Yashwantrao
Chavan
Maharashtra
Open University

CMP507

Computer
Networks

Computer Networks

Yashwantrao Chavan Maharashtra Open University
Dnyangangotri, Near Gangapur Dam
Nashik-422222

Yashwantrao Chavan Maharashtra Open University

Vice-Chancellor: Prof. E. Vayunandan

SCHOOL OF COMPUTER SCIENCE

Dr. Pramod Khandare Director School of Computer Science Y.C.M.Open University Nashik	**Shri. Madhav Palshikar** Associate Professor School of Computer Science Y.C.M.Open University Nashik	**Dr. P.V. Suresh** Director School of Computer and Information Sciences I.G.N.O.U. New Delhi
Dr. Pundlik Ghodke General Manager R&D, Force Motors Ltd. Pune.	**Dr. Sahebrao Bagal** Principal, Sapkal Engineering College Nashik	**Dr. Madhavi Dharankar** Associate Professor Department of Educational Technology S.N.D.T. Women's University, Mumbai
Dr. Urmila Shrawankar Associate Professor, Department of Computer Science and Engineering G.H. Raisoni College of Engineering Hingana Road, Nagpur	**Dr. Hemant Rajguru** Associate Professor, Academic Service Division Y.C.M.Open University Nashik	**Shri. Ram Thakar** Assistant Professor School Of Continuing Education Y.C.M.Open University Nashik
Mrs. Chetna Kamalskar Assistant Professor School of Science and Technology Y.C.M.Open University, Nashik	**Smt. Shubhangi Desle** Assistant Professor Student Service Division Y.C.M.Open University Nashik	

Writer/s	Editor	Co-ordinator	Director
Prof. Yogesh Pawar Assistant Professor, Sanjivani Polytechnic College, Kopargaon	Prof. Madhav Palshikar Assistant Professor, School of Computer Science, Y.C.M. Open University, Nashik	Ms. Monali R. Borade Academic Co-ordinator School of Computer Science, Y.C.M. Open University, Nashik	**Dr. Pramod Khandare** **Director** School of Computer Science, Y.C.M. Open University, Nashik

Production

Unit No. & Name	Details	Counselling Sessions	Weightage
Unit 1.: **Introduction to Networks**	1.1 Fundamentals of Computer Network- Definition Need of Computer Network, Applications, Component of Computer Network. 1.2 Network Benefits- Sharing Information(File Sharing, E-mail) - Sharing Resources (Printer Sharing, Application Services) - Facilitating Centralized Management-Managing Software, Maintaining the Network, Backing up data 1.3 Computer Network Classifications- Classification of Network by their Geography.- PAN, CAN, LAN, MAN, WAN 1.4 1.4 Classification of Network by their Component Role--Peer-to-Peer Network, Server-Based Network, Types of server	**3**	**10**
Unit 2.: **Network Topologies & Networking Devices**	2.1 Network Topologies - Introduction, Definition, Selection Criteria, Types of Topology- i) Bus ii) Ring iii) Star iv) Mesh v) Tree vi) Hybrid. 2.2 Network Control / Connecting Devices - Need of Network Control devices, Role of Network Control devices in a Network, Connectors, Hub, Repeater, Bridges, Switches, Router, Gateway, Modem. 2.3 Network software: NIC Device Driver, client-server software e.g. DHCP, TELNET, FTP	**3**	**5**
Unit 3.: **Transmission Media**	3.1 Need of Transmission Media, Selection Criteria. 3.2 Types of Transmission Media- 1) Guided Media: Cable Characteristics, Types of Cable- Twisted Pair Cable, Co-axial Cable, Fibre Optic Cable. 2) Unguided media: Types of Communication Band-Microwave Communication, Radio wave 3.3 Communication, Satellite Communication, Infrared Communication. 3.4 Latest Technologies in Wireless Network- Bluetooth Architecture, Wi-Fi, Wi- Max. 3.5 Cellular (Mobile) Telephone – Band in Cellular Telephony, Calls using Mobile Phones, Transmitting receiving / Handoff operations.	**3**	**10**
Unit 4.: **Network**	4.1 Layered Architecture	**3**	**10**

Unit No. & Name	Details	Counselling Sessions	Weightage
Architecture and Protocols	4.2 Peer-to- Peer Processes Interfaces between Layer, Organization of the Layers 4.3 Protocols 4.4 Encapsulation.		
Unit 5.: **OSI Reference Model**	5.1 Layers of the OSI Reference Model 5.2 Physical Layer, Data-Link Layer, 5.3 Network Layer, Transport Layer, 5.4 Session Layer, Presentation Layer, Application Layer	**5**	**15**
Unit 6.: **TCP / IP Suite**	6.1 Introduction –Addressing mechanism in the Internet 6.2 IP Addressing – IP Address classes, classless IP addressing, Subnetting, supernetting, Masking, 6.3 Layered Structure of the TCP / IP Model – Host-to-Network, Internet, Transport, Application 6.4 TCP / IP Protocol Suite: Host-to-Network-SLIP and PPP, Internet Layer-ARP, RARP and IP: Introduction, IPv4, IPv6 (Header Format), Difference between IPv4 & IPv6. 6.5 Transport Layer- TCP and UDP (Frame Format, port addresses), Application Layer- FTP, SMTP, DNS. 6.6 Comparison between OSI and TCP/IP Network Model 6.7	**3**	**10**
Unit 7.: **Computer Security**	7.1 Introduction to Computer Security, Need for security, 7.2 Security basics: Confidentiality, Integrity, Availability, Accountability, Non-repudiation. 7.3 Threats to Security: Viruses (its types) and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare Avenues of attack, Steps in attack 7.4 Security Attacks: Active and Passive attacks (Types of attack) 7.5 Password Management 7.6 Role of people in Security: Do’s and Don’ts	**3**	**10**
Unit 8.: **Cryptograph**	8.1 Introduction: Cryptography, Cryptanalysis, Cryptology.	**3**	**10**

Unit No. & Name	Details	Counselling Sessions	Weightage
y & Network Security	8.2 Cryptography Techniques: 8.2.1 Substitution techniques: Caesar's cipher, monoalphabetic and polyalphabetic, one-time pad. 8.2.2 Transposition techniques – Rail fence technique, simple columnar. 8.3 Hashing – concept 8.4 Firewalls: Introduction, Why Firewall, features, advantages and disadvantages. Types of Firewall. 8.5 Virtual Private Network work 8.6 Security topologies: security zones, DMZ, Internet, Intranet, VLAN. 8.7 Intrusion Detection: Intrusion detection systems (IDS), host based IDS, network based IDS		
	Examples with revision	**4**	**0**
		30	**80**

Course Structure:

Course Code	Course Name	Theory/ Practical/ Project	Contact (HRS)	Credit Points	Assessment Type	Passing Marks
CMP506	Computer Network	Theory	60	4	CA(20) + EE(32/80)	40/100

Course Outcome:

- Understand concepts of network, classify types of networks & benefits of networks.
- Understand, compare and implement different types of Topology using Network Control Devices.
- Compare different types of network devices.
- Understand and use different types of communication media.
- Understand OSI reference model and working of its different layers
- Understand functioning of different Layers of TCP/IP protocol suite and its configuration.
- Understand importance of Computer Security
- Understand CIA model and identify various risks and threats.
- Understand types of security attacks
- Understand role of people in security
- Understand cryptographic techniques
- Understand Firewalls and its types, VPN and intrusion detection system and its types.

