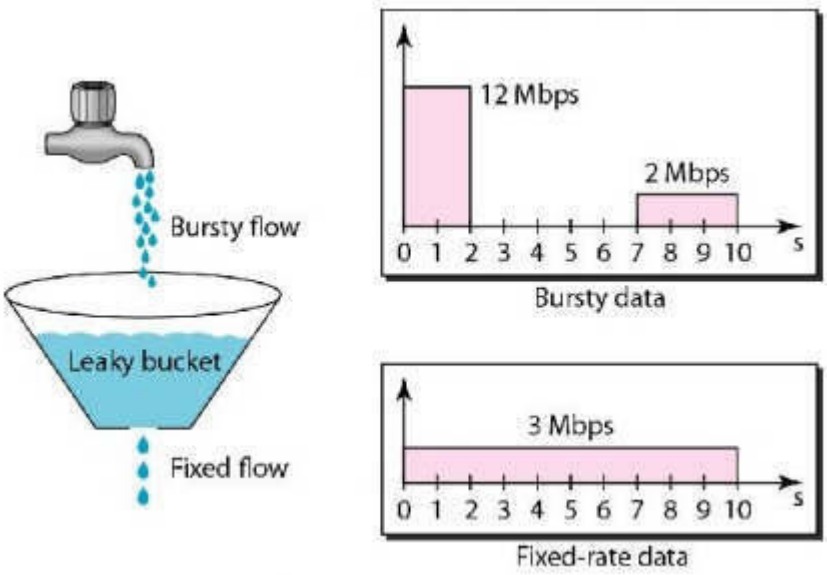


Figure: Leaky Bucket

A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.

4.6.2.5 Token Bucket

The leaky bucket is very restrictive. It does not credit an idle host. The time when the host was idle is not taken into account.

The token bucket is another traffic shaping technique that allows idle hosts to accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) of data sent. For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens.

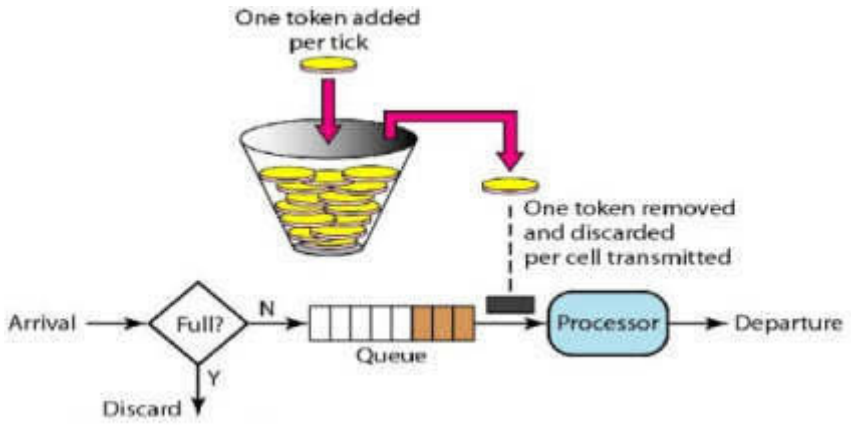


Figure: Token Buchet

The token bucket can easily be implemented with a counter. The token is initialized to zero. Each time a token is added, the counter is incremented by 1. Each time a unit of data is sent, the counter is decremented by 1. When the counter is zero, the host cannot send data.

The token bucket allows burst of traffic at a regulated maximum rate.

4.6.2.6 Resource Reservation in QoS

A flow of data basically needs resources such as a buffer, bandwidth, CPU time, and so on to maintain a steady flow. The quality of service is improved if these resources can be reserved in advance.

4.6.2.7 Admission Control in QoS

It is the mechanism used by a router, or a switch to accept or reject a flow based on predefined parameters called flow specifications. Before a router accepts any flow for processing, it checks the flow specifications to check if its capacity and its previous commitments to other flows can handle the new flow.

CHECK YOUR PROGRESS

6. In transport layer, message is divided into _____.
7. Flow Control use _____ Protocol.
8. _____is the measurement of the overall performance of a service.
9. _____ measures the number of bytes of user data transferred per second.

10. _____ and _____ are used for traffic shaping.

11. State true or false.

    A. The leaky bucket algorithm allows idle host to accumulate credit.
    B. Multiplexing can be only downward in transport layer.
    C. Each packet in transport has it's sequence number.

4.7 Data Transfer

Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link by providing the following methods

- Error control
- Sequence control
- Loss control
- Duplication control

4.7.1 Error Control

When transferring data, the primary goal of reliability is that Data must be delivered to their destination exactly as they originated from the source. The reality of physical data transport are that while 100 percent error free delivery is probably impossible, transport layer protocols aredesigned to come as close as possible.

4.7.2 Sequence Control:

The transport layer is responsible for ensuring that the data received from the upper layers are usable by the lower layers. On the receiving end it is responsible for ensuring that the various sequence of a transmission are correctly reassembled.

4.7.3 Loss Control:

The third aspect of reliability of data transfer covered by the transport layer isloss control. The transport layer ensures that the all segment of thetransmission arrive at the destination. When data havebeen segmented for delivery, some segments may be lost in transmit. Sequence number allows the receiver's transport layer

protocol to identify any missing segment and request for retransmission for the missing segment.

4.7.4 Duplication Controls:

The fourth aspect of reliability of data transfer by the transport layer isduplication control. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers allows the receiver to identify and discard duplicate segments.

4.8 Connection Management

End to end delivery can be accomplished in two ways connection oriented and connectionless. The connection oriented mode is most commonly used from both two modes. A connection oriented protocol establishes a virtual circuited or pathway between the sender and receiver. All of the packets belonging to a message are then sent over this same path.

In both cases, connections have three phases: Connection establishment, Data transfer and Connection termination.

4.8.1 Connection Establishment:

Before communicating device can send data to the other. The initializing device must first determine the availability of the other to exchange data and a pathway must be found through the network by which the data can be sent. This step is called connection establishment.

To establish a connection, one transport entity sends a CONNECTION REQUEST TPDU to the destination and waits for CONNECTION ACCEPTED reply. The problem occurs when the network can lose, store, and duplicate packets.

The existence of delayed duplicates can be attacked in various ways.

The first technique prevents packets from looping. It is difficult because internets may range from a single city to international in scope.

The second method uses the hop count. It is initialized to some appropriate value. The hop count is decremented each time the packet is forwarded. The network protocol simply discards any packet whose hop counter becomes zero.

In the third method, each packet bears the time it was created. The router discards any packet that is older than some given time.

Three-way handshaking used to solve the incorrect connection establishment.

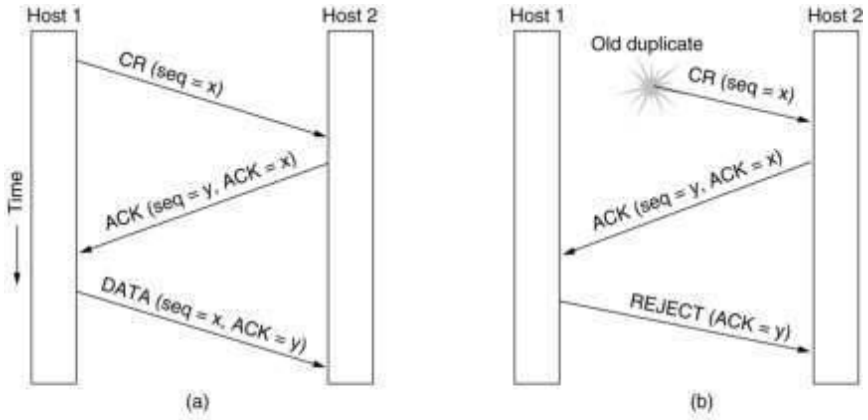


Figure: CR denotes CONNECTION REQUEST (a) Normal operation. (b) Old duplicate CONNECTION REQUEST

In figure (a), the establishment protocol involves one peer checking with the other that the connection request is indeed current. Host 1 selects a sequence number x and sends a CONNECTION REQUEST segment carrying it to host 2. Host 2responds with an ACK segment to acknowledge x and declcares its own initial sequence number is y. Finally, host 1 acknowledges host 2's choice of an initial sequence number in the first data segment that it sends.

In fig (b),the first segment is a delayed duplicate CONNECTION REQUEST from an old connection. This segment arrives at host 2 without host 1's knowledge. Host 2 responds to this segment withan ACK segment . Host 2 asks for confirmation that host 1 was indeed trying to set up a new connection. When host 1 rejects host 2's attempt to establish a connection, host 2 realizes that it was misleaded by a delayed duplicate and leaves the connection. In this way, a delayed duplicate does no damage. The worst case is when both a delayed CONNECTION REQUEST and an ACK are floating around in the subnet.

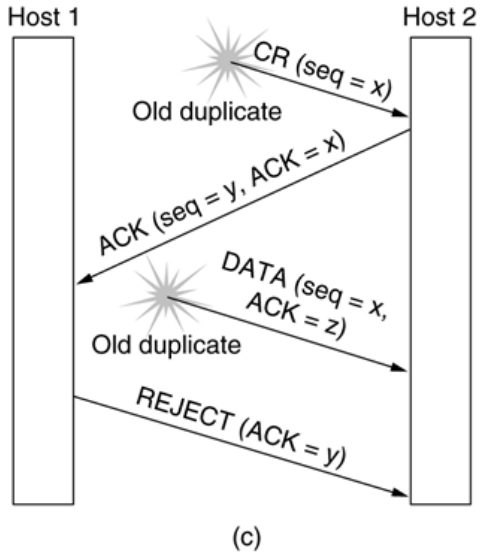


Figure: Duplicate CONNECTION REQUEST and duplicate ACK.

In fig (C), host 2 gets a delayed CONNECTION REQUEST and responds to it. It is crucial to realize at this point that host 2 has proposed using y as the initial sequence number for host 2 to host 1 traffic, knowing that no segments containing sequence number y or acknowledgements to y are still in existence. When the second delayed segment appears at host 2, z has been acknowledged before y tells host 2 that this is an old duplicate. The major thing to notice here is that there is no combination of old segments that can cause the protocol to fail and have a connection set up by accident when no one wants it

4.8.2. Connection Release

A connection is released using either asymmetric or symmetric variant.

Asymmetric release is the way the telephone system works: when one party hangs up, the connection is broken. Symmetric release treats the connection as two separate unidirectional connections and requires each one to be released separately. Data can be lost when connection is released.

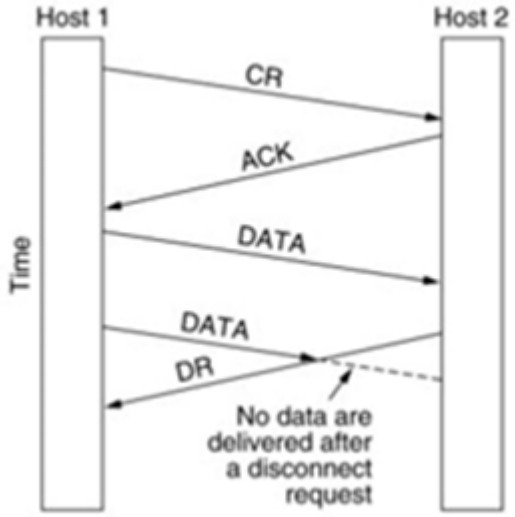


Figure: Disconnection with loss of data

But, the improved protocol for releasing a connection is a 3-way handshake protocol.

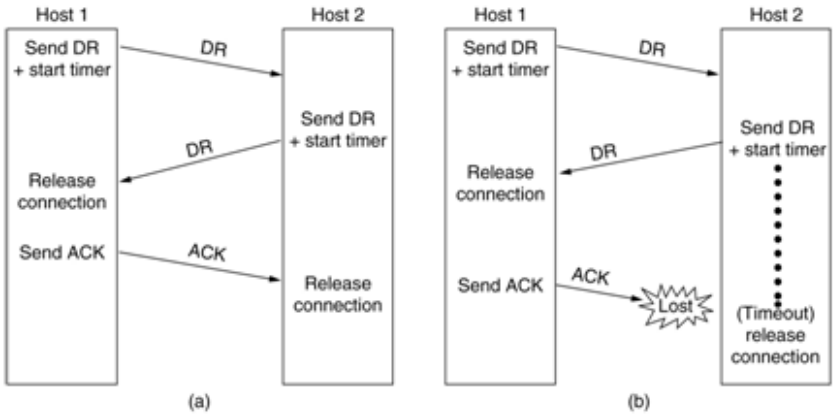


Figure: (a) Normal case of Three-way handshake (b) Final ACK lost

In figure (a), One of the user sends a DISCONNECTION REQUEST TPDU to initiate connection release. When it arrives, the recipient sends back a DR-TPDU and starts a timer. When this DR arrives, the original sender sends back an ACK TPDU to releases the connection. Finally, when the ACK-TPDU arrives, the receiver also releases the connection.
In figure (b), the initial process is same asthe figure-(a). The situation is saved by the time if the final ACK-TPDU is lost. When the timer is expired, the connection is released.

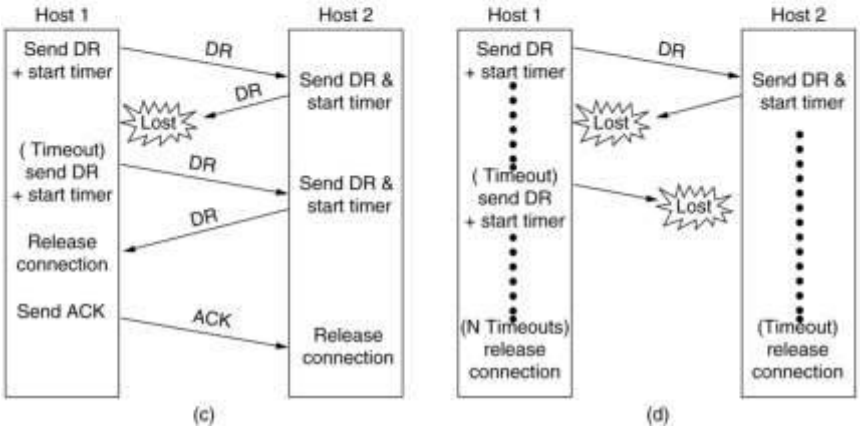


Figure: (c) Response lost. (d) Response lost and subsequent DRs lost.

In figure (c), the user wants to disconnect will not receive the expected response. It will timeout and starts again. In the second time, it assumes that all DR are delivered properly on time.

In fig (d), it is same as figure(c) except all repeated attempts to retransmit the DR is assumed to be failed due to lost TPDUs. After 'N' entries, the sender just gives up and releases the connection.

CHECK YOUR PROGRESS

12. Transport layer provides_____data transfer.
13. _____allows the receivers transport layer to identify any missing segment.
14. A_____protocol establishes a virtual circuit between the sender and receiver.
15. State true or false
    a. Incorrect connection establishment is solved by using hop count.
    b. Connection management has three phases.
    c. The error control at the transport layer is implemented across an individual link.

4.9 Transmission Control Mechanism

Transmission Control Mechanism can be defined as a standard that defines how to establish and maintain a network conversation

through which application programs can exchange data.The type of transport layer protocol an application chooses to use depends on the application requirement.

There are two main protocols in the transport layer, a connectionless protocol and a connection-oriented. The protocols complement each other.

The connectionless protocol is UDP.It sends packets between applications, letting applications build their own protocols on top as needed. It provides no reliability or reordering of the data segment and flow control.

The connection-oriented protocol is TCP. It makes connections and adds reliability with retransmissions, along with flow control and congestion control.

4.9.1 User Datagram Protocol

User Datagram Protocol (UDP) provides connectionless, unreliable, datagram service. Connectionless service means that there is no logical connection between the two ends exchanging messages. Each message is an independent entity encapsulated in a datagram.

UDP does not see any connection between consequent datagram coming from the same source and going to the same destination.

UDP has an advantage: it is message-oriented. It gives boundaries to the messages exchanged. An application program may be designed to use UDP if it is sending small messages and the simplicity and speed is more important for the application than reliability.

Fig : The UDP header

UDP packets, called *user datagram,* have a fixed-size header of 8 bytes made of four fields, each of 2 bytes (16 bits). The 16 bits can define a total length of 0 to 65,535 bytes. However, the total length needs to be less because a UDP user datagram is stored in an IP datagram with the total length of 65,535 bytes. The two

ports serve to identify the end-points within the source and destination machines.
UDP lengthincludes 8-byte header and the data.UDP checksum **i**ncludes the UDP header, the UDP data padded out to an even number of bytes if need be. It can carry the optional checksum.In UDP, a process sends messages with predefined boundaries for delivery. UDP adds its own header to each of these messages and delivers it to IP for transmission.

Each UDP packet is independent from other packets sent by the same application program. UDP does not provide error control. It provides an unreliable service. UDP is suitable for a process with internal flow- and error-control mechanisms.UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software.

4.9.2 TRANSMISSION CONTROL PROTOCOL

Transmission Control Protocol (TCP) is a connection-oriented, reliable protocol. TCP explicitly defines connection establishment, data transfer, and connection teardown phases to provide a connection-oriented service. TCP provides process-to-process communication using port numbers. TCP allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes.
Each machine that supportTCP has a TCP transport entity. This entity accepts user data streams from local processes and breaks them up into pieces not exceeding 64kbytes and sends each piece as a separate IP datagram. When these datagram arrive at a machine, the TCP entity reconstructs the original byte streams. It is up to TCP to time out and retransmits them as needed. It also reassembles datagram into messages.

4.9.2.1 The TCP Service Model

TCP service can be obtained by having both the sender and receiver creating end points. This end point is called **SOCKET.** Each socket has a socket number contain the IP address of the hostand a 16 bit number local to that host, called a **PORT.** A connection must be established between a socket on the source machine and a socket on the destination machine to get a TCP service.

Port numbers below 1024 are called Well- known ports and are reserved for standard services. For example, Port-21 is used to establish a connection to a host to transfer a file using FTP. Port-23 is used to establish a remote login session using TELNET.

TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time.

4.9.2.2 TCP Protocol

The main feature of TCP is that every byte on a TCP connection has its own 32-bit sequence number. The primary protocol used by TCP entities is the sliding window protocol. It starts a timer while a sender transmits a segment. When the destinationreceive the segment, it sends back an another segment containing an acknowledgement number equal to the next sequence number it expects to receive. The sender transmits the segment again if the acknowledgement is received after the sender's timer goes off.

The network layer, as a service provider for TCP, needs to send data in packets, not as a stream of bytes. At the transport layer, TCP groups a number of bytes together into a packet called a segment.