Course Introduction

The future of computer technology is in computer networks. Global connectivity can be achieved through computer networks. It is important to understand the function of computer networks. Knowledge about hardware and software requirements of networks is essential. The emphasis of the course is towards the various components and software required to make a network operational. The world in the information era has become network centric. A Computer networks has been growing with rapid technological progress. Computer communication through networking becomes essential part of our life. We can manage many application like Air Line Reservation, Railway Reservation, E-banking, E-Governance, On-Line shopping, E-learning etc. by clicking mouse button from our own place. Because of this, world become the global village. By considering importance of networking towards all aspects of our life, we here introduce basic concept of networks, network classification, network topologies, network devices, Transmission media, Network reference models, concept of TCP/IP.

This knowledge explores the student for understanding current network management technology.

Computer security is not just a science but also an art. It is an art because no system can be considered secure without first examining how it is to be used. The definition of a "secure computer" necessitates a statement of requirements and an expression of those requirements in the form of authorized actions and authorized users. Its theory is based on mathematical constructions, analyses and proofs. Its systems are built following the accepted practices of engineering. It uses inductive and deductive reasoning to examine the security of systems from key axioms and to discover underlying principles. These scientific principles can then be applied to untraditional situations and new theories, policies, and mechanisms. Computer security is one of the most important and relevant area of computing today. The requirement to address security in computer system design is an important design consideration in many of today's systems. It is essential to understand various threats to secure computing and the basic security design principles and techniques developed to address these threats. The student will achieve a firm intuition about what computer security means, be able to recognize potential threats to confidentiality, integrity and availability.

This course will introduce basic cryptography, fundamentals of computer/network security, Risks faced by computers and networks, security mechanisms, operating system security, secure System design principles, and network security principles. It will develop knowledge for security of information and information systems within organizations. It focuses on concepts and method associated with planning, managing, and auditing security at all levels including networks.

Unit1: Introduction to Networks

1.1 Learning Objectives: After successful completion of this unit, you will be able to:

- Individually understand basics of computer network technology.
- Understand the need for computer networks
- Understand various applications of computer network
- Understand the use of different components of computer network
- Understand different network benefits
- Understand different classifications of computer network
- Classify the network by its components and roles

1.2 **Introduction to Computer Networks:** The combining of computers and communications has a great impact on the way computer systems are organized. The old model of standalone computers working for the whole organizations need has been replaced by one in which the large no of separate but interconnected computers does the job. These interconnected systems are called as a computer network. Now a days the Computer Networks have changed the way of business and the other daily business works. Today most of the Governmental Organizations, Business Enterprises, Educational Institutions and individuals rely on computer networks and internetwork.

1.2.1 **Fundamentals of Computer Network (Definition):** Communication is the process in which two or more computers or other devices transfer's data and instructions, share information and resources.

A group of two of more computers that shares services and interacting in some manner is known as Computer Network. This interaction is, accomplished through a shared communication link, with the shared components being data. A network is a collection of machines those are linked both physically and through software components to facilitate communication and the sharing of information. A network is a set of devices often mentioned as nodes connected by media link. A node can be a device which is able to send or receive data generated by other nodes on the network, for e.g. a computer, printer etc. These links connecting the devices are called Communication channels.

A computer network is a communication channel used to share data or information. It is also called data network. The best example of the computer network is Internet. A computer network can be two or more inter-connected computers. Figure 1.1 shows an example of a computer network comprising a local area network or LAN connecting computers and various devices with each other.

A physical pathway is known as the transmission medium, that connects the systems and a set of rules determines how they communicate. These rules are known as protocols. A network protocol is a software installed on a machine that determines the agreed upon set of rules for two or more machine to communicate with each other.

Networks are widely used by companies or on a personal level also. Network for companies should provide high reliability, cost efficient, and resource sharing.

A network must be able to meet certain criteria, these are mentioned below:

- Performance
- Reliability
- Scalability

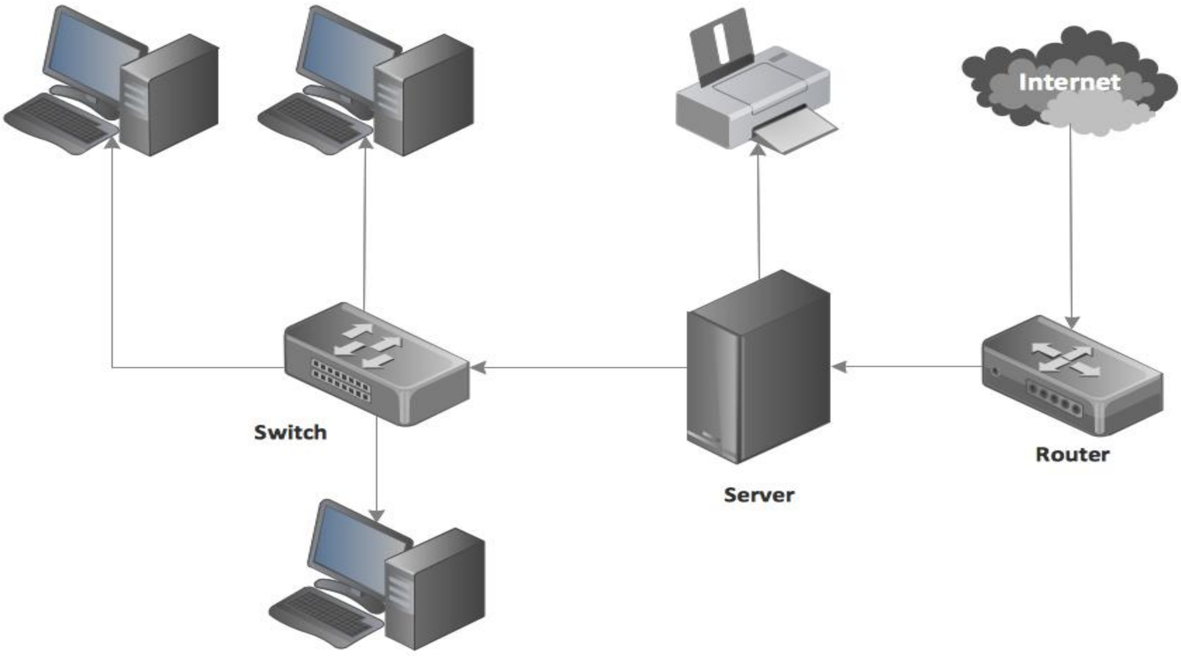


Figure 1.1 Computer Network

1.2.2 **Need of Computer Network:**Today no one can imagine the world without emails, online newspapers, blogs, chat and the other services those are offered by the internet. Computer networks support users on the network to share the information, services, and information.

Computer Network benefits in:

- Cost reduction by sharing hard- and software resources
- High reliability by having multiple sources of supply
- Cost reduction by downsizing to microcomputer-based networks instead of using mainframes
- Greater flexibility because of possibility to connect devices from various vendors

Networking increases efficiency and reduces costs. These goals can be achieved in three primary ways:

- Sharing information (or data)
- Sharing hardware and software
- Centralizing administration and support.

The following are the potential needs and benefits of a computer network:

- **File Sharing:** Networking helps the network users to share data files. Computers connected to a network share files and documents with each other. Personal computers connected to a business network can select to which files and folders should be made available to be shared in the network.
- **Information Sharing:** Computers connected to a network are capable of sharing and exchanging data and information between different individual users, it is necessary to interconnect the individual users' computers.
- **Resource Sharing:** When computers are interconnected, users connected to the network can share the expensive resources like a laser printer, bulk storage, and large enterprise software.
- **File Sharing:** Computers connected to a network share files and documents with each other. Personal computers connected to a business network can select which files and folders to be made available to share within the network.
- **Sharing Media:** In computer network sharing media is very easy. Similar to file sharing, computers are capable of streaming music, videos and movies from one computer to another.

1.2.3 **Applications of Computer Network:** Computer network is a collection of computing devices interconnected to achieve communication and to share available resources. The Network is comprised of software and hardware devices. Computer networks support to transfer files from one place to another and to communicate in possible shortest time.

Computer network applications are software applications those utilize Internet or other network hardware infrastructure to execute important functions like file transfer within a network. It helps to transfer data from one point to another within a network.

There are two types of network applications:-

a. Pure network applications
b. Standalone network application

a. **Pure Network Applications:** These applications are developed only to use in networks. These applications help in the transfer of data and to communicate within a network. These applications have a separate and distinct user interface.

Some examples are as:

- **Email programs:** allows users to write messages on their computers and then send to someone within the network. Examples of electronic mail are:
    - Gmail
    - Outlook express
    - Rediffmail
    - Fox mail
    - Opera
    - Poco mail

- **File transfer protocol (FTP):** An application that facilitates the transfer of files from one computer to another e.g. from a client to a server. There are two common processes involved in FTP
    - **Downloading**: It is the process of getting files from a server to a local computer or a client (for example when you download programs and music from a server).
    - **Uploading**: It is the process ofgetting of files transferred from a local computer or a client to a server (for example attaching and uploadingof documents to a server).
- **TELNET:** An application that allows a local computer or a client to access the server for an application program. TELNET enables to control the server and communicate with other servers on the network.
- **Groupware:** Applications those are used for atomization of the administrative functions of a modern office for example video conferencing and chatting. They facilitate the work of groups and improve their productivity.

b. **Stand Alone Applications**: These are the applications those run on standalone computers. To enhance their activity, these programs are rebuilding to run on network environments. For e.g. word processors, database management systems, spreadsheets,graphicspresentations, project management etc. They function even when the computer is offline.

Besides these applications are also categorized on the basis of their place of usage like:

- Business:
- Banking:
- Insurance:
- Education:
- Marketing:
- Health Care:
- Engineering Design:
- Military:
- Communication:

- Government:

1.2.4 **Components of Computer Network:**Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other hardware and software resources, network interface card(NIC), a local operating system(LOS), and the network operating system (NOS). Computer network components consists of the mainparts those are required to install a network mutuallyat the office and home level.Computer network components include cable, Hub, Switch, NIC (network interface card), modem and router. Depending on the type of network some of the components can be eliminated. For example, wireless network cables and hubs are not needed.

Essential Components for Computer Networks are:

- Network Interface Card (NIC)
- Hub
- Switches
- Cables and connectors
- Crimping Tool
- LAN tester
- Router
- Modem
- Bridge

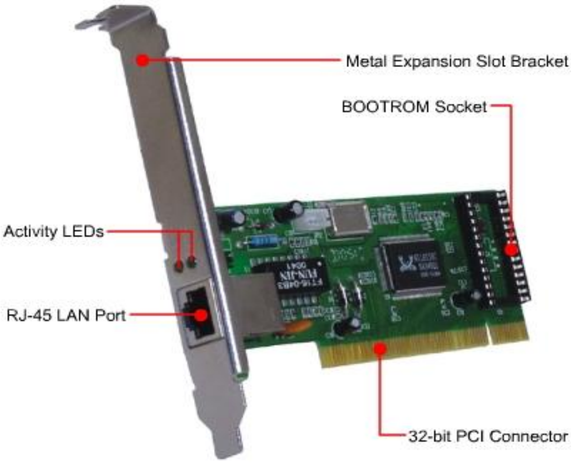


Figure 1.2: Network Interface Card

Network Interface Card (NIC): It is a hardware component that connects a computer to a computer network. It is also known as **network interface controller, network adapter, LAN adapter**. Now a day's almost all computers have built-in NIC, i.e. functionality of NIC is available on the motherboard directly.

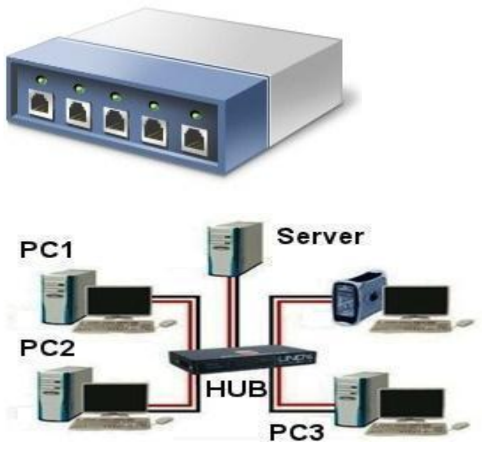


Figure 1.3: HUB

HUB: Hub is a device used todividea network connection into severalcomputers. It is a distribution center. Hubs are generally used to connect segments of a LAN. A hub contains multiple ports. When a packet reaches at the port, it is transmitted to the other ports hence all segments in the LAN can see all packets.

Switches: A network switch is a networking device that is used to link network devices. The switch is like a Hub but built in with advanced features. It uses MAC addresses of each incoming messages so that it couldtransmit the message to the right destination or port.