The segments are encapsulated in an IP datagram and transmitted. This entire operation is transparent to the receiving process.

STOP TO CONSIDER

An application establish a connection with another application by binding a socket by a port number.Port number permits unique identification of several simultaneous processes using TCP/UDP. The Ports are used by TCP and UDP to deliver the data to the right application, areidentified by a 16-bit number present in the header of a data packet. The three **types of Port are**

1. Well known port (0 to 1023)
2. Registered Port (1024-49159)
3. Dynamic port (49152-65535)

4.9.2.3 TCP Segment Header

Transmission Control Protocol accepts data from a data stream, segments it into chunks, and adds a TCP header creating a TCP

segment. The TCP segment is then encapsulated into an InternetProtocol (IP) datagram. A TCP segment is the packet of information that TCP uses to exchange data with its peers.The segment consists of a header of 20 to 60 bytes, followed by data from the application program. The header is 20 bytes if there are no options and up to 60 bytes if it contains options.After the options, data bytes may follow. In data bytes, the first 20 refer to the IP header and the second to the TCP header. Segments without any data are legal and are commonly used for acknowledgements and control messages.

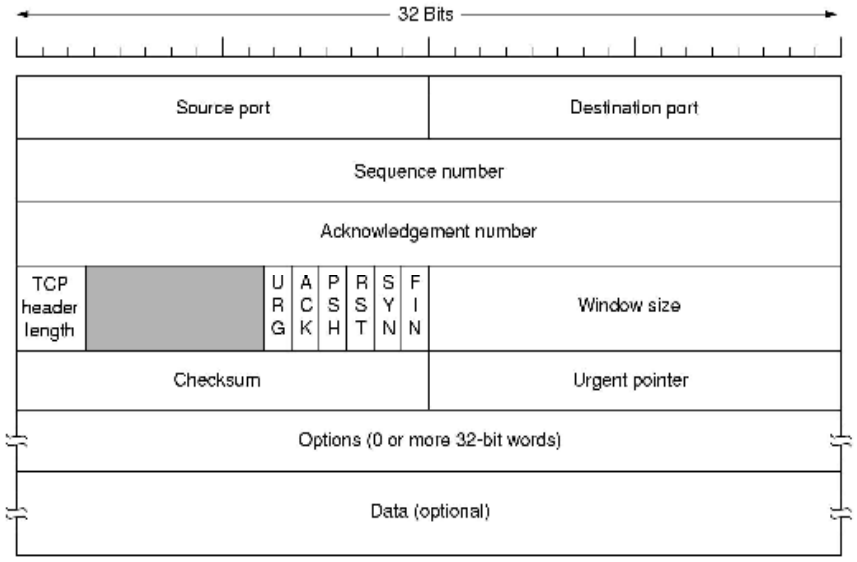


Figure: TCP Header

The Source port is a 16 bit field that that defines the port number of the application program in the host that is sending the segment.
The Destination port address is a 16-bit field that defines the port number of the application program in the host that is receiving the segment. These port address identify the local endpoint of the connection. Each host may decide for itself how to allocate its own ports starting at 1024.
The Sequence and ACK number are 32-bit fieldused to give a sequence number to each and every byte transferred. This has an advantage over giving the sequence numbers to every packet because data of many small packets can be combined into one at the time of retransmission, if needed. The ACK signifies the next byte expected from the source and not the last byte received.

The Header length tells how many 32-bit words are contained in the TCP header. This is needed because the options field is of variable length. The length of the header can be between 20 and 60 bytes.

There are six one-bit flags in the TCP header

1. **URG :**This bit indicates whether the urgent pointer field in this packet is being used.It is set to 1 if URGENT pointer is in use, which indicates start of urgent data.
2. **ACK :**This bit is set to 1 to indicate the ACK number field in this packet is valid.
3. **PSH :**This bit indicates Pushed data. The receiver is requested to deliver the data to the application upon arrival and not buffer it until a full buffer has been received.
4. **RST :**This flag is used to reset a connection that has become confused due to a host crash or some other reason.It is also used to reject an invalid segment or refuse an attempt to open a connection.
5. **SYN :**This bit is used to establish connections. The connection request(1st packet in three-way handshake) has SYN=1 and ACK=0. The connection reply (2nd packet in 3-way handshake) has SYN=1 and ACK=1.
6. **FIN :**This bit is used to release a connection. It specifies that the sender has no more fresh data to transmit. However, it will retransmit any lost or delayed packet.

The Window Size field tells how many bytes may be sent starting at the byte acknowledged. Flow control in TCP is handled using a variable-size sliding window.

A Checksum is provided for extreme reliability. It check sums the header, the data, and the conceptual pseudo header. The pseudo header contains the 32-bit IP address of the source and destination machines, the protocol number for TCP, and the byte count for the TCP segment including the header.

The Urgent Pointer indicates a byte offset from the current sequence number at which urgent data are to be found. Urgent data continues till the end of the segment.

The Optionsfield provides a way to add extra facilities that are not included by the regular header.

The Data field can be of variable size. TCP knows its size by looking at the IP size header.

SAQ

1. Why do you need Port number to make a connection between source and destination machine?
2. What is the importance of Urgent pointer field in TCP header?

4.9.2.4 TCP Connection

To establish a connection, TCP uses a three-way hand shake. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Here BIND primitive is used to attach a local address to a socketand LISTEN primitive is used to announce the server is ready to accept a connection. Once the passive open is established, a client may initiate an active open.

A three-way handshake is established using two flags:
Synchronization (SYN) flag and Acknowledge (ACK) flag

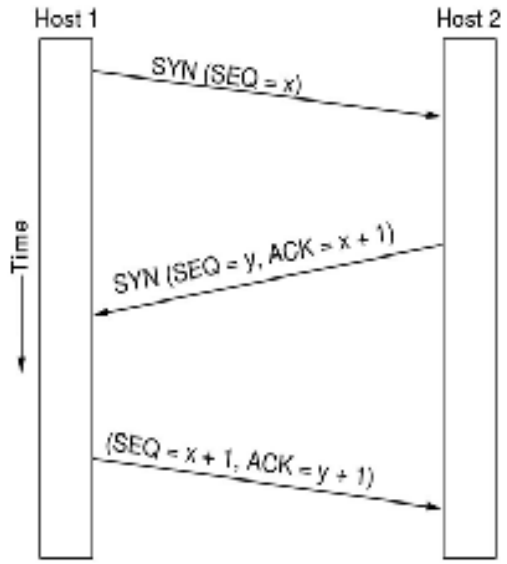


Figure: TCP connection establishment

Step 1 (SYN) : The client sends a segment with SYN (Synchronize Sequence Number) which informs server that client

wants to start communication. The client sets the segment's sequence number to a random value x.

Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set as seq=y, ACK=x+1. ACK signifies the response of segment it received and set to one more than the received sequence number. SYN signifies the sequence number that the serverchooses for the packet.

Step 3 (ACK) : Finally, the client acknowledges the response of server.The sequence number is set to the received acknowledgement value i.e. x + 1 and the acknowledgement number is set to one more than the received sequence number i.e. y + 1. Thenthey both establish a reliable connection with which they will start the actual data transfer.

The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged.Thus, a full-duplex communication is established.

4.9.2.5 TCP Connection Release

You know that the TCP connections are full duplex. But to discuss how connections are released it is best to consider the connection as a pair of simplex connections.

The initiator sends a TCP packet andit'sFIN bit is set. The Fin bit of the packet informs the application program of the responder that it has no more data to transmit. When the responder acknowledges the FIN, the connection is closed from one side.

The responder on receiving this informs the application program that it will receive no more data and sends an acknowledgement of the packet. The connection is now closed from one side. Now the responder will follow similar steps to close the connection from its side. Once this is done the connection will be fully closed.

Generally, to release a connection, four TCP segment one FINand one ACKfor each direction are needed.

4.10 Flow Control

Transport layer flow control uses a sliding window protocol on each connection to keep a fast transmitter from over running a

slow receiver. Sliding window is used to make data transmission more efficient as well as to control the flow of data so that the receiver does not become overwhelmed. The window at the transport layer can vary in size to accommodate buffer occupancy as depicted in figure given below.

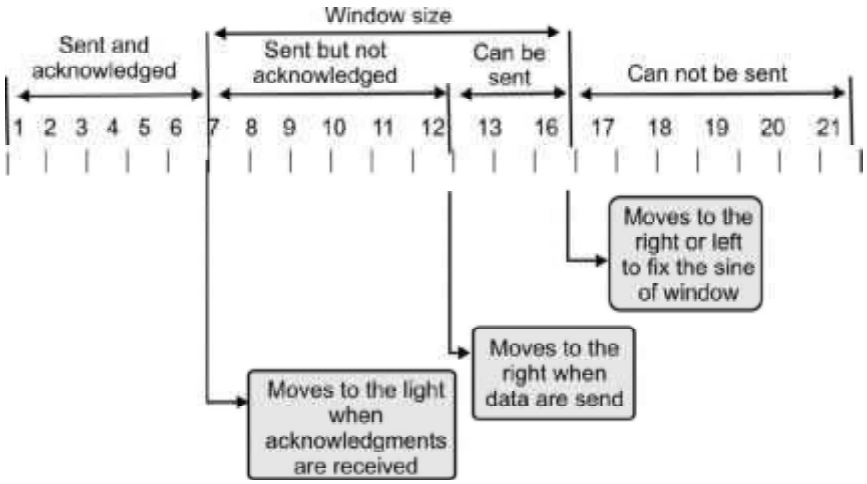


Figure : Sliding Window for Flow Control

The transport entity uses a modified form of sliding window protocol for flow control. Some points about sliding window at the transport layer are as follows:

1. Sender does not have to send a full window's worth of data.
2. An acknowledgement can expand the size of the window based on the sequencenumber of the acknowledged data segment.
3. The size of the window can be increased as decreased by the receiver.
4. The receiver can send acknowledgement at anytime.

Buffering must be done by the sender, if the network service is unreliable. The sender buffers all the TPDUs sent to the receiver. If the sender knows that the receiver always has buffer space, it needs not to keep TPDU's it sends.The buffer size varies for different TPDUs.

They are:

a) Chained Fixed-size Buffers

b) Chained Variable-size Buffers

c) One large Circular Buffer per Connection

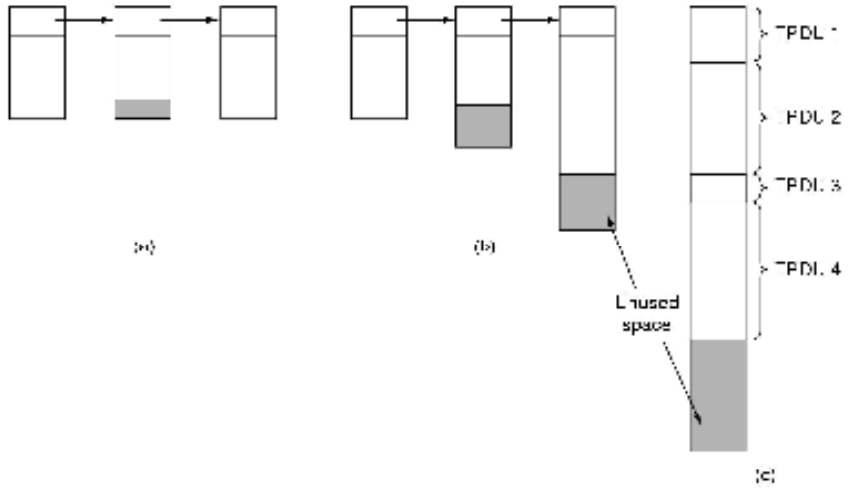


Figure: (a) Chained fixed-size buffers. (b) Chained variable-sized buffers. (c) One large circular buffer per connection.

(a) Chained Fixed-size Buffers:

The buffers can be ordered as a pool of similar size buffers as one TPDU per buffer if the majority of TPDUs are almost of the equal size.

(b). Chained Variable-size Buffers:

If there is broad variation in TPDU size, it leads to the buffer size problem. The buffer space will be wasted on the arrival of a short TPDU if the buffer size is selected equal to the largest possible TPDU.When the buffer size is chosen less than the maximum TPDU size, multiple buffers will be needed for long TPDUs.

So variable-size buffers are used to solve these problem.

(c). One large Circular Buffer per Connection:

When all connections are heavily loaded a single large circular buffer per connection is allocated**.** The type of traffic determines the optimum trade-off between source and destination buffering

1. Source Buffering is used for low band width bursty traffic.

2. Destination Buffering is used for high band width smooth traffic.

3. Dynamic Buffering is used if the traffic pattern changesrandomly.

CHECK YOUR PROGRESS

16. TCP and UDP are called_____protocol.
17. UDP packets are called_____.
18. To achieve reliable transport in TCP, _____is used to check the safe and sound arrival of data.
19. Port number below _____are called well-known port.
20. UDP header is of size_____.
21. State true or false
    a. In TCP header, the source and destination port is of 16 bit field.
    b. ACK flag in TCP header specifies that the sender has no more data to transmit.
    c. In TCP connection, three way hand shake is established using Syn and Ack flag.

4.11 SUMMING UP

- Transport layer is mainly responsible for end to end reliable delivery, segmentationand concatenation. It provides the communication services directly to the application processes running on different hosts.
- The transport layer services are specified by a set of primitives through which user can access those service.
- The Transport Protocol Data Unit (TPDU) is used for messages sent from transport entity to transport entity.
- The data link layer and the transport layer perform many same duties. The data link layer works on a single network while the transport layer operates across an internet. Transport layer works on port address.
- Multiplexing can be downward or upward in transport layer.
- Flow control at the transport layer is handled by the Sliding Window to prevent the sender from overwhelming the receiver.
- The connectionless transport layer treats each packet as independent and delivers it to the destination.
- The connection-oriented transport layer first makes connection then send the data.
- Quality of service can be determined mainly from reliability, delay, Jitter and bandwidth.

- Transport layer provides reliable data transfer by error control, sequence control, loss control and duplication control.
- Connection establishment can be done by using three way handshakes to handle the delayed duplicate.
- Transport layer has two main protocols UDP and TCP. UDP is a connectionless protocol which provides unreliable datagram service. TCP is a connection-oriented protocol which provides a reliable end-to-end byte stream over an unreliable internetwork.

4.12 ANSWERS TO CHECK YOUR PROGRESS

1. 4

2. Transport Layer

3. Network Layer

4. Transport protocol Data Unit (TPDU)

5. a. True b. True c. False

6. Segment

7. Sliding Window Protocol

8. QOS

9. Throughput

10. Leaky Bucket and Token Bucket

11. a. False b. False c. True

12. Reliable

13. Sequence Number

14. Connection-Oriented

15. a. False b. True c. False

16. Transport

17. Datagram

18. Acknowledgment

19.1024

20. 8 byte

21. a. True b. False c. True

4.13POSSIBLE QUESTIONS

Short answer type questions:

1. What are the main services that the transport layer provides to it's upper layer?
2. What is Addressing?
3. What is Connection Establishment Delay?
4. What is meant by QOS?
5. What do you mean by packet scheduling?
6. What is Leaky Bucket algorithm?
7. Define sequence control.
8. Define the transport layer connection establishment.
9. What is Transmission control protocol (TCP)?
10. What do you mean by UDP?
11. Define TCP service model.
12. Define flow control.
13. What do you mean by checksum field present in TCP header?

Long answer type questions:

1. How can the transport layer service be accessed by user. Explain the transport service primitives.
2. Explain the types of service provided by the transport layer.
3. What is Multiplexing? Explain
4. Explain briefly the main requirements of QOS.
5. Explainone technique that is used to control traffic sent to a network.
6. How does the transport layer control the reliability of data transfer? Explain.
7. Explain briefly the transport layer connection establishment with three way handshaking.

8. Explain UDP.
9. Explain TCP Segment Header briefly.
10. How can TCP connection be established using SYN and ACK flag.
11. Explain the different flags present in TCP header.
12. Explain the importance of buffering in flow control.

4.14 FURTHER READINGS

1. Tanenbaum, Andrew S. Computer Network. Pearson.
2. James, F. Kurose, Keith, W. Ross. Computer Networking. A Top-Down Approach. Pearson.
3.http://www.vbspu.ac.in/wp-content/uploads/2020/05/CN-Notes.pdf

UNIT 6 : APPLICATION LAYER

CONTENTS

6.1 Introduction

In networking the standard models:TCP/IP and OSI both use the same term for their respective highest – level layer i.e. Application Layer. The Application Layer provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, surfing the World Wide Web, network management and other types of distributed information services. It is the layer that the users interact with.

> The Application Layer is responsible for providing different web services to the user.

6.2 Objectives

This unit basically includes some Application Layer's applications and protocols. In this unit you will be able to learn:

- ✓ SNMP its components and versions.
- ✓ WWW and HTTP protocol
- ✓ FTP protocol
- ✓ DNS and the role of name servers
- ✓ NFS and RPC
- ✓ E-Mail and its components.

6.3 SNMP(Simple Network Management Protocol) :

6.3.1 Introduction

The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCPI/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet. In SNMP uses the concept of managers and agents. That is, a manager, usually a host, controls and monitors a set of agents, usually routers. SNMP uses port number 161/162 to monitor the network, keep tract of the changes to the network, determine the status of network devices in real time, detect network faults and sometimes used to configure remote devices. SNMP uses UDP as the transport protocol for passing for data between managers and agents.

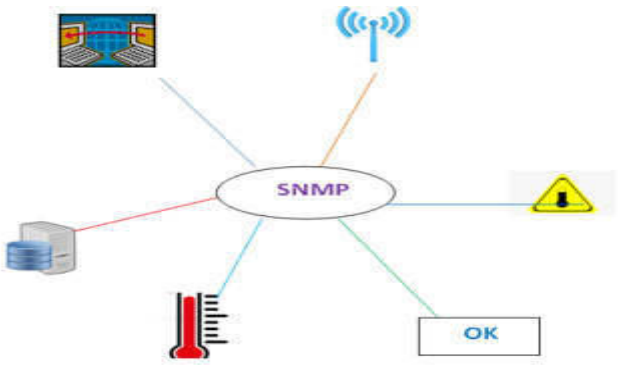


Fig:6.1 Simple Network Management Protocol (SNMP)

STOP TO CONSIDER

SNMP is a framework for managing devices in an internet using the TCP/IP protocol suite. SNMP uses port number 161/162 to monitor the network, keep tract of the changes to the network, determine the status of network devices in real time, detect network faults and sometimes used to configure remote devices.

6.3.2 What are Managers and Agents?

In SNMP concept of the manager and the agent are very important. A manager is a host that runs the SNMP client program. Again ,agent is a router that runs the SNMP server program. When there is a simple interaction between a manager and a agent ,management of the internet is achieved. Both manager and agent perform different task. Normally agent is used to keep the information in a database where the manager is used to access the values in the database. Interaction between agent and manager can be discussed considering simple example ,suppose a router can store the appropriate variable such as number the packets received and forwarded while the manager can compare those stored variables to determine whether the router is congested or not.

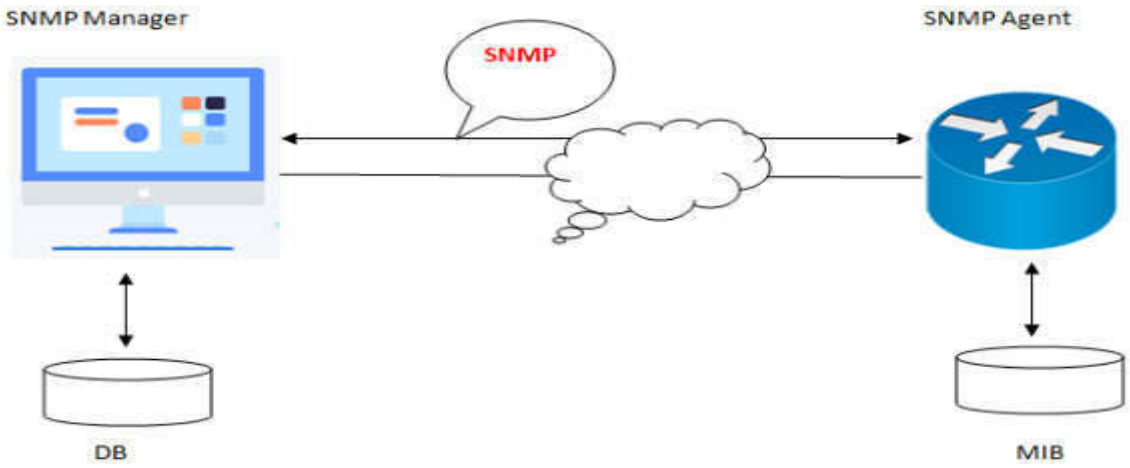


Fig 6.2: SNMP Manager/Agent

Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong , the agent sends a warning message to the manager. Details about MIB will be discuss in the Network Management chapter.(Chapter-7)

Check your progress
Q1.SNMP uses TCP.(True/False)
Q2.Define Manager and Agent concept used in SNMP?

6.4.The World Wide Web(WWW):

6.4.1 Introduction:

The World Wide Web(W3) or the Web is an architectural framework for accessing linked content spread over millions of machines all over the Internet or it is the repository of information linked together from points all over the world. In the web HTTP (Hypertext Transfer Protocol) is used to connecting all resources and user .The basic features of the web includes flexibility, portability and user friendly. WWW was started with the basic idea to merge the evolving technologies of computers, networks and hypertext into a powerful and easy to use global information system. The WWW concept was first introduce by Tim Berners Lee ,a CERN scientist in 1989.

Fig:6.3 Tim Berners Lee

6.4.2 Architecture:

As shown in figure- 6.4 a client is associated with many sites .Again each site holds one or more web documents, which are referred to as Web pages. Each Web page can contain a links to other pages in the same site or at other sites anywhere in the world. The users can retrieved and viewed these web pages by using browsers. The figure 4 shows that if client needs to see some information that it knows belongs to site A. Then client sends a request through its browser, using a program that is designed to fetch Web documents. In that client request , among other information, it includes the address of the sites and the Web pages, which is called as the URL, At site A ,the server finds the required web document and sends it to the intended client. When the user receive the document and view it , it finds some references to other web documents which located a at site B. The reference has the URL for the new site B. If the user is also interested in viewing this document. Then the client sends another request to the new site B, and the new page is retrieved from that site.

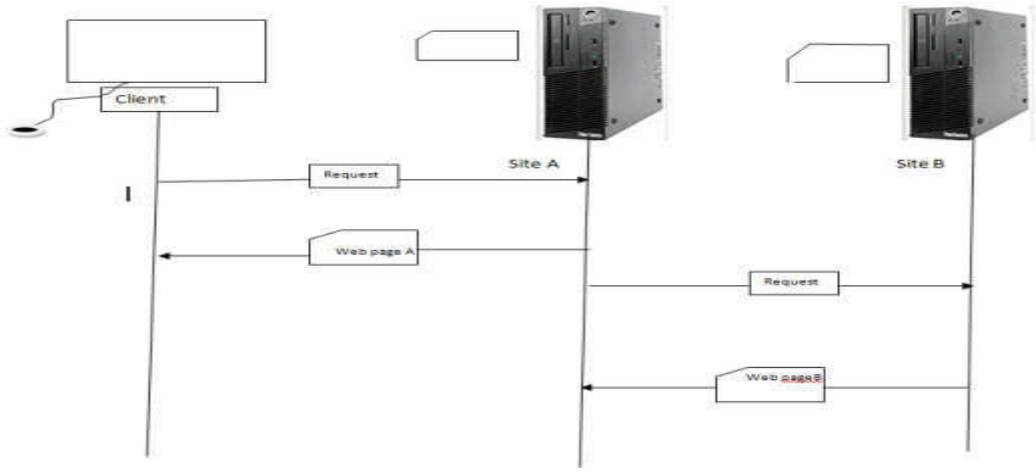


Fig 6.4: Architecture of WWW

Client(Web Browser):

The web browser or the browser is an application software used to interact the user with the content and data on the web. When any user send request for some content, the browser fetches the particular content from a web server and then only display the content based webpage on the user screen. In 1990 Tim Berners Lee first ever introduce browser known as WorldWideWeb(no space).Later on ,Firefox, Internet Explorer, Google Chrome, etc are the commonly used web browsers across the globe. Each browser consists of different parts. A web browser normally consists three parts:

i. A controller

ii. Client protocol and

iii. Interpreter

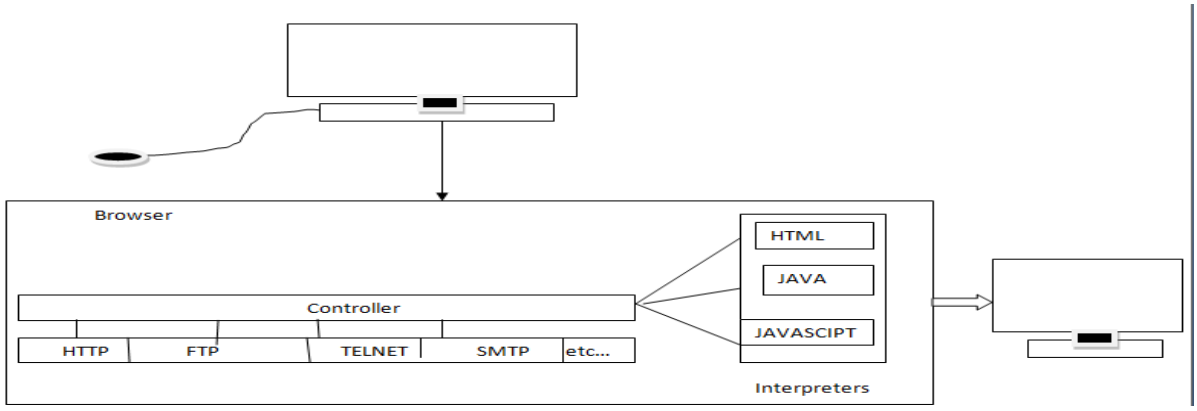


Fig 6.5.Browser

A controller receives input from input devices such as mouse or keyboard and uses the client programs to access the document from the web. When the document has been accessed, the controller uses any interpreters to display the required document on the user's screen. The client can use protocol such as FTP or HTTP. Depending on the type of the document interpreter can be HTML, JavaScript or Java.

Server:

Web server is the part of Internet where all web pages are stored. When a client send a request for a particular document to the server on arriving the request corresponding document is sent to the client from the server. To improve efficiency, web servers normally store requested files in a cache in memory; where memory is faster to access than disk. Multithreading and multiprocessing also used to improve the efficiency of the server ,in that case a server can answer more than one client request at same time.

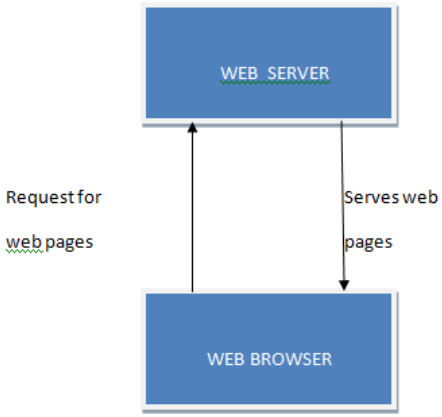


Fig 6.6.Web server

Uniform Resource Locator (URL):

URL is known as web address, is a unique identifier used to locate a resource on the internet composed of multiple parts. In 1994 ,URL was first introduced as a part of the Uniform Resource Identifier(URI).URLs are the subset of URIs and are used to address the electronic resources. The syntax of URL is similar to mail address, which contain several fields.

The URL syntax:

The following syntax is used in URL

scheme: / /host:port/path?query-string#fragment-id

A URL consists of some of the following:

i. Scheme name:-It identifies the protocol to be used to access the e-resource on the web. The scheme names followed by a colon and two slashes (: / /).Commonly used protocols are http: / / ,https :/ /,ftp : / / etc.

ii. Host name: It identifies the host where resource is located .Normally a host name is a name of the domain.

iii. Port Number: Port no. tell the server what service is being requested as servers often deliver more than one type of service.For example HTTP runs by default port 80.

iv. Path: It defines the specific resource within the host that the user wants to access..

v. Query String:It contains data to be passed to server-side scripts,running on the web server.The quesry string proceded by a question mark (?),is a string of name and value pairs separated by ampersand(&).

vi. Fragment identifier: The fragment identifier introduced by a hash character(#) is the optional last part of a URL for a document. The fragment identifier, if present specifies a location within the page, browser may scroll to display that part of the page.

STOP TO CONSIDER

Tim Berners Lee proposed the concept of WWW in 1989. The basic features of the web includes flexibility, portability and user friendly. The first web browser was WorldwideWeb don't confused with World Wide Web introduced by Tim Berners Lee. URL is known as web address, is a unique identifier used to locate a resource on the internet composed of multiple parts

Cookies:

Cookies are alphanumeric values stored at the client by the browser. In web browser store relevant data of previous search (connection) as cookies to facilitate quick access when the user tries to establish the same search (connection) again. Now a days in e-commerce, looking at customer's interest, the website can construct personal profiles for all users and can give personal look to its home page when a specific user accesses the previously searched website. The following figure can shows role cookies.

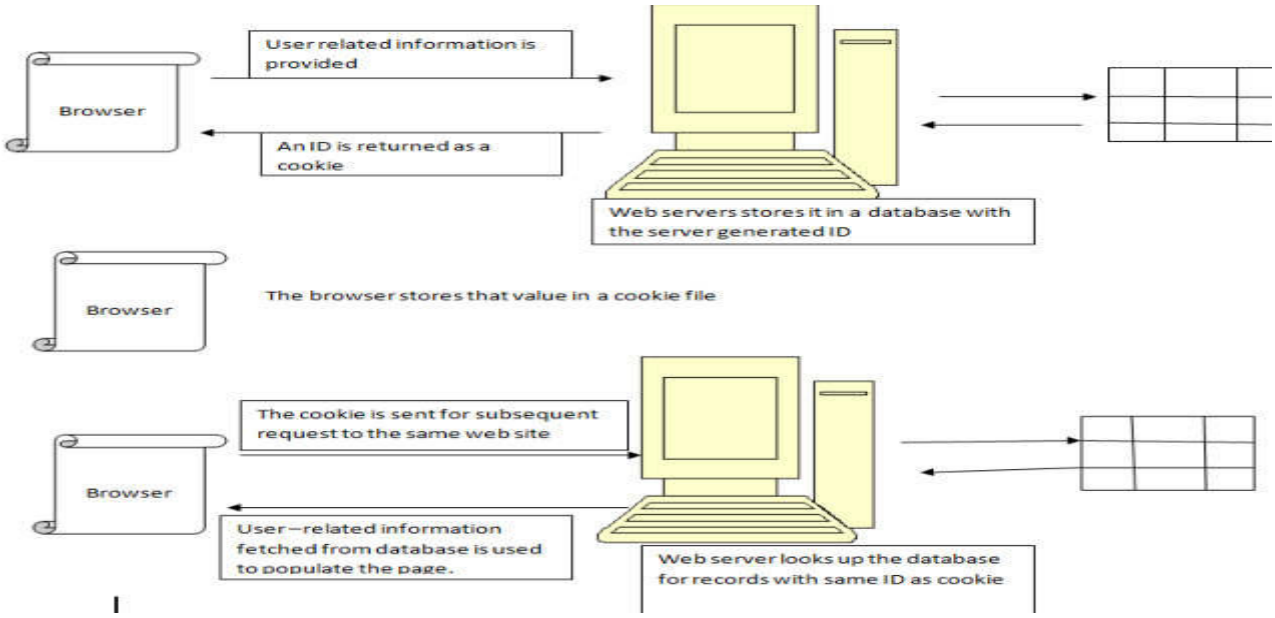


Fig6.7: The role of cookies

Cookies have some disadvantages also from the view of security, any intruder can easily open these files and can view information and also all sites that collect information from cookies are legitimate as some of them may be malicious and can be used for the purpose of hacking. Again cookies can store only few kb of information ,most are upto only 4kb.Browser assign some restriction on cookies also for example except internet explorer, the browsers allow only upto 20 cookie for a single website.

Cookies are alphanumeric values stored at the client by the browser

Check Your Progress

Q3.Define URL?

Q4. WorldWideWeb is first web browser.(True/False.)

Q5. State basic features of WWW.

Q6.What is cookies?

6.4.3 Web documents:

Web documents can be boadly classified into the categories:

- Static
- Dynamic and
- Active

Static web page:

The content of static page cannot changed by client, the client can get only a copy of the document. When the file is created the contents are determined i.e static documents are fixed –content documents that are created and stored in a web server. Of course, the content in the web server can be changed, but client cannot change .When a client accesses the document, a copy of the document is sent .The client the can use a browsing program to display the document.

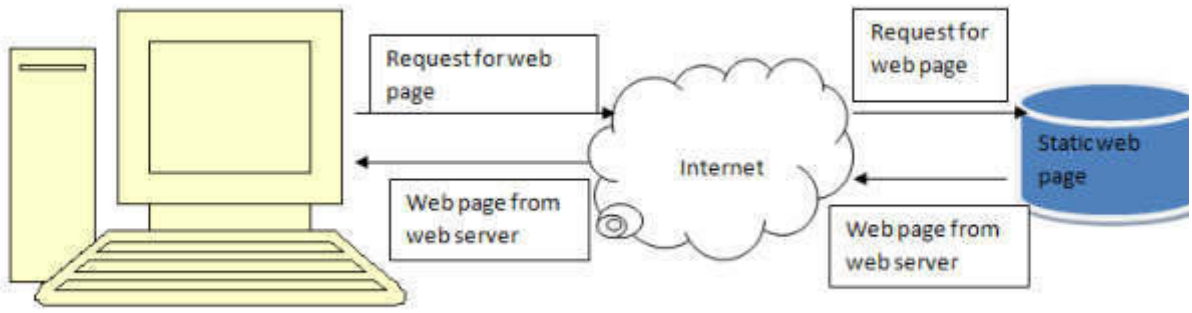


Fig6.8: Static HTML page

HTML:

Hypertext Markup Language (HTML) is use to create web pages.HTML can describes the structure of the web pages. While developing a web page with HTML, it consist series of elements. And these elements tells the web browser how to display the content of the web page. A markup language allows developer to embed formatting instructions in the file itself. The required instructions are included with the text. And in this way, any browser can read the instructions and format the text according to the specific workstations.

Only ASCII characters for both the main text and formatting instructions are use in HTML. Every computer receive the whole web document as an ASCII document. While HTML is used to develop web pages it consists of two parts:

- The head and
- The body

The first section of web page is head where head contains the title of the web page and other parameters also that the browser will use . The contents of a web page are lies in the body section, which includes text and the required tags. In HTML the tag define the actual appearance of the web documents such as color, heading size and other effects also. The <html>….</html> is the root element of the HTML based web page. An HTML element follow the following syntax :

<tag name> content are write here </tag name>

In HTML tags are not case sensitive i.e upper or lower case is accepted .An attribute if present in document is followed by an equal sign(=) and the value of the attribute. The browser takes the decision about the structure of the text based on the tags ,which are embedded into the text.

Dynamic web page:

A dynamic web page can display different content and has user interaction by making use of advanced programming (Scripting languages, Ajax technology) and databases in addition to HTML.

In dynamic web pages scripting languages are used with HTML.Scripting languages are written for a run time environment. In scripting languages step by step compilation is not required rather they are interpreted. In dynamic web pages server side and client side dynamic pages are available. The server side scripting usually use in back-end of websites and user does not get access to view .In server side scripting all responses can be customized only based on the user requirements. Commonly in server side PHP, ASP, ASP.NET, Perl, J2EE, Python, Ruby are used in back end. Again client side script is executed in client's side also called front end. Client side scripting are normally used for page navigation, formatting and data validation etc i. e it is used to make web pages interactive. Scripts are used to create cookies .Client side generally used CSS, HTML, JavaScript, Adobe Flex etc languages.

Active documents:

In client server architecture for many applications sometimes a program or a script to be run at the client site. These types of document are called active documents. Generally an active document consists of a program that the server sends to the browser and the browser must run that locally. When it run locally, the program within active document can interact with the user and change the display continuously. Active documents can be explained with the help of an example, say user want to run a program that creates animated graphics or multimedia on the screen or a program that interact with the user, then the program surely runs at the client site where the animation or interaction takes place. In that case when the browser request an active document, the server send a copy of the active document or a script and the document is run at the browser.

STOP TO CONSIDER

Web documents have three categories: static, dynamic and active document. Scripts are used to create cookies .Client side generally used CSS, HTML, JavaScript, Adobe

Check Your Progress

Q7.What do you mean by static web page?

Q8. HTML tags are case sensitive.(True/False)

Q9.What is markup language?