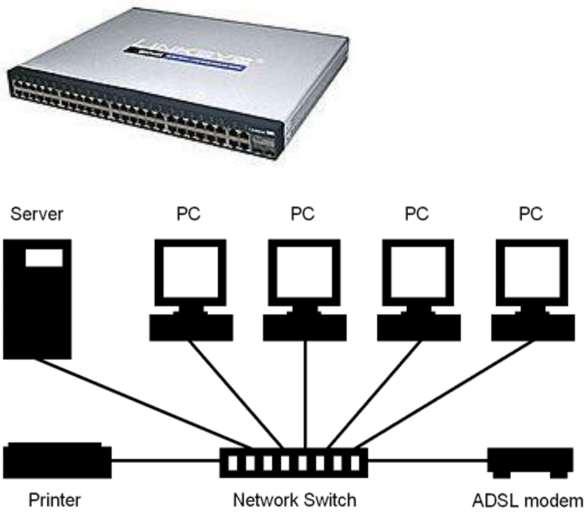


Figure 1.4: Network Switch

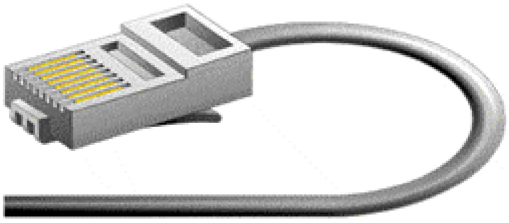


Figure 1.5 Cables & Connectors

RJ = Registered Jack

Cables & Connectors: Cable is unidirectional way of transmission media that is used transmit communication signals. The wired network typology uses a special type of cable to connect computers on a network.

There are several types of cables as below:

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Unshielded Twisted Pair (UTP) Cable

RJ – 45 connectors are used for networking.

RJ-45 Connector = Category 5 (CAT5) Connector = 8 position 8 Contact Connector (8 Pin)

Crimping Tool: A crimping tool is a tool that is designed to crimp or connect a connector to the end of a cable.

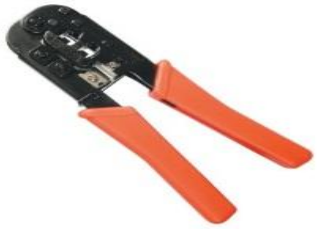


Figure 1.6: Crimping Tool

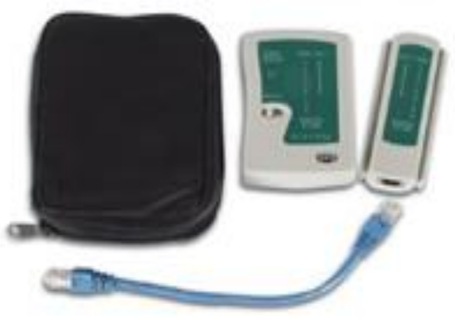


Figure 1.7: LAN Tester

LAN Tester: T*esters* assist in the installation and control of networks. LAN testers are able to determine IP addresses,connected port, identify polarity, and link connectivity. Even they can test fiber optic cables. They also show cable break points, incorrect connections in fiber optic lines.

Router: Router is a networking device that forwards data from one network to another. It forwards data packets between computer networks, creating an overlay internetwork. A router is used to connect two or more connections from different networks. When a data packet arrives in one of the lines, the router examines the address info in the packet to determine its ultimate destination.

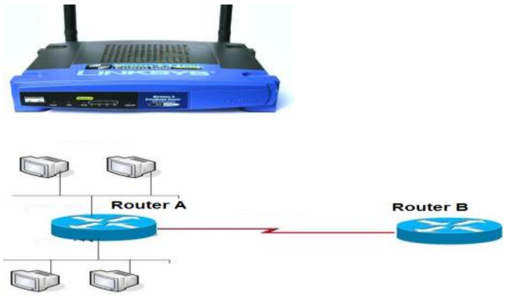
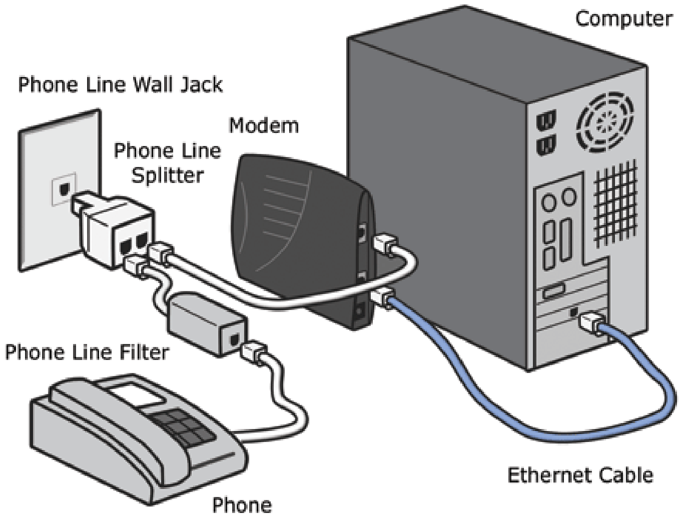


Figure 1.8: Router



Modem: It is a device that enables computers to transfer data from one location to another location via the telephone line. It **mod**ulates the (converts) digital signal to analog at the transmission end and **dem**odulates (converts/ reverts) analog signal to digital signal.

Bridge: It is a device that connects two parts of a network together at the data link layer (layer 2 of the OSI model). Bridges work like the network switches, but the traffic is controlledotherwise. A bridge only transmits traffic from one side to the other side if it is going to a destination. This is unliketo a layer 1 switch thattransmits all

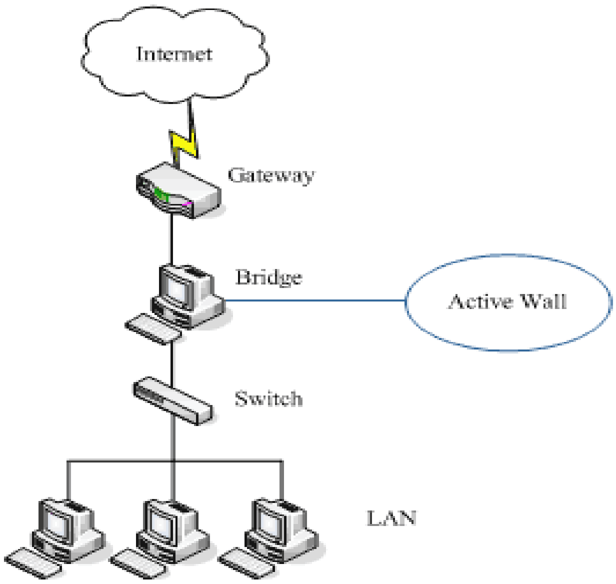


Figure 1.10: Bridge

traffic from either side. Sometimes network bridges are called layer 2 switches.

Self-Test (Multiple Choice Questions):

1. A network consists of what minimum number of entities sharing resources and information?

   a. One b. Two c. Three d. Ten
2. Which of the following is required before a computer network is present?

   a. Two or more computing devices b. Connections between devices c. Electronic resources and information to share d. All of the above
3. A network must be able to meet which of the following certain criteria?

   a. Performance b. Reliability c. Scalability d. all of above

Self-test question:

1. Fill in the blanks.
   a. A Network is a group of two or more computer system sharing ………
2. Define Computer Network. Describe fundamentals of a computer network in brief.
3. Describe the needs of Computer Networks in brief?
4. What are the applications of Computer Network?
5. Enlist different network component. Explain any four components.