Q10.What are the basic sections of HTML

6.5 Hyper Text Transfer Protocol (HTTP):

HTTP is an application layer protocol used basically to access data on the World Wide Web. HTTP is a request –response protocol. It uses the services of TCP. It provides an interface to the user to transfer resources in terms of request –response message using TCP protocol. In HTTP before transferring original message using TCP protocol a connection is established between the client and the server. It is somehow similar to FTP as it also transfer files but simpler because HTTP uses only one TCP connection. In HTTP there is no separate connection for control operation, only data are transferred between the client and the server. Well-known port 80 is used by HTTP.HTTP uses the services of TCP but itself a stateless protocol.

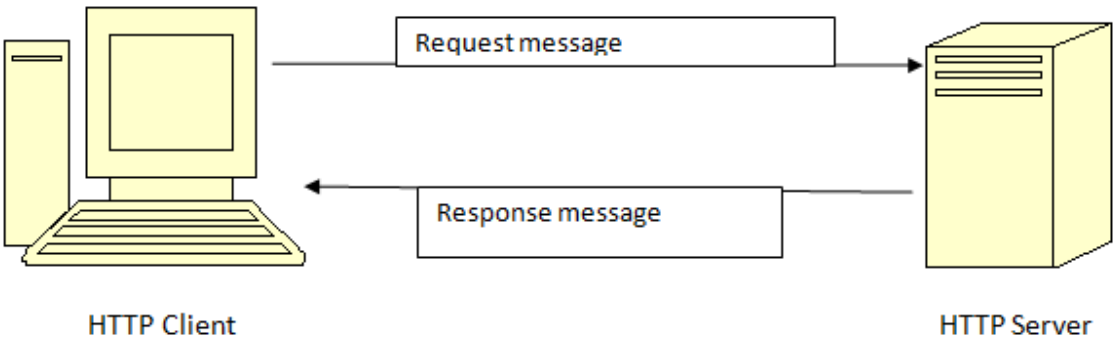


Fig 6.9 : HTTP request and response

When a HTTP server find some request from client side it accept it and then HTTP client sends a request for resource to the server. On receiving the request from the client, the server processes the request, perform the desired task and send response back to the client. After that HTTP server closes the

TCP connection and the HTTP client receives the responses from the server containing the desired information and processed it.

6.5.1 Request :

A request is send by a client to the web server. It consists of several parts:

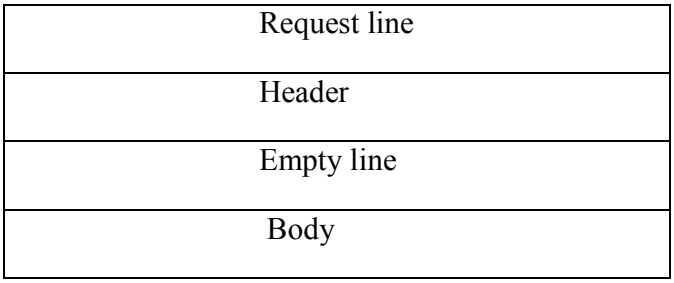
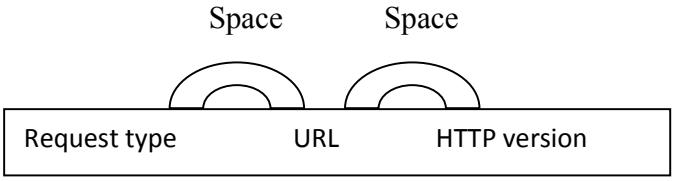


Fig6.10: HTTP request message format

6.5.1.1 Request line in HTTP

In HTTP a request line consist of the three sections: request type, URL and HTTP versions again between two sections spaces are there.



URL: The URL part is discussed in the earlier section.

6.5.1.2 Request method:

It indicates the type of the request, a client wants to send. They are called methods. A method makes a message either a request or a command too the server. Request and command both are different in that sense that request messages are used to retrieve data from the server and a command message tells the server to do the specific task. Commonly used some of the methods are as follows:

GET: Most widely used method in WWW is GET. Using this method a client can retrieve a resource from the server.

PUT: This method is used to upload a new resource or replace an existing document in the web.

HEAD : This method is used when the client wants to know the header information about a resource but not the resource content. Here address of the document is defined by the URL.

COPY: The method COPY is used to copy a file from a location to another location.

DELETE: This method is used to delete a web document from the server.

TRACE: The TRACE method is used to instruct the web server to echo the request back to the client i.e it is used as loop-back.

6.5.2 Response or status:

Responses are sending by the server to the client. A response consists of the following parts.

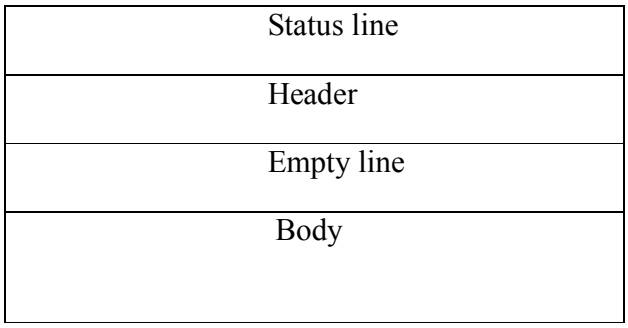


Fig 6.11:HTTP response format

Status line containg HTTP vesrsion,status code and status phrase.

Version: Current version of HTTP is 1.1.

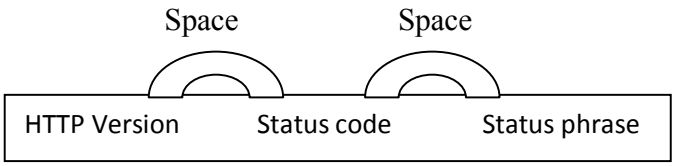


Fig6.12: HTTP response line

6.5.2.1Status code

In HTTP it use a three digit code which indicates the responses or status. The status code has five categories depending on their functionalities. The categories can be discussed as follows:

- 1xx series:- This category of status code represent provisional responses.
- 2xx:- This category of status code represents that the client's request are accepted successfully.
- 3xx:- This category of status code represents that some additional actions must be taken by client to complete the request.
- 4xx:- This category of status code represents that client request had some error and so it cannot be fulfilled.
- 5xx:- This category of status code represents server error i.e the server encountered some error and hence the request cannot be completed at this time.

Table6.1 HTTP status code

Status code	Status phrase	Description
1xx category-informational		
100	continue	The initial part of the request has been received by the server, and the client may proceed further.
101	Switching	The server switches the protocol while receiving a request from the client to do the same.
2xx category-Success		
200	OK	The request is successful
201	Created	A new URL is created.
202	Accepted	The request is accepted, but it is not immediately acted upon.
204	No content	There is no content in the body.
3xx category-Redirection		

301	Moved permanently	The resource resource is no longer used by the server
302	Moved temporarily	The requested URL has moved temporarily
303	See other	The method may be wrong.
4xx category-Client Error		
400	Bad request	There is a syntax error in the request.
401	Unauthorized	The request lacks proper authorization
403	Forbidden	Service is denied.
404	Not found	The document is not found.
5xx category-Server Error		
500	Internal server error	Indicates a error message,server face some problem.
501	Not implemented	Unable to fulfill the request.
503	Service unavailable	The service is temporarily unavailable, due to maintenance or other issue may be arise .

6.5.2.2 Header

Header are very important part in HTTP. In both request message and in response message header are important. The header shares additional information between the client and the server of a particular request. For example, a client may want to accept video in a special format, that time the server can send extra information about the video. Generally a header can consists of one or more header lines. A header line contains a header name, a space and a header value.

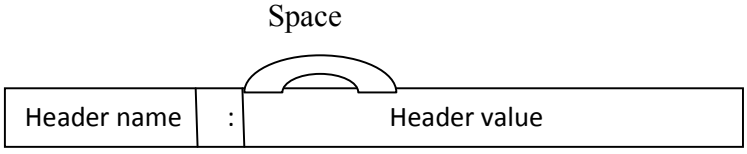


Fig6.13: HTTP Header Format

A header name is not case sensitive; but the header value may be case sensitive.

HTTP Header line belongs to one of four categories:

- General header
- Request header
- Response header and
- Entity header.

General header:

In HTTP some general header are present in both request message and response message but with different meaning.

Table 6.2 HTTP General header

Header	Description
Cache-control	Specifies information about caching, whether caching should be used or not.
Connection	Shows and specifies whether the connection should be closed or not
Date	Shows the current date and time

Request header:

As the name suggest the request header is present only in the request message. Request header specifies the client's information such as client's configuration and the client's preferred document format etc.

Table6.3 HTTP request header

Header	Description
Accept	It Shows the format of the medium the client can accept.
From	Shows the e-mail address of the user.
User-agent	Identifies the client program.

Response header:

As request header is present only in request message similarly response header is present only in the response message. So it contains the data about the web server and the data that are being sent.

Table6.4 HTTP response header

Header	Description
Accept-rang	Shows the partial range type the server support.
Age	Shows the age of the document
Server	Shows the information of the server such as server name and version number.

Entity header:

Entity header also present in both request message and response message and it contains the information about the body of the document.

Table 6.5 HTTP Entity header

Header	Description
Allow	Lists of valid methods that can be used on a URL.
Content-language	Specifies the language of the content.
Etag	An identifier for entity tag.

6.5.2.3 Body :

The body is present in a request or response message. Usually, it contains the document to be sent or received by the user.

6.5.3. Persistent Versus Nonpersistent Connection

The persistent connection is the default version 1.1.Again HTTP prior version of 1.1 is specified as nonpersistent connection.

Persistent Connection

As mention earlier HTTP version 1.1 specifies a persistent connection by default.After sending a response in persistent connection the server leaves the connection open for more requests .The server also can close the opened connection at the request of a client if a time out has been reached.

Nonpersistent Connection:

In nonpersistent connection after sending a response the connection does not exist i.e here in nonpersistent connection, one TCP connection is made for each request/response.

6.5.4 Proxy Server

A proxy is an application program or a computer system that behaves like an intermediary between the clients looking for services and servers. HTTP protocol support proxy server. It keeps copies of responses to recent requests .In HTTP, the HTTP client sends a request to the proxy server on receiving the request the proxy checks it in the cache. If the responses are available it response otherwise the proxy server sends the request to the corresponding server. In that case incoming responses are sent to the proxy server and stored for future request from other clients. With the use of proxy server the load of the original server can be reduced which can decrease traffic and improves latency. To use proxy in client's machine, the client must be configured to access the proxy instead of the original server.

STOP TO CONSIDER

Well-known port 80 is used by HTTP.HTTP uses the services of TCP but itself a stateless protocol.In HTTP request is send by the client to the server using different method like GET,PUT,HEAD,COPY etc. Responses are send by the server to the client. Current version of HTTP IS 1.1. HTTP Version 1.1 specifies a persistent connection.

Check your progress

Q11.HTTP status 200 code defines "OK"? (True/False)

Q12.HTTP used welknown port---------- (Fill in the blank)

Q13.Why proxy server is used?

6.6 File Transfer Protocol (FTP)

FTP is an application layer standard protocol for transferring files from a server to a client or from a host to another. During transfer of file from one system to another there may be several issues say, two systems may use different ways to represent text and data or may use different file name conventions. Sometimes two systems may have different directory structures ,so all these types of problems during file transfer have been solved by FTP .FTP also follow client/server but it somehow different from other client/server application as in FTP it establishes two connections between the connecting systems. One connection is for data transfer and the other one for the control information as shown in fig.6.11 .Due to this separation of connection FTP services are considered as more efficient.

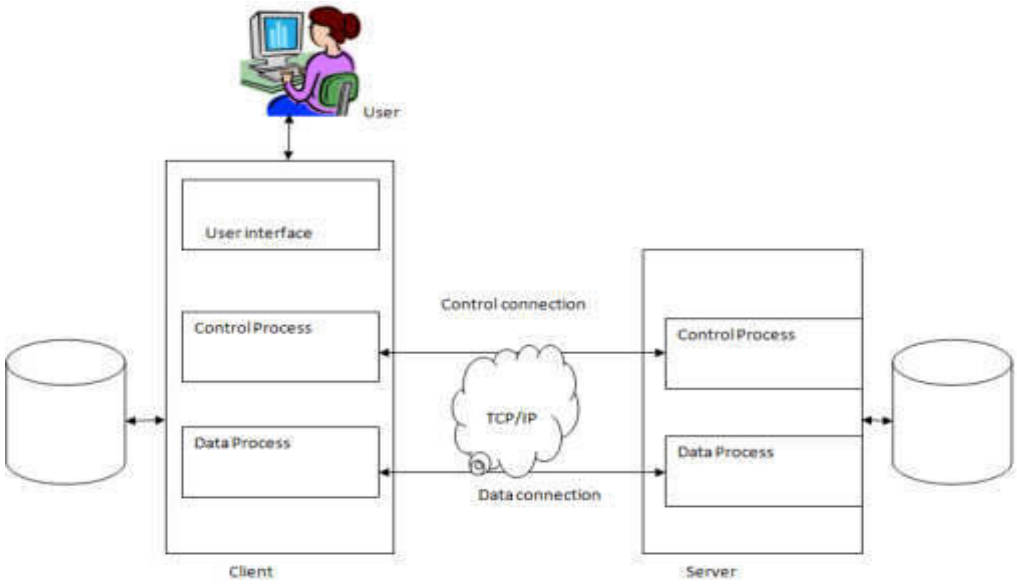


Fig6.11 :FTP connections

Compare to control connection, data connection is more complex as variety of data types need to be transferred.FTP uses all the services of TCP and it needs two TCP connections .For control connection FTP use the well known port 21 and for data connection it use port 20.

In FTP data connection is opens each time commands that involves transferring of files and after transfer it closes. But the control connection remains connected during the entire interactive FTP session. In FTP while control connection is opened, the data connection can be opened or may be closed several times if multiple files are transferred. Like SMTP, FTP also use the same approach to communicate across the control connection i.e it uses the 7-bit ASCII character set. Communication between systems achieved through command and responses.

In data connection the client must several information such as it has to define the types of the transfeered file, the structure of the data and the mode of transmission. Again before data connection preparation should be done through control connection.

6.6.1.File Type:

Across data connection FTP can transfer one of the following type of file:an EBCDIC file, image file or an ASCII file. The default format for transferring text file is ASCII. In ASCII each character is encoded into 7 –bit ASCII form. In both side i. e in the sender transform the original file representation is converted into ASCII character and in the receiver side ,the receiver transform ASCII characters into its original representation. But if one or both systems of the connection use EBCDIC encoding format then the file can be transferred using EBCDIC encoding. Again ,for binary files image file is the default format. In that case the file is sent as a stream of binary bits without any interpretation or encoding.

6.6.2Data Structure

In FTP three types of interpretations about the structure of the data is used:

- File structure,
- Record structure, and
- Page structure.

In different format , the files are transferred in different format. In the file structure format, the file is a continuous stream of bytes. The record structure can be used only with test files and the file is divided into records. In the page structure format , the file is divided into pages. The divided pages can be stored and accessed randomly or sequentially.

6.6.3 Transmission Mode

In FTP three transmission modes are used to transfer files: stream mode, block mode, and compressed mode. The default mode is stream mode. In this mode Data are delivered from FTP to TCP as a continuous stream of bytes. TCP is responsible for dividing data into segments of appropriate size. In block mode, data can be delivered from FTP to TCP in blocks. Again in the compressed mode, if the file is big, the data can be compressed. The compression method normally used is run-length encoding.

Point to be remember that to use FTP a used must needs an user account and a password on the remote server .But some sites have a set of files available for public access, to enable anonymous FTP. For access any files in those sites user password and account may not be required. Instead, the user can use anonymous as the user name and guest as the password but user access to the system is very limited.

STOP TO CONSIDER

FTP is an application layer protocol used to transfer files .It has two connection ,one for control connection and one for data connection.Port-20 used for data connection and port 21 used for control connection. In FTP default mode of data transfer is stream mode. Moreover, it has block and compressed mode.

SAQ

Q1.Write down the purpose of using FTP protocol.

Q2.Discuss the different connectionS available in FTP.

6.7 Domain Name Service (DNS)

In application layer, there are various protocols right, like some related to file transfer, email, remote login, network management and there is a name management or name resolution for name resolution which is DNS. In the application layer several applications are used that follow the client / server model. It is a sort of a global data base for internet addressing, mail and other information. So, why suddenly we require this? Now you see, whenever you want to communicate one packet or one data packet from one to another, what we require? We require primarily the IP address of the destination. So, specially when internetworking is done, the IP address of the destination is required. Now, remembering IP address is the tedious job right. If anyone want to say if you want to open gauuni "www gauuni ac dot in" and instead of this if someone say that you remember the IP address of "gauuni" at 199 dot 17 dot so and so forth it is very tedious difficult to remember. So, in other sense whether some naming convention; so, that mean some names which in turn can be resolved to IP. Now on the other if you see the routers which can open up to or look up to network layer or IP, we'll not understand this names right, names can be only understood at the application level . So, routers should be given data in form of IP only. So, there is requirement of which some means can convert this name to IP. The primary job of DNS is that it works on this resolving name to IP. So, there is a concept of domain and sub domains as a in a sense that how much a domain cover in DNS. So, suppose Gauhati University DNS. So, what it its responsibility whether it will take care the "gauuni' as its domain, can have sub domain and so and so forth like we "gauuni dot ac dot in" may be a domain, "idol dot gauuni is ac dot in" a sub domain on the things, and the type of things, and there are concept of DNS servers which translate the domain name to the IP address. So, one is that management of this distributed domain, another is that I require domain name server which we'll transport which we will translate this domain name to IP addresses right. These two are the primarily one of the major activities of the things. The services offered by DNS is somehow similar to phone book for the internet as it translating human – friendly host name into IP address.

In client /server two categories of programs are use, in one that can directly used by the user such as e-mail and those that support other application programs. So, Domain Name System (DNS) is belongs to that category which is use as a supporting program that is used by other program.

6.7.1 Domain Name Space:

In DNS to have a hierarchical name space ,a domain name space was designed in an inverted –tree structure with the root at the top.It is defined that the tree can have only 128 levels, where level 0 is the root and level 127 is the top .

Label:

In hierarchical structure each node in the tree has a label, maximum of 63 characters string.The root one is a null string.DNS requires that nodes that branch from the same node have different labels and it must be unique.

Domain name:

A full domain name in this form is a sequence of labels and they are separated by (.) dots. And one must remember that the domain names are always read from the node up to the root.

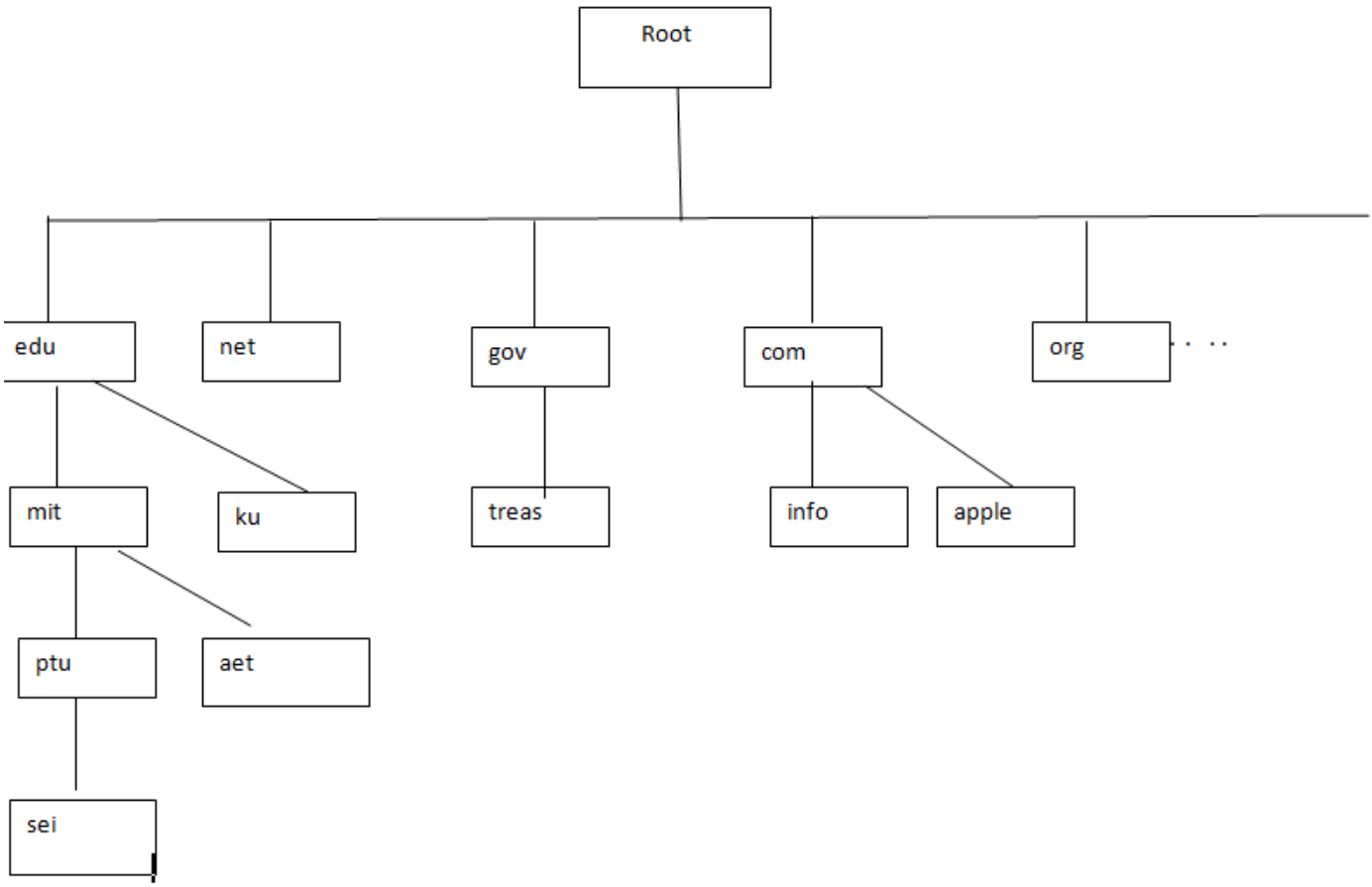


Fig 6.12 Domain tree

Fully Qualified Domain Name(FQDN)

If a domain name contains the full name of a host it is known as FQDN. In FQDN a label is terminated by a null string. Generally in FQDN it contains all labels from the most specific to the most general and it is uniquely defined the name of the host. It must be remembered that, the label ends with a dot (.) indicating null.

Partially Qualified Domain Name

A PQDN does not reach to the root which is strated from a node and it is not terminated by null string. It is used when the name to be resolved belongs to the same site as the client. Here the resolver can supply the missing part, called the suffix, to create an FQDN.

Domain

A domain can be defined as a sub tree of the domain name space. The name of the domain is the domain name of the node at the top of the sub tree. Domains are itself divided into some subdomains.

6.7.2 DNS in the Internet

Generic domains, country domains, and the inverse domain ,these three categories of domain name space is used in internet.

Generic domain:

According to the generic behavior generic domains define the registered host .In this category each node in the tree defines a domain. Example of generic labels.

Table 6.6 Internet domains

Label	Description
edu	Educational institution
gov	Government institutions
net	Network support centers
org	Nonprofit organizations
mil	Military groups
com	Commercial organizations

Country Domains

In country domains section it uses two character of particular country abbreviations i.e in for India.

Inverse Domain

The inverse domain is used in internet to map an IP address to a name. This situation is arise when a server has received a request from a client to do a task. The server has a file that contains a list of authorized clients, only the IP address of the client is listed. The server asks its resolver to send a query to the DNS server to map an address to a name to determine if the client is on the authorized list.

6.7.3 Resolution

As already mentioned that mapping a name to an address or an address to a name is called name-address resolution.

Resolver

As DNS is designed for a client/server application so a host that needs to map an address to a name or a name to an address calls a DNS client called a resolver. The resolver accesses the closest DNS server with a mapping request. If the server has the information, it reply the resolver; otherwise, it either refers the resolver to other servers or asks other servers to provide the information. After the resolver receives the mapping, it interprets the response to see if it is a real resolution or an error, and finally delivers the result to the process that requested it. In DNS mapping names to addresses and addresses to names is possible.

In name to address mapping most of the time ,the resolver gives a domain name to the server and requesting for corresponding address. On receiving request ,the server checks the different domains(generic or country domain) to find the mapping. If the domain name is from the generic domain or from the country domain the resolver gives a proper reply.

Mapping Names to Addresses Most of the time, the resolver gives a domain name to the server and asks for the corresponding address. In this case, the server checks the generic domains or the country domains to find the mapping. If the domain name is from the generic domains section, the resolver receives a domain name such as "chal.atc.jhda.edu.". The query is sent by the resolver to the local DNS server for resolution. If the local server cannot resolve the query, it either refers the resolver to other servers or asks other servers directly. If the domain name is from the country domains section, the resolver receives a domain name such as "ch.jhda.cu.ca.us.". The procedure is the same.

Mapping Addresses to Names

A client can send an IP address to a server to be mapped to a domain name. As mentioned before, this is called a PTR query. To answer queries of this kind, DNS uses the inverse domain. However, in the request, the IP address is reversed and the two labels in-addr and arpa are appended to create a domain acceptable by the inverse domain section. For example, if the resolver receives the IF address 132.34.45.121, the resolver first inverts the address and then adds the two labels before sending. The domain name sent is "121.45.34.132.in-addr.arpa." which is received by the local DNS and resolved.

STOP TO CONSIDER

In the Internet, the domain name space is divided into three different sections: generic domains, country domains, and the inverse domain. In DNS mapping name to address and address to name is possible.

6.7.4 DNS messages

DNS uses query and response types of messages. In query message it has two records a header and question records. The response message consists of a header, question records, answer records, authoritative records.

Check your progress

Q14.In DNS what is the label for non profitable organization?

Q15.PQDN stand for---------- (Fill in the blank)

6.8 Network File System(NFS)

This protocol was developed in 1984 for distributed file system. It applicable for client/server platform. This protocol enables system administrator to consolidate resources onto centralized servers on the network .In NFS it uses Remote Procedure Calls (RPC) to route requests between the client and the server .Details discussion on RPC will done shortly. It uses TCP or UDP for accessing files and delivering data. Using this protocol users can access the data and files remotely over the network.NFS are an open standard so any user can easily implement the protocol.NFS allow multiple computers to use the same files and everyone on the network can access the same file data. Thus NFS service makes the physical location of the file system irrelevant to the user.If anyone want to work with default installation of Red Hat Enterprise Linux with a firewall enables,IP tables must be configured with the default TCP port 2049.

6.8.1Versions of NFS

Currently there are three versions of NFS are available with different features of each versions. The vesions are NFSv2, NFSv3 and NFSv4.It must be note that all versions of NFS can use TCP running an IP based network. But NFSv2 and NFSv3 both can use UDP also and it provide a stateless network connection between the client and the server.

NFSv2: This version is the older version and widely used .As already mentioned NFS v2 uses the UDP to provide a stateless network connection between the client and the server.This version is widely supported by different operating systems.

NFSv3: This version several features are introduced to improve interoperability and performance.It supports safe asynchronous writes on the server which improve performance and makes response time faster.It also more robust at error handling than the earlier v2.NFSv3 supports 64-bit file sizes and offsets and allow clients to access data more than 2GB.

NFSv4: It enhances the performances and security of the network .This version requires TCP connection.

STOP TO CONSIDER

NFSv2 and NFSv3 can use UDP but NFSv4 requires TCP connection

Check your progress

Q16.What is NFS?

Q17.What are the different versions of NFS.

Q18.NFS uses TCP port ……..(Fill in blanks)

6.9Remote Procedure Call (RPC)

RPC or Remote Procedure Call is use as a fundamental building block for implementing remote operations in a distributed systems. The basic model of the RPC has been proposed Bruce Jay Nelson in 1981 was an American scientist. It is a request-response(client/server interaction) protocol i.e in RPC, a request message is send by client to the remote server to execute a specified procedure with supplied parameters. On receiving the request message from the client the server response to the client and the application continues its process.An important difference between a local call and remote call is that a remote call may be failed because of the unpredictable network problems may be in server side or client side.

6.9.1How RPC works

A complete RPC mechanism has mainly two components:

i. A protocol which manage the messages sent between the client and the server processes .

ii. Compiler support and programming language to package the arguments into a request message on the client machine and then to translate this message again into the arguments on the server machine and with the return value.

As it is already mentioned that RPC follow client /server model.A client has a request message that the RPC translates and sends that request to the server.On receiving a request (request may be a procedure or a function call to a remote server)from a client ,it sends the required response back to the client. While the server processing the call that time the client is blocked and only resume execution after the server processing is being finished.RPC has follow a sequence of events which can be listed as follows:

Firstly the client stub is called by the client. Then the client stub makes a system call to send the message to the remote server. From the client's operating system the message is sent to the server. Then the message is passed to the server stub by the server operating system .Whatever the parameters are assigned with client's message are removed from the message by the server stub and finally the server procedure is called by the server stub.

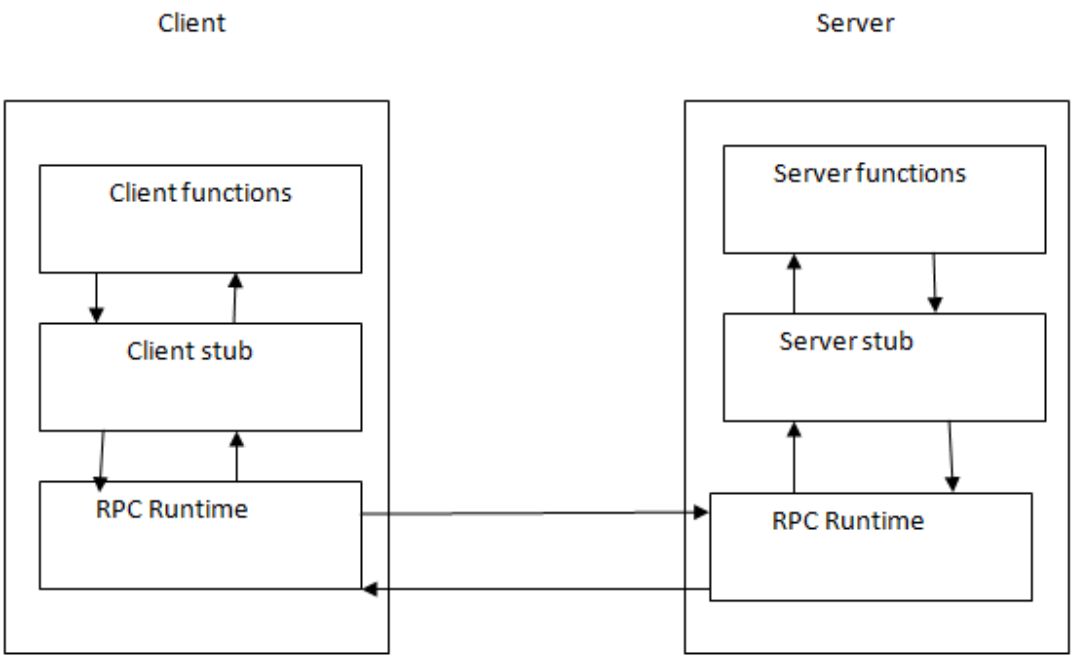


Fig 6.13 RPC

RPC or Remote Procedure Call is use as a fundamental building block for implementing remote operations in a distributed system.

SAQ

Q3.Explain RPC .

6.10 E-Mail (Electronic Mail)

Electronic mail or e-mail is one of the most popular Internet application program .Its architecture consists of several components and the components are discussed here shortly .At the very beginning e-mail messages were very short and only text messages were exchanged. Now a days electronic mail is too complex and it allows not only text message instead it includes text, image, audio and video .It integrate that facility also where more than one recipients can view the message at the same time .So here we study the architecture of an e-mail including its components and then protocols that implement this application discuss here. In an e-mail system three basic components are included: user agent, message transfer and message access agent.

6.10.1 Components of e-mail

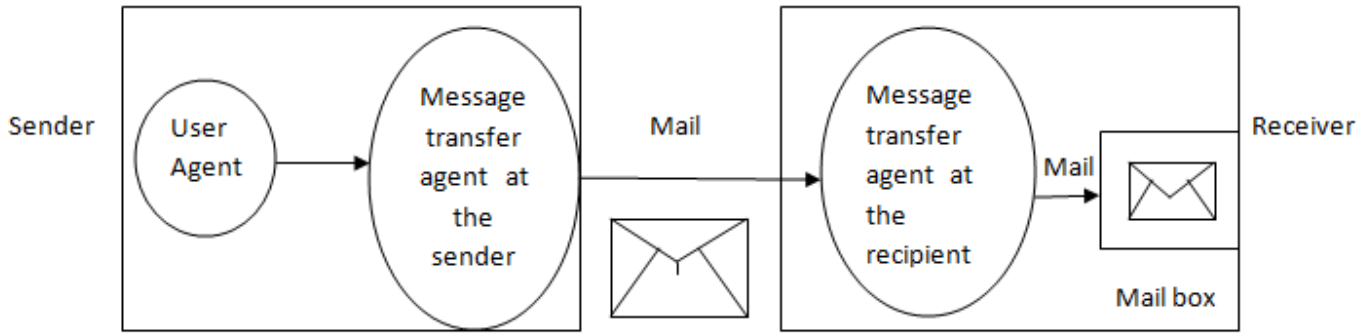
The e mail application contains three components:

i. The first one is known as user agent.User agent is what users responsible for interact with to send and receive mails.

ii. The second one is known as message transfer agent which navigates the mails to their recipients.

iii. The third and last component of the email is the mail itself.

Following figure shows the entire mailing process and different components of e-mail application.



. Fig 6.14 The e-mail process

i. **User Agent:** The user agent provide user the facilities for composing and helps in sending mails, reading message, replying messages, storing the address of the recipient in the address book and retrieve those address while sending mails, also providing option for storing them in a particular folder or for forwarding, etc. The services provided by user agent makes any user messages easier (sending or receiving).There are two types of user agent: GUI based and command driven agent.

GUI based: Now a days GUI based user agent are used i.e modern agent are GUI based. The GUI based user agent contains graphical based interface components. In this type the user can interact with software by using mouse or keyboard. It contains some graphical icons, bar, menu other icons which makes the services easy to access.GUI based user agent are Microsoft's outlook, Netscape.

Command driven agent: In earlier days command based agents are used.Still they are used as user agent in server side.In this types of agent one character command from the keyboard is accepted to perform a particular task.Examples of this type are pine,elm and mail etc

ii. **Mail transfer agent (MTA):** The other component of e – mail. It picks up the mail and delivers it to the other end of user .It set-up a TCP connection between the end user and prepares the mail .SMTP has set it rules how the sender proceeds after set up a connection .Discussion on SMTP will done later in this chapter.

iii. **The mail:** The important component of email. The content may be simple text ,an image, an audio ,a video clip or may be an html page. The different content may also may be in different format also. For example an image file may be in ".jpeg" or ".png" or may be in ".gif" .

There are two types of user agent: command based or GUI based.

E-mail address:

For sending and receiving any e-mail each user requires a unique email account. This is known as e-mail address. Generally e-mail are known as specific address in networking and it follow a particular rule for its addressing of the form username@domainname .

To create an e-mail address following rule should be followed:

- The user name and the domain name are separated by "@" symbol.
- This address is not case sensitive.
- Spaces are not allowed.

Sending Mail:
Through the UA, an user can creates mail that looks very similar to postal mail. It has different parts such an envelope and a message.

Envelope

The envelope usually contains the sender and the receiver addresses. (TO and FROM)

Message

The message contains two sections: the header and the body. The header has as mentioned several sections .Following parts are there in header:

- To: To whom the mail is sent.
- From: Who sent the mail.
- Subject:It indicates the purpose of the mail.
- Date:It indicates the date when the mail is sent
- CC: **CC** for Carbon copy. It includes those recipient addresses whom we want to keep informed but not exactly the intended recipient.

- BCC: Bcc for **blind carbon copy** . It is used when we do not want one or more of the recipients to know that someone else was copied on the message.

Greeting

Greeting is the opening of the actual message.

Signature

This is the final part of an e-mail message. It includes Name of Sender, Address, and Contact Number.

The body of the message contains the actual information to be read by the recipient.

6.10.2 Simple Mail Transfer Protocol (SMTP)

In e- mail actual mail transfer is done using Mail Transfer Agents(MTA).To send email user need a client MTA and to received the sending mail the server must have a MTA.SMTP is a standard protocol that defines the MTA client and server in the internet. SMTP defines how commands and responses are sent back and forth between the user.