1.3 Network Benefits:

1.3.1 **Sharing Information (File Sharing, E-mail):**Networks allow users to share information in various ways. The most conventionalway of sharing information is to share specificfiles. For example, many people can work together on a single document like spreadsheet file or word-processing. In most of the networks, a large hard diskis set up on a central server computer as a sharedstorage area where users can store files to be shared.

Networking benefit is not only sharing files, but also it allow various users to communicate with each other. For example, messaging applications like emailallows the network users to exchange messages within each other. Users can hold online video conference meetings over the network, with cheapvideo cameras and the right software.

1.3.2 **Sharing Resources (Printer Sharing, Application Services):**Certain computer resources, such as printers or hard drives, can be set up so that network users can share them. Sharing these resources can result in significant cost savings. For example, it isworth cheaper to purchase a single good-speed printer with higherfeatures whichmay be shared by awholeworkgroup rather to buy separate printers for individual user in the group.

Hard drives can also be shared resources .It is the most common method ofsharing files on a network by givingusers with access to a shared hard drive. A computer which is meant for the purpose to host shared hard drives is called a file server.

Actually, the entire hard disksare not usually shared,ratherseparate folders on a networked hard drive are shared. This is the way using which the network administrator allows different network users to have access to different shared folders. For example, a company may share folders for its sales department and accounting department. Sales personnel may access the sales department’s folder, as well as the accounting department’s folder.

Other resources can also be shared on a network. For example,to share the Internet connection a network can be used. In the initialdays of the Internet, it was normalfor every user who neededaccess to the Internet was required to have his or her own modem connection. Today, it is general for the network to offera shared and high-speed Internet connection so that everyone on a network can access Internet.

1.3.3 **Facilitating Centralized Management:** One of the most common reasons for networking in many businesses is so that several users can work together on a single business application. For example, an accounting department may have accounting software that can be used from several computers at the same time, or a sales handlingdivisionmay have an order recordapplication which runs on different computers to managea large volume of orders.

Networks are used to assist in management tasks associated with their own operation and maintenance. Using networks results in increased efficiency and a resultant reduction in maintenance costs. The software can be installed at a central location using servers, where the installation files are made accessible over the network.

1.3.4 **Managing Software:**Using the network helped in reduction of software costs. It happens when all users on a network used the same software and when software is bought in bulk quantities gets a discount. Centralizing the installation of software also reduces operational costs sincemost installations can be accomplished remotely, within the network. The computer programs that are needed to perform the installations are stored on servers and are made accessible in the network. The maintenance personnel simply logs on from a client computer and install the needed applications using the installation software stored on the server. In the past few years, more savings have been accomplishedby having the centralized server initiate the software installations or updates on the client computers without the need for maintenance personnel to actually visit any of the clients.

1.3.5 **Maintaining the Network:** Purchasing similar equipment for use on the network means that network maintenance costs are reduced because there are fewer dissimilar components. Maintenance workers no longer have to attend numerous training sessions on many different components, which meant they could spend more time maintaining the actual components.

1.3.6 **Backing up data:**Along those same lines, a network minimizes the time spent backing up (saving extra copies, called backups) of necessary files. If a hardware or software failure causes information or applications lost, vital information and necessary applications can be restored with the help of existing backup. The backup process is normally a regular activity in a company, and all transactions between scheduled backups are recorded so that the files can be restored as completely as possible. Technicians can access the backup files and recorded transactions from a central location without having to physically visit the source computers.

Self-test question:

1. What are the benefits of Computer Network? Explain any two.

1.4 Computer Network Classifications:

Networks areclassifiedby using one or more technical or functionalproperties likethe type of technology used or number of users and devices it connects. One basicproperty used to classify networks is its geographic area, where a network is categorized on thebasis of the physical area covered by it.The five basic types of networks in terms of geographical area from the smallest to thelargest are:

- **Personal Area Networks (PAN)**
- **Local Area Networks (LAN)**
- **Campus Area Networks (CAN)**
- **Metropolitan Area Networks (MAN)**
- **Wide Area Networks (WAN)**

1.4.1 **Personal Area Networks** (PAN): PAN cover the areas related with specific workspaces like a home office or an office workspace. Within PAN,an individual network connecting two or more devices may be facilitated using wireless technologies, as shown in Figure 1.11. PAN is a personal network equipped within a limited area. PAN consists of mobile devices like cell phone, tablet, and laptop. Such network can also be wirelessly connected to the Internet. PAN handles the interconnection of networking devices nearby of a single user. Usually, PAN contains appliances likewirelessmouse and keyboards, wireless phone, Bluetooth.

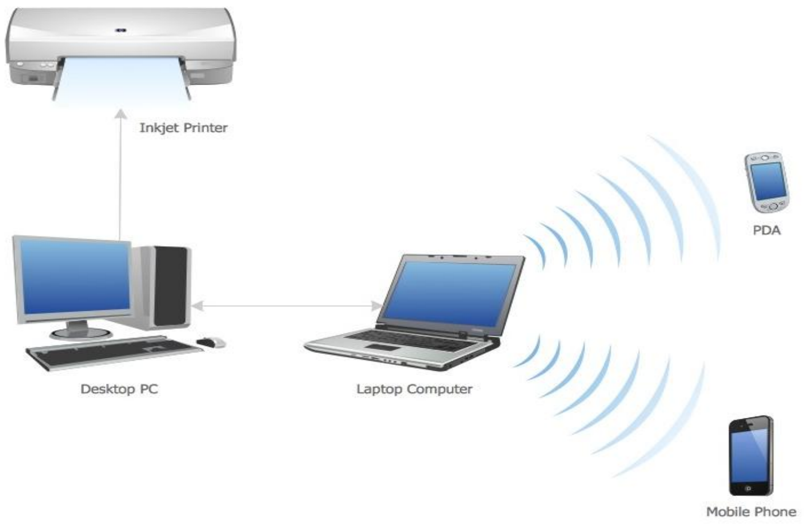


Figure 1.11: Personal Area Networks (PAN)

Advantages:

- **Portable:** Since it is a portable type of network, if a person is traveling he can carry his portable devices such as laptops, mobile phones, personal digital assistant and etc. So it is possible for him to establish his network wherever he wishes without using any wire, only by using wireless technology.
- **Security:** Since the information stored in the devices is shared with only authorized peoples within the network. Hence it is secure to transfer information between devices.
- PAN is expedient, lucrative and handy.

Disadvantages:

- **Health Issue:** Since most devices used for communication are wireless, use microwave signals as a medium for communication. Working for a long time within this signals radius may lead to some brain and heart-related problems.
- **Expensive:** Since expensive devices like smartphones, laptops, Digi camera, PDA and etc. are used.
- Sometimes has a bad connection to other networks at the same radio bands.
- Bluetooth networks have slow data transfer speed, but comparatively safe.
- Bluetooth has distance limits.