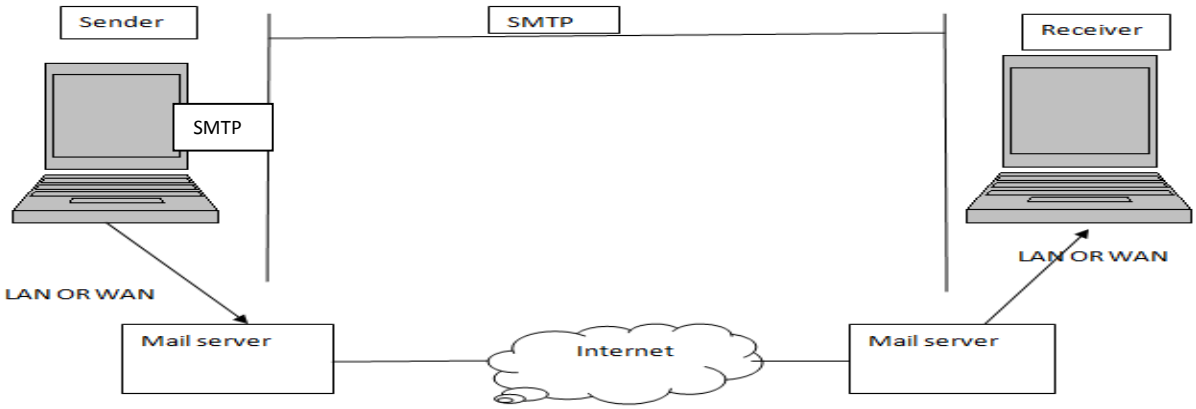


Fig 6.15 SMTP protocol range

In email SMTP is used between the sender and the sender's mail server and between the sender and receiver's mail server. Another protocol POP3 and ICMP are used to carry the mail to the receiver from the server. Different command and responses are uses in SMTP between an MTA client and an MTA server

SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.

In SMTP Commands are sent from the client to the server. SMTP defines 14dfifferent commands. Some of the commands are mandatory and remaining commands are often used. Some of the SMTP commands are given as follows:

Table 6.7 SMTP Commands

Keyword	Argument
HELO	Sender's host name
MAIL FROM	Sender of the message
DATA	Body of the sending mail
HELP	Command name

In SMTP responses are from the server to the client. Responses are normally three digit code followed by some textual information. Some of the responses are included in table 6.8

Table 6.8 SMTP responses

Three digit code	Description
211	System help
250	Request command completed
354	Start mail input
421	Service not available
500	Syntax error
554	Transaction failed

Mail Transfer Phases

The mail transfer occurs in following phases: connection establishment, mail transfer, and connection termination.

6.10.3 POP and IMAP:

Post Office Protocol, version 3 (POP3) and Internet Mail Access Protocol, version 4 (IMAP4) are the currently used as e-mail mail access protocol.

In the recipient computer the client POP3 software is installed and the server POP3 software is installed on the mail server. The client use the TCP port 110 and mail access starts with the client when the user needs to down load e-mail from the mailbox .When the client opens a connection with TCP ,it then sends its user name and password to access the mailbox. From the mailbox the can then list out and retrieve the mailbox. In POP3 if the mail can be deleted from the mailbox after each retrieval then it is known as delete mode and if the mail remains in the mailbox after retrieval also it is known as keep mode. Thus in POP3 two modes are available.

IMAP(Internet Mail Access Protocol)

Internet Mail Access protocol version 4 is similar to POP3 which is also can be use in e-mail as mail access protocol. But POP3 has some limitation and those limitation can be overcome by using IMAv4 protocol . IMAP v4 is more complex and more powerful than POP3.IMAPv4 has additional functions over POP3.Some of them are listed below:

i. Before downloading a user can check the mail header.

ii.On the mail server a user can create, delete or rename mail boxes.

iii.Prior to downloading a user can search the contents of the mail for a specific string of characters.

6.11 SUMMING UP

- The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCPI/IP protocol suite.
- The World Wide Web(W3) or the Web is an architectural framework for accessing linked content spread over millions of machines all over the Internet or it is the repository of information linked together from points all over the world.
- In 1990 Tim Berners Lee first ever introduce browser known as WorldWideWeb(no space).
- URL is known as web address, is a unique identifier used to locate a resource on the internet composed of multiple parts. In 1994 ,URL was first introduced as a part of the Uniform Resource Identifier(URI).
- Web documents can be broadly classified into the categories: Static, Dynamic and Active.
- Hypertext Markup Language (HTML) is use to create web pages.HTML can describes the structure of the web pages. While developing a web page with HTML ,it consist series of elements and these elements tells the web browser how to display the content of the web page.
- HTTP is an application layer protocol used basically to access data on the World Wide Web. HTTP is a request –response protocol. It uses the services of TCP. It provides an interface to the user to transfer resources in terms of request –response message using TCP protocol.
- In HTTP it use a three digit code which indicates the responses or status. The status code has five categories depending on their functionalities.
- A proxy is an application program or a computer system that behaves like an intermediary between the clients looking for services and servers.

- FTP is an application layer standard protocol for transferring files from a server to a client or from a host to another. During transfer of file from one system to another there may be several issues say, two systems may use different ways to represent text and data or may use different file name conventions.
- Domain Name System (DNS) is belongs to that category which is use as a supporting program that is used by other program.
- In application layer, there are various protocols right, like some related to file transfer, email, remote login, network management and there is a name management or name resolution for name resolution which is DNS.
- FTP is an application layer standard protocol for transferring files from a server to a client or from a host to another.FTP need to connection: control connection and data connection.
- NFS enables system administrator to consolidate resources onto centralized servers on the network .In NFS it uses Remote Procedure Calls (RPC) to route requests between the client and the server.
- RPC or Remote Procedure Call is use as a fundamental building block for implementing remote operations in a distributed system.

- Electronic mail or e-mail is one of the most popular Internet application program.

- In an e-mail system three basic components are included: user agent , message transfer and message access agent.

- SMTP is a standard protocol that defines the MTA client and server in the internet. SMTP defines how commands and responses are sent back and forth between the user.

- Post Office Protocol, version 3 (POP3) and Internet Mail Access Protocol, version 4 (IMAP4) are the currently used as e-mail mail access protocol.

- IMAP v4 is more complex and more powerful than POP3.

6.12 KEY TERMS

- Manager :A manager is a host that runs the SNMP client program.
- Agent : An Agent is a router that runs the SNMP server program.
- Web Browser :The web browser or the browser is an application software used to interact the user with the content and data on the web
- Server: Web server or server is the part of Internet where all web pages are stored. When a client send a request for a particular document to the server on arriving the request corresponding document is sent to the client from the server.

- Mail transfer agent(MTA) :The other component of e- mail. It picks up the mail and delivers it to the other end of user.

6.13 ANSWER TO CHECK YOUR PROGRESS

1.False

2. A manager is a host that runs the SNMP client program.

An agent is a router that runs the SNMP server program.

3. URL is known as web address,is a unique identifier used to locate a resource on the internet composed of multiple parts.

4.True.

5. The basic features of the web includes flexibility, portability and user friendly.

6. Cookies are alphanumeric values stored at the client by the browser

7. The content of static page cannot changed by client ,the client can get only a copy of the document. When the file is created the contents are determined i.e static documents are fixed –content documents that are created and stored in a web server.

8.False.

9. A markup language allows developer to embed formatting instructions in the file itself.

10. The head and the body.

11.True.

12.80

13. A proxy is an application program or a computer system that behaves like an intermediary between the clients looking for services and servers. HTTP protocol support proxy server. It keeps copies of responses to recent requests.

14..org

15.Parially Qualified Domain Name.

16. This protocol enables system administrator to consolidate resources onto centralized servers on the network.

17.NFSv2,NFSv3 and NFSv4.

18.2049

6.14 QUESTION AND ANSWERS:

1. SNMP is the framework for managing devices in an internet using the ---------- protocol. .(Fill in the blank)

2. The application level protocol in which a few manager stations control a set of agents is called SNMP .(TRUE/FALSE)

3.The DNS translates internet domain and host names to IP address.(TRUE/FALSE)

4. FQDN is terminated by a -------string.(Fill in the blank)

5. An HTML file is a text file containing…… .(Fill in the blank)

6. FTP works on transport layer.(TRUE/FALSE).

7. FTP uses port number 21 for control connection.(TRUE/FALSE)

8 .Microsoft Outlook is an example of user agents for e-mail.(TRUE/FALSE)

9. URL stands for _____.(Fill in the blank)

10.What are the two types of user agent used in e-mail?

ANSWERS:1.TCP 2.TRUE 3.TRUE 4.NULL 5. markup tags 6.FALSE 7.FALSE

8.TRUE 9.UNIFORM RESOURCE LOCATOR 10. command based or GUI based user agent.

Short type questions:

1.What do you mean by manager and agent in SNMP?

2.What is DNS?

3.Define WWW.

4.Mention name of different connections required in FTP?

5.What are the different pages used in HTML?

6.Write down the different components of e-mail.

7.Why NFS is used?

8.What is RPC?

9.What is SMTP?

10.What do you mean by MTA?

11.What is status code used in HTTP?

12.Why IMAP is used ?

13.What do you mean by active document?

Long answer type question:

1.Discuss the role of SNMP in network management.

2.Explain about the different connection of FTP with suitable diagram.

3.Expalin how DNS works as address resolver?

4.Discuss the different types of pages uses in HTML.

5.Write a short note on NFS.

6.Expalin about different protocols used in e-mail.

7.Why RPC is used explain in detail.

8.Discuss the need of FTP protocol.

6.15 SUGGESTED READINGS

- Bhushan Trivedi,Computer networks Oxford higher education.2019
- B.A Forouzan ,Data communications and network McGraw Hill higher education,2018

UNIT 7: Network Management and Security

CONTENTS

Network Management and security

7.1 Introduction

In this chapter we discuss the Basics of network management and the security. Moreover the infrastructure for network management and security are also discussed. Networks and distributed processing systems are of critical and day by day growing importance in enterprises of all sorts. So network management and security is one of the important topic of discussion. Network management is the process of administering and managing computer network or network management can be defined as overall monitoring of networks, testing, troubleshooting network components and configuring the network to meet a set of requirements defined by different organization. To perform network management operation a network management system uses a combination of software, hardware and human. Here we discuss the most common protocol SNMP used in management .Again security part network security part is of equal importance in network, so that part is also discussed here. Cryptography, Firewall and Digital signature parts are introduce here.

7.2Objectives

This unit basically includes basic concept of network management and security. Infrastructure for network management and security part is also include in this unit. In this unit you will be able to learn:

- Key requirements that a network management system should satisfy
- Give an overview of the architecture of a network management system and explain each of its key elements.
- Describe SNMP with different versions
- State and explain the need of network security and the different services of network security
- Explain basics of Cryptography.
- Symmetric and asymmetric key cryptography.
- Explain basics of Digital signature.
- Idea of hash function

7.3Network Management system

As it is already explained that network management is the combination of software, hardware and human .The different functions performed by a network management system can be divided into different categories such as :

Security management, configuration and name management, fault management , Performance management and accounting management .

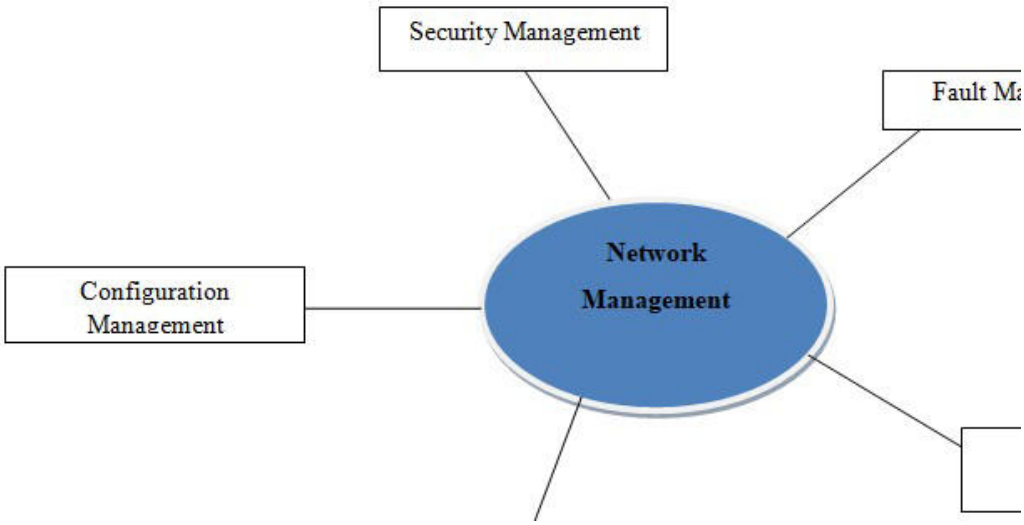


Fig 7.1 Different functions of Network Management system.

- Security Management

Security management is basically concerned with monitoring and controlling access to computer networks and access to all or part of the network management information obtained from the different network nodes. It also concerned with generating, distributing and storing different encryption keys. User passwords and other authorization or control information are also maintained and distributed. Network resources and user information protection are done in security management. Logs are considered as one of the important security tool, so security management involve with the collection and storage of records .Again network security facilities should be available for authorized users only in a network. It is responsible for controlling access to the network depending on the predefined security policy

- Configuration and Name Management

As we know that networks are composed of hundreds of entities that are connected somehow i. e may be physically or logically they are connected with each other .All these entities have an

configuration at the initial stage when a network is set up but it may not be permanent .It need to be change with time. Some of the computers may replaced by others , sometimes the operating system may be updated to a newer version and the particular user may be moved from one network to another. So at any time the configuration management must know the status of each entity in that network and relation of one entity with others. Depending on the type of function performed in different parts of network, configuration management can be classified into two subsystems: reconfiguration and documentation.

Reconfiguration

Reconfiguration may be of several types such hardware reconfiguration, software reconfiguration and user account reconfiguration. Any changes of hardware under hardware reconfiguration for example, suppose a switch may need to be moved to another part of the network or may be one desktop is replaced by a laptop etc. All these need the time and attention of network management, again these types of reconfiguration cannot be automated and must be manually handled by some specialized person case by case. Software reconfiguration coves functions any changes to the software such as a operating system need to be updated for a newer version .But most of the software reconfiguration can be automated .User account reconfiguration can be to some extent automated but human interaction is also required. User account reconfiguration covers adding and deleting of user, or other task such as a user may have some write and read permission with regard to some files or some permission for downloading a file etc.

Documentation

In network configuration ,the original network configuration or any changes in the network must be recorded. In any kind of reconfiguration(i.e in software, hardware or user account reconfiguration)documentation is required. In hardware documentation two sets of documents involves: maps and specifications. Where maps tract each piece of hardware and its connection to the network but it is not sufficient and the specifications include types of hardware, its serial no. if any ,time of purchase, warranty information etc. Similarly all software also must be documented including different information about the software such as type of software, installed version and the time of installation etc. Using documentation the network management must make sure that the files with this information are updated and secured.

- Fault Management

Fault management is that particular are of network management that specially deals with any fault of the network components. A fault is usually indicated by failure to operate correctly or by excessive errors. An example of a fault is a damaged transmission medium. This fault may interrupt communication or produce excessive errors .In the present scenario, networks are more complex and it made up of hundreds or thousands of components. Proper operation of this type

complex network depends on the proper operation of each and every component individually and in relation to each other. Fault management handles these types of issues. Reactive fault management and proactive fault management are two subsystems of fault management. Short term solutions of any fault (error) are handled by reactive management. It is basically responsible for detecting, isolating, correcting, and recording faults. The other subsystem of fault management is proactive fault management which tries to prevent faults from occurring. Some types of failures can be predicted and prevented before occur but this is not always possible.

- Performance Management

A performance management function includes monitoring and controlling .It is closely related to fault management which tries to quantify performance by observing capacity, traffic, throughput and response time. Here activities of the network are tracked by monitoring.

Capacity

Performance management system monitors the capacity of the network. As we know that every network has a specific limited capacity, and the performance management system must ensure that it is not used above this capacity. It can be explained with a example say a network is designed for 250 stations at an average speed of 900Kbps,then it never operate properly for 500 stations .

Traffic

During a particular time which is also can be considered as peak hours when all the systems are heavily used blocking may occur if there is excessive traffic in that network. Traffic can be measured internally or externally. Inside the network if number of packets is measured it indicates as internal traffic again if it measured exchange of packets outside the network it known as external traffic.

Response Time

Performance management also measure the response time .Response time is measured from that time when a user request for a service till the server granted it. Increase response time consider as a serious condition and it indicates traffic .

Throughput

Performance management monitors the throughput also and try not to reduce it beyond a limit.

Accounting Management

Accounting management observes the users' access to network resources through charges. For any service from the network individual users, departments, divisions are charged. In accounting management charging may not be always mean cash; it may be debiting the departments or divisions for budgeting purposes. Different organizations use an accounting management system for different reasons such as to prevents users from using the system inefficiently and network managers can planned some short or long-term planning based on the demand for network use. In accounting management reports should be generated under network manager control.

STOP TO CONSIDER

The Network Management System is the combination of software, hardware and human .The different functions performed by a network management system can be divided into different categories such as : security management, configuration and name management, fault management , Performance management and accounting management .

CHECK YOUR PROGRESS

Q1.What are the different types of reconfiguration management under Configuration and Name Management?

Q2. Inside the network if number of packets is measured it indicates as internal traffic.(TRUE/FALSE)

7.4 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol is a network management protocol using TCP/IP protocol suite .It is a framework for managing devices in an Internet and it provides a set of fundamental operations for monitoring and maintain an Internet. The basic concept of SNMP with Managers and Agents explained in chapter 6.In this chapter we are discussing management components of SNMP, its role and versions of SNMP.

7.4.1Management components

SNMP uses two other protocols to do management task on the Internet which are: Structure of Structure Of Management Information(SMI) and Management Information Base (MIB),Shown in Fig 7.2

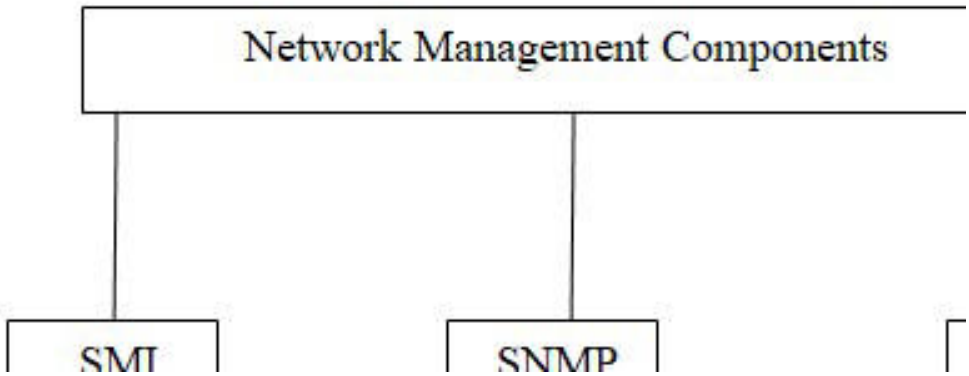


Fig 7.2 Network Management components

SMI

Structure of Management Information (SMI) is a collection of general rules to name object and to define type of data that can be stored in an object. It also shows how to encode data for transmission over the network.. To handle an object it emphasizes three attributes: name, encoding method and type.SMI follow a hierarchical structure for an object identifier. To name objects globally, an object identifier is used by SMI.SMI requires that each managed object have a unique name.