1.4.2 **Local Area Networks (LAN):** LAN cover the limited geographical area like some or complete space within a building and usually owned and maintained by a single organization. LAN is mostly used to connect PC’s and workstations at home, in company offices and factories, to share resources and information. They are classified as other types of the network by their size, transmission technology, and topology. Since are relatively small in size, network management is relatively easy, and LAN generally has high data rates, fewer propagation delays, and low error rates. Multiple computers and other networking devices are connected to the devices like switches, servers to form a LAN. Single LAN can serve a single department, several workgroups, or all users within that building. Cable or wireless or a combination of both can be used to connectnetworking deviceson a LAN, as shown in Figure 1.12

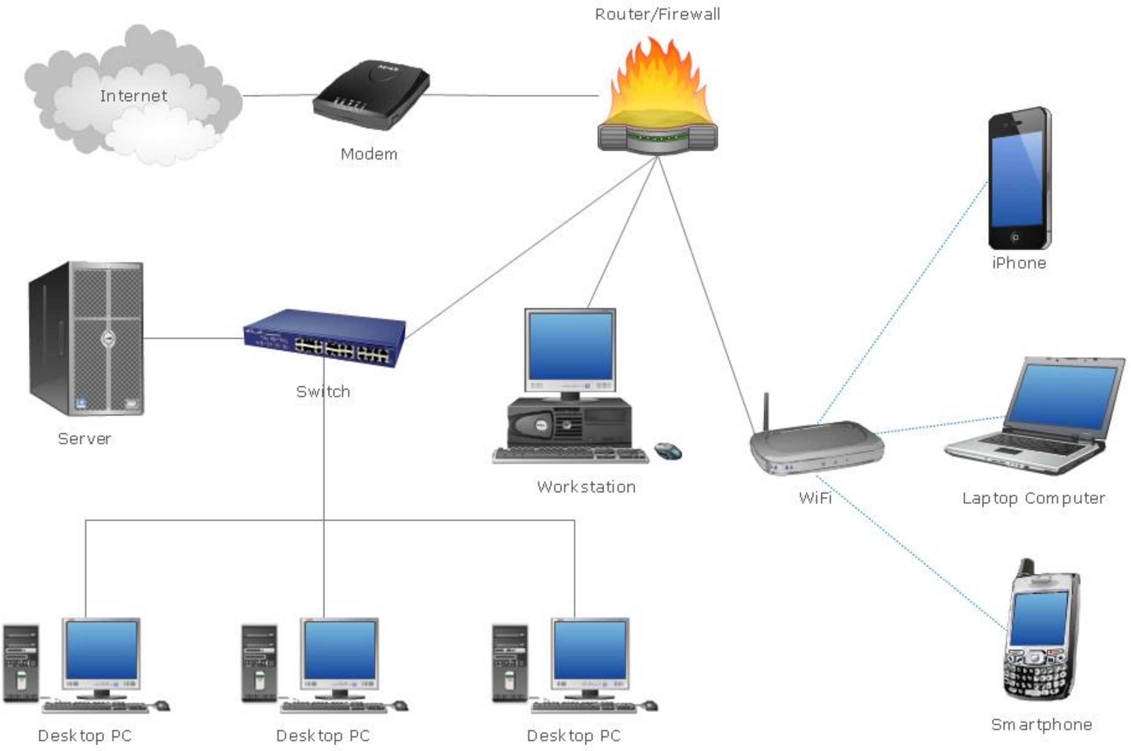


Figure 1.12: Local Area Networks (LAN)

Advantages:

- **Resource Sharing:**Resources like printers, modems, hard disks and etc. can be shared within the local area networks. It helps in reduction of hardware purchasing cost.
- **Software Applications Sharing:**Same software can be used within the network rather purchasing separate licensed copy for every client in the network.
- **Easy and Cheap Communication:**Information can easily be transmittedto the networked computers.
- **Centralized Data:**All network users can save their datacentrally on a hard disk of the server computer.Users can access their files from any workstation.
- **Data Security:**As data is centrally stored on a server, it is easy to manage data at only one place and which makes the data more secure.

- **Internet Sharing:**Single internet connection is shared within LAN keeps the internet expenses cheaper.

Disadvantages:

- **High Setup Cost:**Initial setup cost of installing Local Area Networks is very high.
- **Privacy Violations:**Since LAN administrator has rights to check personal data, he can check the personal use history of the LAN users.
- **Data Security Threat:**If the centralized database is not secured properly by the LAN administrator any unauthorized user can access the importantdata of an organization.
- **Slow Internet Speed:** Since single internet connection is shared and if all computers will run at once, lead to slow internet speed for each
- **LAN Maintenance Job:**Since Local Area Network requires a LAN Administrator. Full-time LAN Administrator is needed.
- **Covers Limited Area:**Local Area Network covers very small area like one office or one building.

1.4.3 **Campus Area Networks (CAN):**Campus Area Network is an interconnection of localarea networks within a limited geographical space, like a school campus or a military base. CANs are formed by connecting the LANs situated in two or more buildings those are mostly close to each other, as shown in Figure 1.13. Connections between the buildings can be done using cables or wireless devices. Term campus LAN is used to describe CAN. CAN is one of the types of MAN but the area is smaller than MAN.

Generallythe CAN usesvarious LAN technologies like Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), Fast Ethernet, Gigabit Ethernet, and Asynchronous Transfer Mode (ATM).

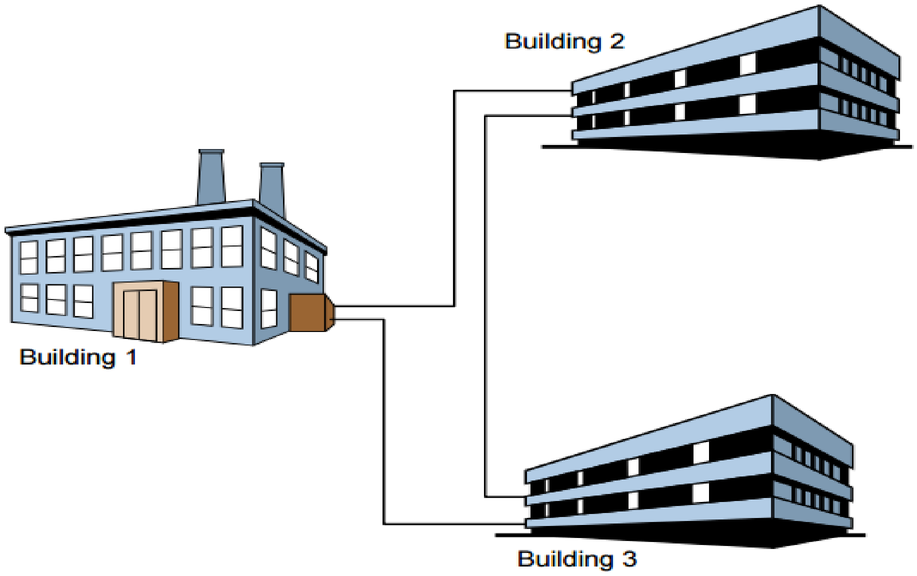


Figure 1.13: Campus Area Networks (CAN)

1.4.4 **Metropolitan Area Networks (MAN):**It is a network that is used to connect computers in a larger geographic area than that is covered by a CAN but smaller than the area that is covered by a WAN. MANs are formed by connecting the networks located at two or more sites within the same city. Connections are done by using cables or wireless technologies, often optical fibercabling is used to connect networks to thefacility provided by a telecomm service provider, as shown in Figure 1.14. MANs are generallydescribedby very high-speed connections using fiber optical cable or other digital media.

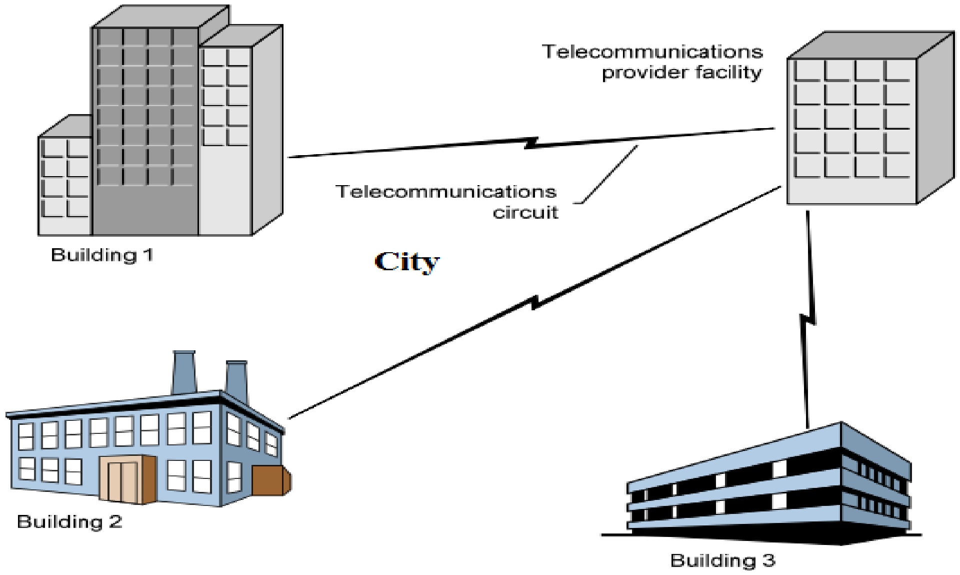

Telecommunications provider facility
Telecommunications circuit
Building 1
City
Building 2
Building 3

Figure 1.14: Metropolitan Area Networks (MAN)

1.4.5 **Wide Area Networks (WAN):** A computer network that covers a relatively large geographical area. WAN connects various small networks that includes local area networks (LANs) and metro area networks (MANs). Computers are connected through public networks to a WAN, for examplepublic telephone system. WAN can also be connected via leased lines or satellites. An example of largest WAN is the Internet.

WANs are created by linking the networks located at two or more sites over geographic distances that extend beyond the span of a single metropolitan area. These include links between cities, countries, and in the case of global WANs, continents. Telecommunications circuits link each building to facilities operated by a telecommunications provider (same as MANs), as shown in Figure 1.15. WAN works similarly like a LAN, on a greater scale. TCP/IP is the protocol used for a WAN in combination with devices such as routers, switches, firewalls, and modems.

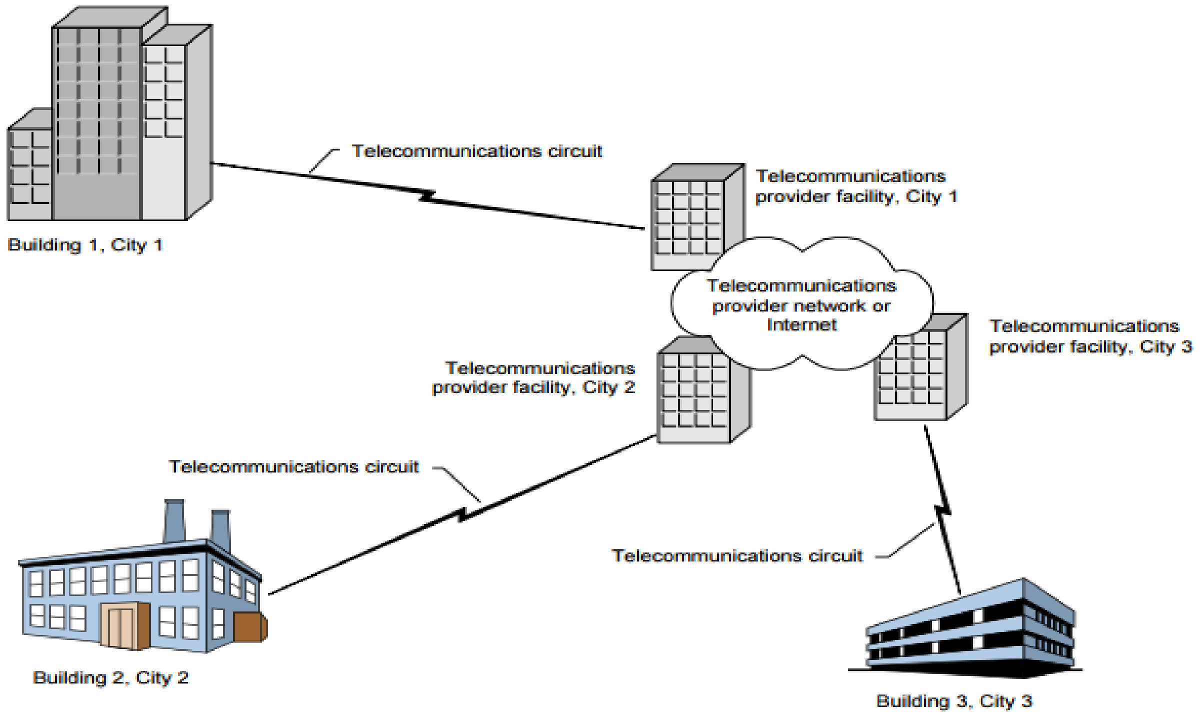

Telecommunications circuit
Building 1, City 1
Telecommunications provider facility, City 1
Telecommunications provider network or Internet
Telecommunications provider facility, City 3
Telecommunications provider facility, City 2
Telecommunications circuit
Telecommunications circuit
Building 2, City 2
Building 3, City 3

Figure 1.15: Wide Area Networks (WAN)

Self-Test (Multiple Choice Questions)

Self-test question

1. List different types of networks?
2. Fill in the definitions for the following Network scaleterms,
   - Personal Area Network (PAN)
   - Local Area Network (LAN)
   - Campus Area Network (CAN)
   - Metropolitan Area Network (MAN)
3. File in the blanks
   a. LAN run at speed of ………………… Mbps
   b. …………………………… is basically a bigger version of LAN
   c. Internetworks are form when no. of network connected through………………………… and ……………………….
4. Match the following

a. MAN	a. Wide Area Network
b. LAN	b. Metropolitan area network
c. WAN	c. 10 to 100 Mbps

1.5 **Classification of Network by their Component:** Computer Networks are also classified on basis of the roles that networked computers play in the network's operation, and more specifically on which computer controls that operation. Networks can be classified on the basis of role in two basic types:

- Peer-to-Peer Networks
- Server-Based Networks

The basis of difference between these two is that, which computer is Incharge of the network. A third classification, client-based networks, has come into existence because of the increased capabilities of the typical client computer

1.5.1 **Peer-to-Peer Network:**Peer-to-peer networks have no centralized control.A peer is considered an equal. All computers on a peer-to-peer network can be considered equals, as shown in Figure 1.16. That is to say, no one computer is in charge of the network's operation. Each computer controls its own information and is capable of functioning as either a client or a server depending on which is needed at the time.