MIB

The Management Information Base, version 2 (MIB2) is another component of network management .As stated earlier SMI defines rules in network management i.e it set rules to name object and defines type of data where in type it defines only the range and size that can be stored in an object but MIB version 2(MIB 2)names each object and also define type of the object.
In MIB2 objects are categorized into different groups which are snmp , udp, tcp,system,address ip,icmp etc. All these groups are under mib2 object in the object identifier tree where each group has defined variables .Some example of objects are:

i. snmp: This object defines general information related to SNMP itself.

ii.tcp: tcp object defines information related to TCP, such as number of packets sent and received, number of ports etc. ”udp” object is also similar to tcp which defines information related to udp.

iii.sys: sys object related to system information such as name, location etc.

A management station performs the monitoring function by retrieving the value of MIB object.

SNMP

As stated earlier the SNMP is the network management tool and it works on concept of managers and agent. The basic introduction of SNMP and the concept of manager and agent is explained in earlier chapter-6.

In network management SNMP takes helps of both SMI and MIB.In SNMP allows a manager to retrieve the value of an object defined in an agent,it also allow a manager to store a value in an object defined in an agent and it allows an agent to send an alarm message about an abnormal situation to the manager.SNMP has different versions with different features of each version .Normally SNMP has three versions:SNMPv1,SNMPv2 and SNMPv3.

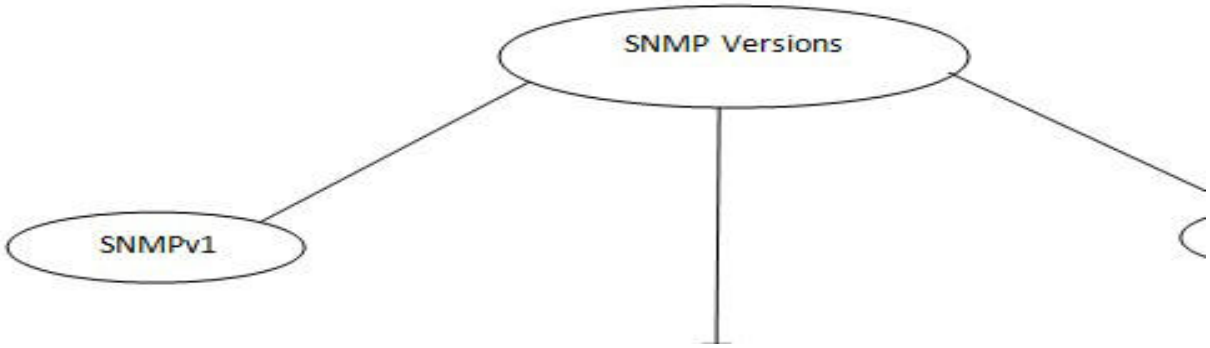


Fig 7.3 SNMP versions

SNMPv1

The original SNMP protocol is also called as SNMPv1.In 1980s ,SNMPv1 was designed.SNMPv1 is widely used and it is the de facto network management protocol .In 1988 the first RFCs(Request for Comments) was appeared.RFC 1065, RFC 1066, RFC 1067 were used by SNMP.SNMP uses UDP connection again we know that UDP is a connectionless protocol so it itself connectioless.In SNMP management request are sent to UDP port 161 and the agent sends traps to UDP port 162.The manager and agent both implement SNMP ,UDP and IP and the other relevant network dependent protocol. Three types of SNMP messages are issued on behalf of management applications which are: GetRequest, GetNextRequest and SetRequest. All messages are acknowledge by agent using GetResponse message. The main issue with SNMPv1 is the security.SNMPv1 was designed with 32 bit counter means that it can count from

0 to 4.29 billion i.e it cannot store maximum of a 10 gigabit or large interface.In SNMPv1 password can be read with packet sniffing

SNMPv2

The enhanced version of SNMP is known as SNMPv2 with more security options. SNMP v2 allows password hashing with MD5 .SNMOv2 was specially developed to provide data security .

SNMPv2 is the revised version of SNMP with enhanced protocol packet types ,MIB structure elements but it uses the existing SNMPv1 administration structure.SNMPv2 uses RFCs 1901,1905 through 1909 and 2578 through 2580.In SNMPv2 it introduce a option for 64 bit data counters which can store from zero to 18.4 quintillion(approximately).

SNMPv3

With more security options SNMPv3 was introduced.SNMPv3 provides three important services which are: privacy, authentication and access control. Privacy and authentication are part of the User Based Security model(USM) and access control is defined in the View-Based Access Control Model(VACM).Moreover SNMPv3 allows a manager to change the different security configuration remotely .

SNMP types of packets or PDUs

The different messages uses in different versions of SNMP are:

i.GetRequest: The GetRequest is sent from the manager (client) to the agent (server) to retrieve the value of a variable or a set of variables.

ii GetNextRequest :It is sent from the manager to the agent to retrieve the value of a variable.

iii.GetBulkRequest : The GetBulkRequest is sent from the manager to the agent to retrieve a large amount of data. It is the replacement of multiple GetRequest and GetNextRequest.

iv. SetRequest : The SetRequest is sent from the manager to the agent to set a value in a variable.

v. Response: The Response is sent from an agent to a manager in response to GetRequest or GetNextRequest.

vi. Trap: The Trap is sent to the manager from the agent to report an event.

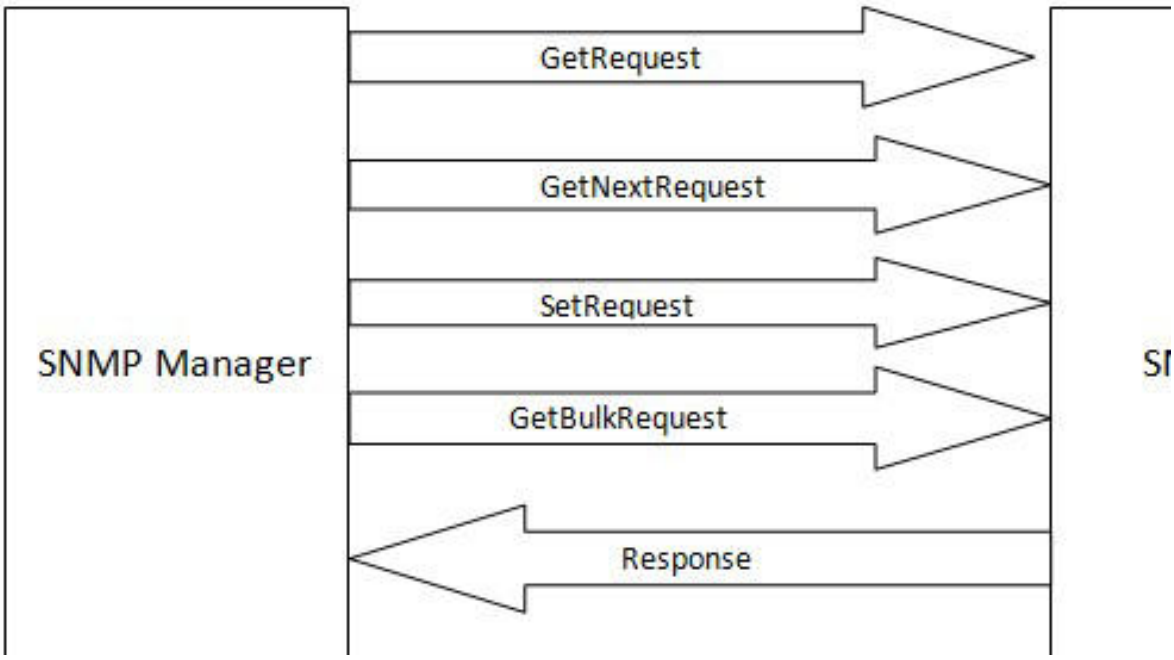


Fig 7.4 SNMP different data packets or PDUs

STOP TO CONSIDER

In network management SNMP takes helps of both SMI and MIB. SMI is a collection of general rules to name object and to define type of data that can be stored in an object. It also shows how to encode data for transmission over the network. MIB version 2(MIB 2) names each object and also define type of the object. SNMP has three versions SNMPv1,SNMPv2 and SNMPv3.

CHECK YOUR PROGRESS

Q3. The Trap is sent to the agent from the manager to report an event. (TRUE/FALSE)

Q4.SNMPv1 contains ----------bit counter.(Fill in the blank)

Q5.What are the different services provided by SNMPv3?

7.5Network Security

Network security is one of the major concern in networking.The network may be attack by several threats but we have to protect our data somehow,so in this chapter we will introduce security services that we typically expect in a network.Then we discuss how cryptography can be used in network security and also discuss about the concept of symmetric and asymmetric keys.Digital signature will also be discussed here.

7.5.1 Security services

Network security can address different services related to the message and the entity. Some of the message related services are: privacy or confidentiality, authentication, integrity and availability. Again service related to entity is entity authentication or identification.

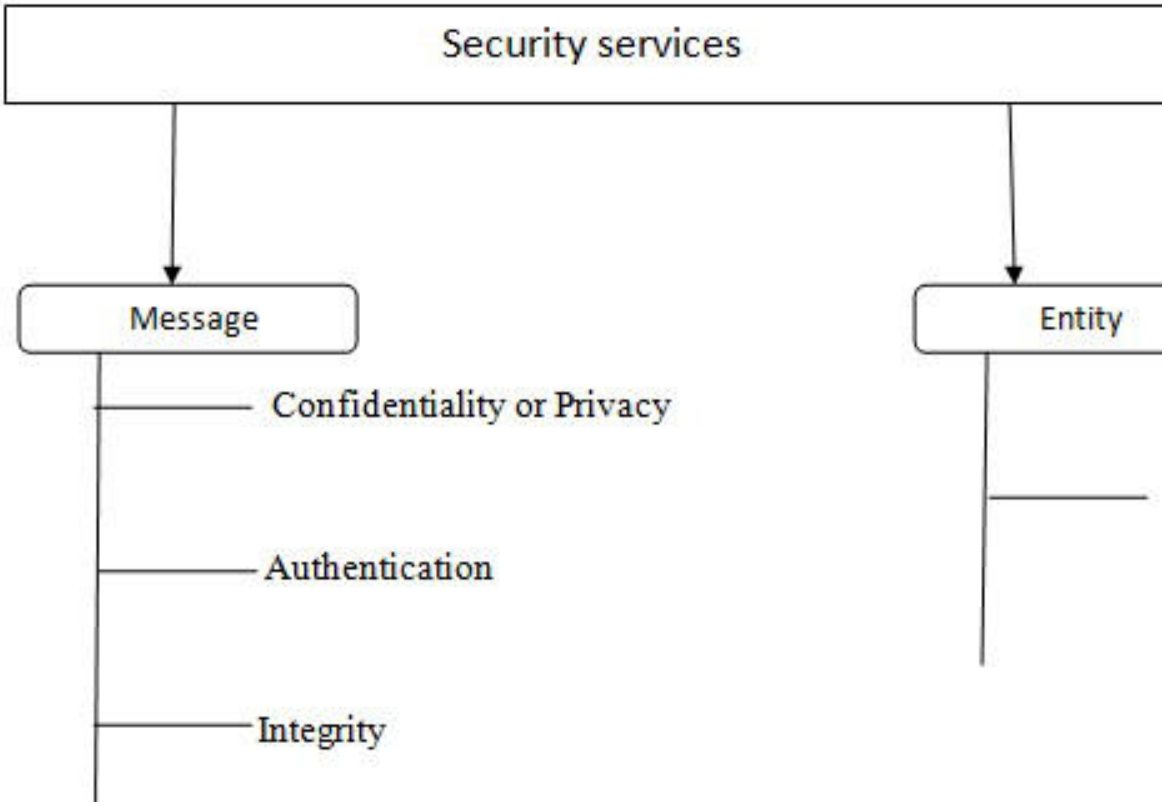


Fig 7.5 Message and entity related security services

Message:

Confidentiality or Privacy

In a network a user expect privacy or confidentiality. When a sender sends a message it sends it to a particular or intended receiver. Say when a customer communicates online with a medical consultant or with online banking is done the user expects that the communication between the two parties must be confidential.

Authentication

While a receiver receives a particular information the receiver needs to be sure that about the sender's identity otherwise in some situations it may be a critical issue.

Integrity

Message integrity describes the concept of ensuring that data has not been modified in transit it requires that only authorized parties can modify data. Message modification includes writing, deleting, changing status etc.

Nonrepudiation

Generally , nonrepudiation combines both authentication and integrity. It provides proof of the originality, authenticity and integrity of the sending data.It helps in sender's identity and later on neither site can deny that a message was sent ,received.

Entity Authentication

The entity authentication or user authentication is done before access of the web resources .The entity authentication is one way to protect the resources and the user.

7.5.2 Message Privacy or Confidentiality

In message confidentiality the message must be secured somehow so that the message is being unintelligible to any of the unauthorized parties.

In that case some privacy techniques are used and this techniques guarantees to some extent .The concept of cryptography is used where messages are encrypted at the sender site and decrypted at the receiver site.

Cryptography

Network security mostly achieved through the use of cryptography which means secret writing. In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms While explaining Cryptography several terms are used such as plaintext ,cipher text, key so all are discussed here. These are considered as components of cryptography. During

cryptography in sender site the sending message is encrypted and in receiver site the message is decrypted. Following fig7.6 shows the components of cryptography:

Fig:7.6 Components of cryptography

Now we are going to discuss about the different terms used in above diagram.

Plaintext

The original message the sender send before being transformed or encryption is known as plaintext.Encryption algorithms are used to transformed a plaintext to ciphertext in sender site.

Ciphertext

When message (plaintext) is transformed using encryption algorithm it is known as ciphertext. In receiver site some decryption algorithms are used to transform ciphertext back into plaintext.

Cipher

Whatever encryption and decryption algorithms are used known as ciphers.

Key

Key are nothing but a number or a set of numbers that the cipher ,as an algorithm operates on.For encryption ,an encryption key and plaintext are required which gives us ciphertext .Simillarly in decryption message (from ciphertext to plaintext) a decryption algotithm,a decryption key and the transformed ciphertext ,which gives a receiver the original message(plaintext)

The categories of cryptography algorithms (cipher):

Cryptography algorithms are divided into two groups:

- Symmetric key cryptography algorithms
- Asymmetric key cryptography algorithms.

Symmetric key cryptography algorithms

The basic concept of symmetric key is that ,in symmetric key both parties uses the same key .In sender site the sender uses this key for encrypt data with an encryption algorithm and in receiver site the receiver uses the same key to decrypt the encrypted data with a decryption algorithm.

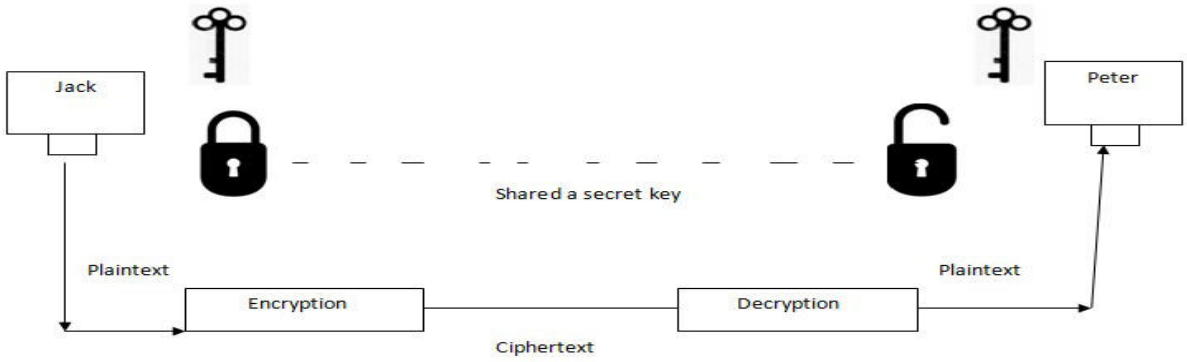


Fig:7.7 Symmetric key cryptography where a shared key can be used in Jack-Peter communication

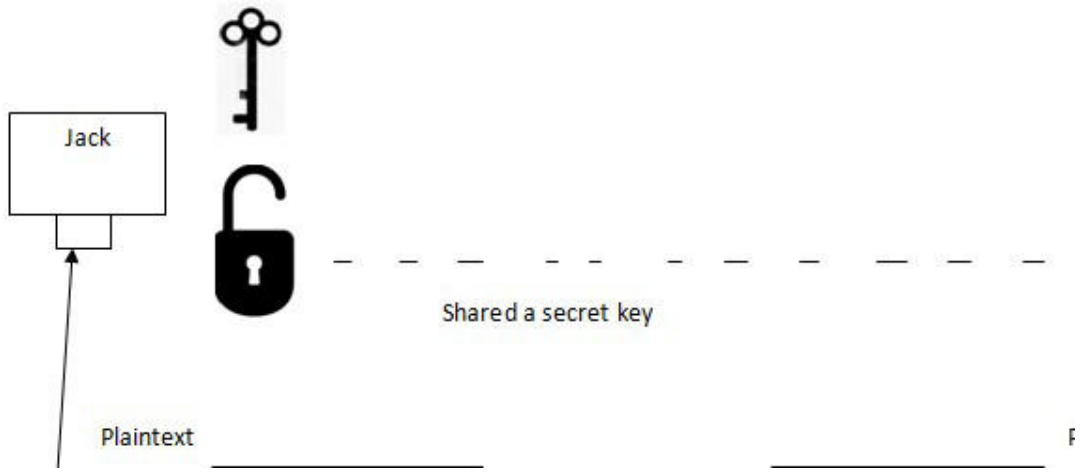


Fig 7.8A different key is recommended in Peter –Jack communication

As shown in the above fig 7.7 and fig 7.8 to provide confidentiality or privacy with symmetric-key cryptography, a sender and a receiver need to share a secret key. The symmetric key allows the communication both direction communication is possible although it is not recommended. In communication two key concepts is most popular .As if one key is compromised, the communication is still confidential in the other direction. So symmetric key is still the dominant method for message confidentiality .But for long message symmetric key cryptography is considered to be more efficient.

Ciphers are more complex used in symmetric key, now we are going to discuss traditional ciphers., which are character oriented. Some ciphers are bit oriented also.

Traditional Ciphers

Now we are introduce some of the traditional ciphers which are obsolete now but we try to show how modern ciphers are evolved from those ciphers. Traditional symmetric key ciphers has two categories:

- Substitution ciphers and
- Transposition ciphers.

Substitution cipher

As the name suggest a substitution cipher substitute one symbol with another symbol. Depending on the plaintext substitution are used say if plaintext are some alphabetic characters than one alphabetic character is replace with another again if it numbers than it replaced by numbers in ciphertext.For example in alphabetic character B replaced with H and character F with U .And in numbers 1 replace with 8 or 4 with 9etc.Numbers 0 to 9 consider. Substitution ciphers have two categories: monoalphabetic or polyalphabetic ciphers.

In a monoalphabetic a symbol(alphabet or number) in the plaintext or always changed to the same symbol means that if that algorithm says that X is replaced with B then every character X is peplacewd with B regardless of the position.Plaintext and ciphertext relationship are one to one.

But in polyalphabetic cipher it is not like that here each occurrence of a character in plaintext can have different substitute in ciphertext i.e it follow one –to- many relationship .

Example 1.The following shows a plaintext and its corresponding ciphertext. Is the cipher monoalphabetic?

Plaintext: SORRY Ciphertext: APXXR

Solution :The cipher is probably monoalphabetic because both occurrences of R's are encrypted as X's.

Example 2

The following shows a plaintext and its corresponding ciphertext. Is the cipher monoalphabetic?

Plaintext: SORRY Ciphertext: ZATCG

Solution : As in ciphertext each occurrence of R is encrypted by a different character so it on not monoalpahbetic rather it is polyalphabetic.

Transposition ciphers.

In this cipher locations are change instead of substitutions. A symbol in the plaintext may be in the first position but in ciphertext it may in 7^{th} position i.e it reorders the symbol in a block of symbols. For example:

Plaintext: 4567

Ciphertext:7654

So in this example we change the position of the symbols. In decryption we have arrange them only in reverse order.

- Asymmetric Key Cryptography

  In asymmetric key cryptography two keys are used instead of one as in symmetric key. Here a private key and a public key are used. The sender uses the public key to encrypt the message and the receiver kept a private key to decrypt the encrypted message. The public key is available to the public but the private key is available only to an individual.

  For a two way communication between Jack and Peter two pairs of keys are needed. When Jack sends a message to Peter ,Jack uses Peter's pair again when Peter sends a message to Jack he uses Jack's pair as shown in fig 7.9 and 7.10 respectively.

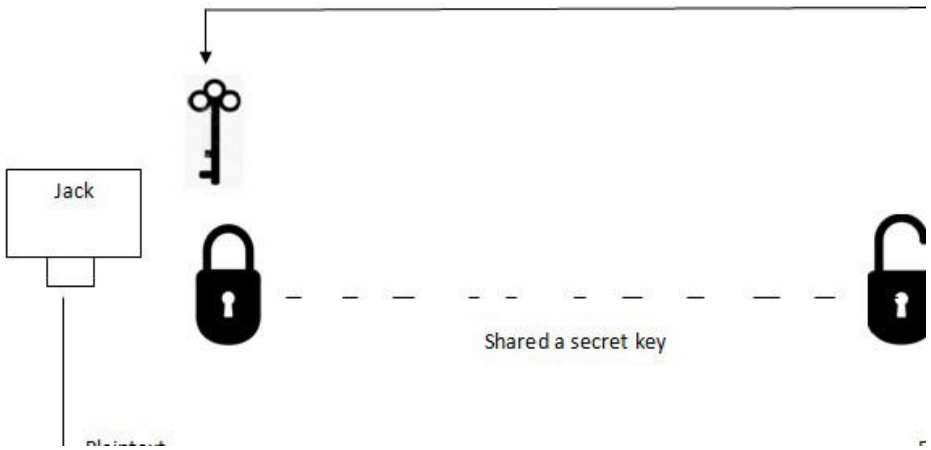


Fig 7.9 Peter ‘s keys are used in Jack-Peter communication

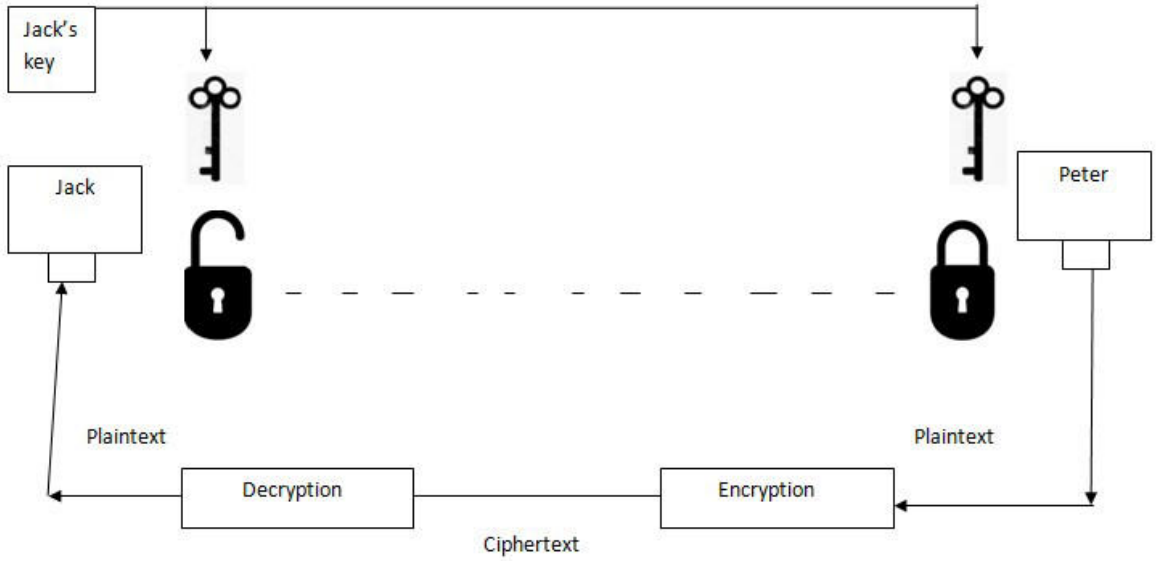


Fig 7.10 Jack’s keys are used in Peter-Jack communication

Asymmetric key is applied only to short messages i.e this system is inefficient for long messages.

The most common public key algorithm used in asymmetric key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA).

STOP TO CONSIDER

Network security mostly achieved through the use of cryptography which means secret writing.

Symmetric and asymmetric key cryptography are the two categories of cryptography.

In symmetric key cryptography single key is shared between the sender and receiver known as

Check your progress

Q6.Message after encryption is known as----------.(Fill in the blank)

Q7.What do you mean by cipher?

Q8.What are the different categories of traditional ciphers?

SAQ

Q1.Disscuss different categories of cryptography .

7.5.3 Message Authentication

In communication message authentication is one of the important factor as the receiver must have to confirm about the sender identity proof.The digest created by a hash function is called modification detection code (MDC) ,this can be used to detect any modification in the messages.Hash function will shortly discussed in message integrity section.

For message authentication a message authentication code (MAC)is required where it uses a keyed hash function .A keyed hash function includes the symmetric key between both parties i.e between the sender and the receiver when creating the digest.

Digital signature

As above mentioned MAC can provide message authentication in MAC it needs a symmetric key that must be established between both parties which is consider as a disadvantage of MAC .So digital signature introduced where it use asymmetric keys i.e public and private keys .An electronic signature can prove the authenticity of the sender of a message and this type of signature is called digital signature. As we know that in a traditional manual manner a person

sign a document to show that it originated from him/her or approve by him/her .Here the signature is the proof to the recipient that the document comes from the correct sender. Similar case in digital document also.

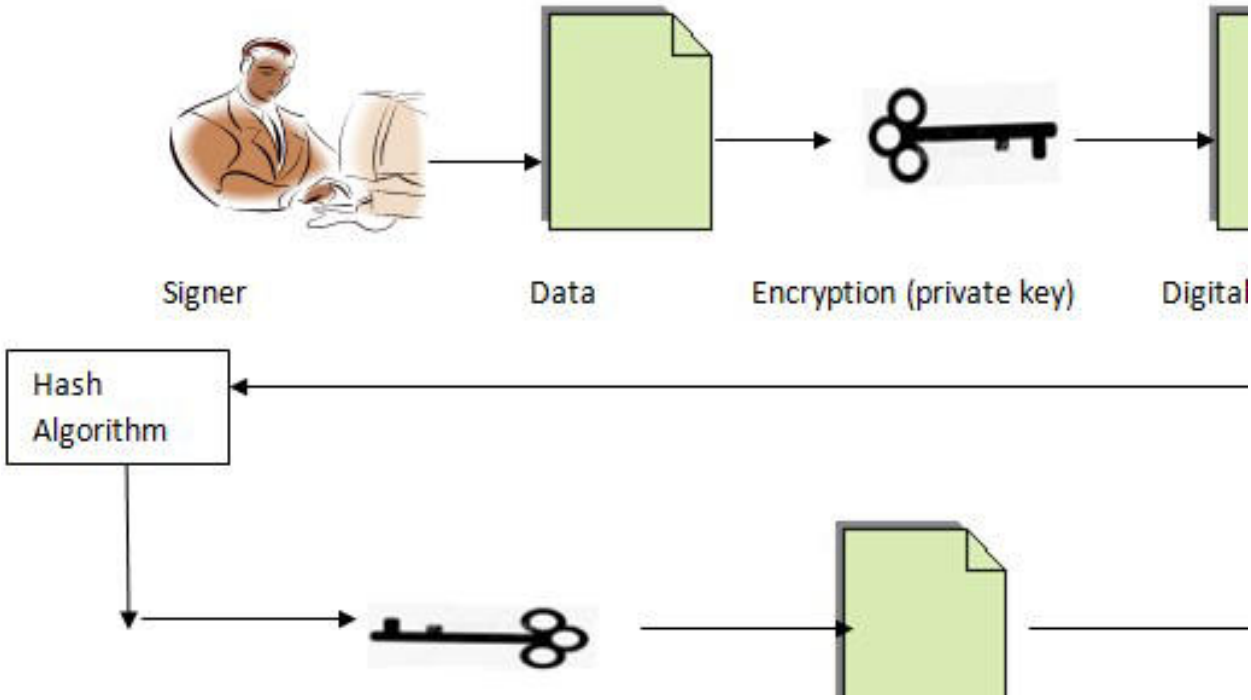


Fig 7.11 Digital signature

Digital signature has two performed in two ways :signing the document or signing a digest of the document. Signing the document probably the easier but sometimes may be consider as less efficient. Signing means document is encrypted it with a private key of the sender and verifying the signed document is decrypting it with the public key of the sender shown in fig 7.11.In digital signature the sender uses its own private key and the receiver uses public key of the sender.

In digital signature normally message are long but it has to use public keys so not to sign the document itself instead sign a digest of the message. The sender can sign the digest and receiver can verify the digest. But it do the same i.e used as message authentication.

A digital signature provides three services in security. A digital signature provides integrity, authentication and message nonrepudiation.

INF2016:

STOP TO CONSIDER
In digital signature use asymmetric keys i.e public and private keys. A digital signature provides three services in security. A digital signature provides integrity, authentication and message nonrepudiation

SAQ
Q2. Explain how digital signature process use for message authentication.

7.5.4 Message Integrity

As already mentioned above that message integrity explained that whatever the original document should not be tempered by other user i.e we have make ensure that original document remains unchanged over the years.The message need to be safe from any tempering by some unauthorized users.

To preserve the integrity of the original message the message passed through an algorithm which is known as hash function where the hash function creates a compressed image of the original message that can be used as a fingerprint as it must be compared on required situation.

7.6Entity authentication

A entity can be a person ,a client ,a server or a process. In entity authentication a technique is designed to let one party proof the original identity of the another party. Here we have claimant and the verifier. The party whose identity need to be proved is called the claimant and the other party that tries to prove the identity of the claimant is called the verifier.

There are some differences between message authentication and entity authentication such as message authentication simply authenticates one message and the same process need to be repeat again for each new message but in entity authentication it authenticates the claimant for the entire duration of a particular session.Again message authentication may not be in real time but entity authentication is in real time etc.

There are three kinds of witnesses can be used in entity authentication such as :something known, processed or inherent. If we see something known than this is a secrete known one and only by the claimant that can be used for verification by the verifier such as password ,a secret key or may be PIN number .In case of something processed ,this is something which can be used to prove the identity such as passport, license of a driver ,creditcard or smart card of a person and if we look something inherent as the name indicates it represent an inherent characteristic of the claimant such as retinal pattern, fingerprints, voice ,handwriting or appearance means facial characteristics etc.

Password

The general and oldest method of entity authentication where a password is used when a particular user needs to access a system to use system's resources, the password is private .In password authentication we have two categories :

- Fixed password and
- One time password

In Fixed password approach the same password is used again and again for every access of the system or services by the user .But in this approach there are some possibilities of attacks such as guessing a password ,stealing a password or accessing a file.

A more secure approach is that instead of the plaintext password the hash of the password should be stored in the password file. In that case other user can read the contents of the file but as it stored using hash which is a one way function ,it almost impossible to guess exact value of the password .

One-Time Password

As name indicates this type of password is used only once. So in this case password stealing, gussing are useless . However, this approach is very complex and not discussed in this chapter.

Challenge-Response

As discussed above we can see that password can be used for entity authentication but it also have some issues. So, now we are discussing another approach which is known as challenge –response .In challenge-response authentication approach, the claimant proves that the user knows a secret without revealing it. Here the claimant does not reveal the secret to the verifier; the verifier either has it or finds it. Here challenge is a time-varying value and sent by the verifier. The claimant applies a function to the challenge and sends the result to the verifier called a response.In response it shows that the claimant knows the secret.

Challenge-response authentication is possible with the use of the several approaches such as using a Symmetric-Key Cipher, using Keyed-Hash Functions, using an Asymmetric-Key Cipher and using Digital Signature.

STOP TO CONSIDER

Password is the most common approach of entity authentication. Fixed password approach has some issues .One time password is more secure than fixed one. Moreover pass word challenge-response approach is also used in entity authentication.

Check your progress
Q9.What are the two categories of password ?
Q10.In entity authentication message is also authenticate.(TRUE/FALSE)

7.7 SUMMING UP

- Security management is basically concerned with monitoring and controlling access to computer networks and access to all or part of the network management information obtained from the different network nodes.
- In network configuration ,the original network configuration or any changes in the network must be recorded. In any kind of reconfiguration documentation is required.
- SMI,SNMP and MIB these three are considered as network management components.
- The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCPI/IP protocol suite which uses UDP Port 161 and 162.
- SNMP has three versions:SNMPv1,SNMPv2 and SNMPv3.
- SNMPv3 has several additional features over SNMPv2.Such as privacy, authentication and access control.
- Network security can address different services related to the message and the entity. Message related services are: privacy or confidentiality, authentication, integrity and availability. Service related to entity is entity authentication or identification.
- In message privacy cryptography is used. Network security mostly achieved through the use of cryptography which means secret writing.
- Two common category of cryptography :Symmetric key cryptography and Asymmetric key cryptography.

- Digital signature use asymmetric key cryptography. A digital signature provides integrity, authentication and message nonrepudiation.
- A entity can be a person ,a client ,a server or a process. In entity authentication a technique is designed to let one party proof the original identity of the another party. Here we have claimant and the verifier.
- Password is the general and old method of entity authentication.

7.8 KEY TERMS

- Fault: A fault is usually indicated by failure to operate correctly or by excessive errors.
- Trap: : SNMP use Trap message .It is sent to the manager from the agent to report an event.
- Manager :A manager is a host that runs the SNMP client program.
- Agent : An Agent is a router that runs the SNMP server program.
- Key: Key are nothing but a number or a set of numbers that the cipher ,as an algorithm operates on.
- PDU:Protocol Data Unit used in SNMP for communication between SNMP Manager and Agent .
- RFC: Request for Comments. A Request for Comments (RFC) is a formal document from the Internet Engineering Task Force (IETF) that is the result of committee drafting and subsequent review by interested parties.

7.9 ANSWER TO CHECK YOUR PROGRESS

A1. hardware reconfiguration, software reconfiguration and user account reconfiguration.

A2.TRUE.

A3.FALSE

A4.32

A5. Privacy, authentication and access control.

A6.Ciphertext.

A7. Whatever encryption and decryption algorithms are used known as ciphers.

A8. Substitution ciphers andTransposition ciphers

A9.Fixed password and one time password.

A10.False

7.10 QUESTION AND ANSWERS:

1.The keys used in cryptography are

a. public key
b. private key

c .secret key

d. all of them

2. Cryptography, a word with Greek origins, means

a.open writing

b.close writing

c.secret writing

d.none of above

3.In symmetric key cryptography----------key is used.(Fill in the blank)

4. The process of transforming ciphertext into readable text.
a. decryption

b. encryption

c. network security

d. information hiding

5.Digital signature use ----------key.(Fill in the blank)

6.A entity can be a

a.server

b.client

c.a person

d.all of them

7.In cryptography encryption is done in ----------site.(Fill in the balnk)

8. In cryptography Decryption is done in ----------site.(Fill in the balnk)

9. SNMPv1 was designed with ---------- bit counter.(Fill in the blank)

10. SNMPv2 was designed with -------.bit counter. .(Fill in the blank)

ANSWERS:1.d.all of them.2.c. secret writing 3.secret key 4.a 5.asymmetric 6.d.all of them 7.sender 8.receiver 9.32 10.64.

Short questions:

1.What do you mean by network management?

2.Mention different versions of SNMP.

3.Menetion services provided by SNMP.

4.why network security is required.

5.What do you mean by message integrity?

6.Define key.

7.What is transposition cipher?

8.Why digital signature technique is required?

9.What do you mean by entity authentication?

10 .What are the different approaches used in challenge response authentication technique?

Long question.

1.Discuss the role of SNMP in network management.

2.What are the different security services,explain in details.

3.Discuss asymmetric –key cryptography.

4.Explain the digital signature method.

5.Discuss how entity authentication is done and why it important.

7.11 SUGGESTED READINGS

- Bhushan Trivedi,Computer networks Oxford higher education.2019
- B.A Forouzan ,Data communications and network McGraw Hill higher education,2016
-