Peer-to-peer networks are very popular since they are inexpensive and easy to install are used inhome networks and in small companies. Many operating systems comes with built in peer-to-peer networking capability. The only other cost involved with setting up a peer-to-peer network comes into play if a computer does not have a network interface card, or NIC (the device that physically connects your computer to your network's cabling), already installed.

Typical initial peer-to-peer networking involves no security measures. Rather, each peer simply shares its resources and allows others open access to them. Actually, a peer-to-peer network is difficult to manage if more and more security is given to the resources. This is because users control their own security by adding password protection to each share they create. Shares are any resources users control on their computers, such as document folders, printers, and other peripherals. Each shared resource can actually have its own password. Someone wanting access to numerous shared resources has to remember many passwords. Security on a peer-to-peer network can quickly become complex and confusing.

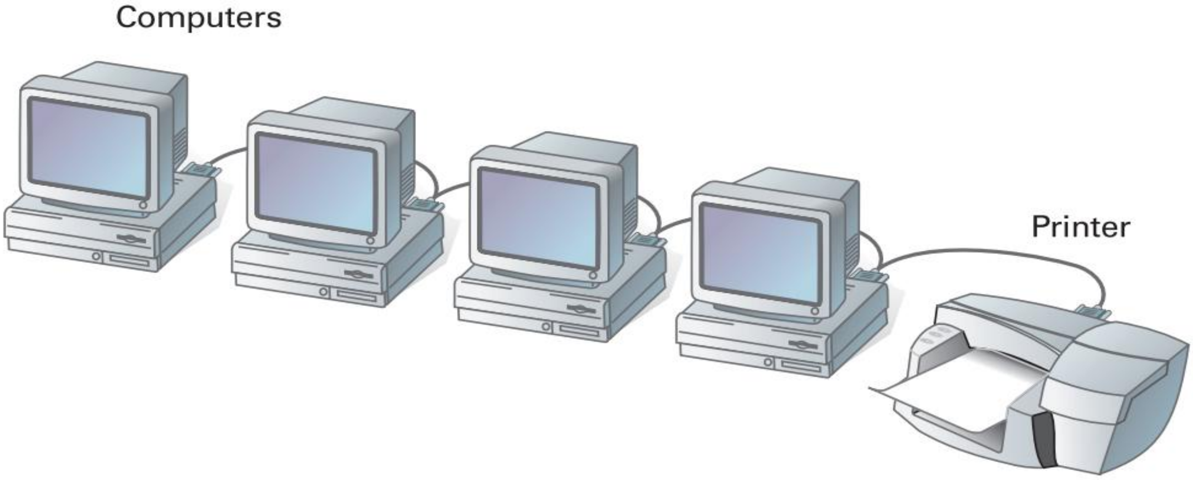


Figure 1.16: A peer-to-peer network.

While peer-to-peer networks are inexpensive to set up, they are extremely limited in scope. The maximum number of peers that can be accepted to operate on a peer-to-peer network is ten. They are, therefore, not appropriate for larger, more secure networks.

1.5.2 **Server-Based Network:**Server-based networks involve centralized control. A server-based network provides centralized control and is createdfor secure operations, as shown in Figure 1.17. Although there are both clients and servers on a server-based network, network is controlled by a dedicated server.

A dedicated server is one that, operates solely as a server for all practical purposes. In a server-based network,a dedicated server serves its network clients by storing data, applications, and other resources, and then provides access to those resources when called for by a client. When a client requests for a resource such as a document, the server transmits the document over the network to the client.When it is processed it is returned to the server for continued storage.

Dedicated servers can also control the entire network’s security from one central location or share that control with other specially configured servers. This central network control gives contribution to the financial systemof scale briefedin the “Facilitating Centralized Management” section earlier in this chapter and makes the server-based network the leadingnetworking model that is used in networks today.

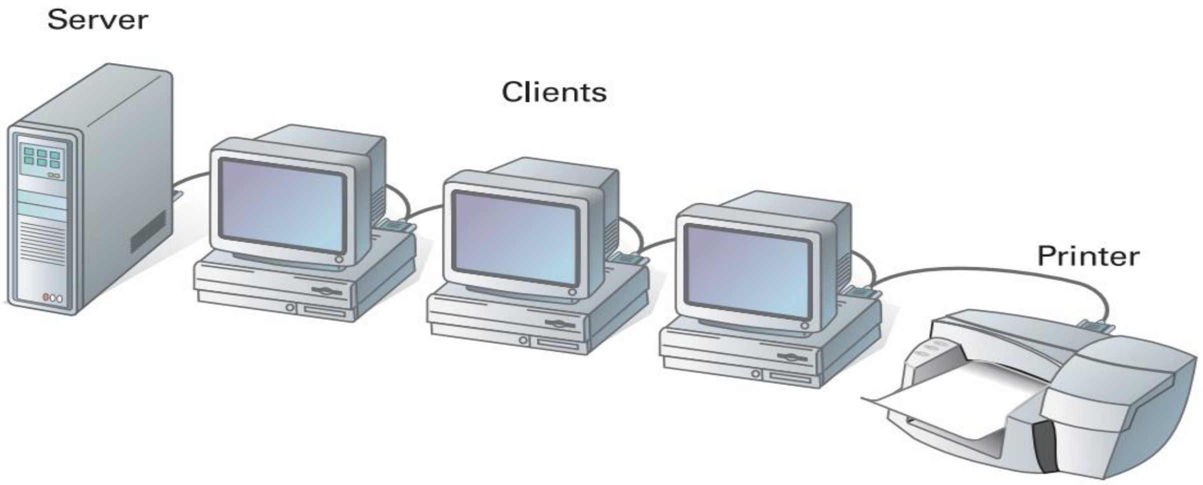


Figure 3.17: A server-based network

1.5.3 **Types of server:** Client-based networks are a further refinement of the concept of a serverbased network that relieves the heavy burden on the network's capacity resulting from frequent server-performed transactions. A client-based network takes better advantage of the server's powerful processors and of the increasingly powerful computers used in typical workstations. Client-based networks, therefore, take advantage of the powerful processing capabilities of both the client and the server, as shown in Figure 1.18.

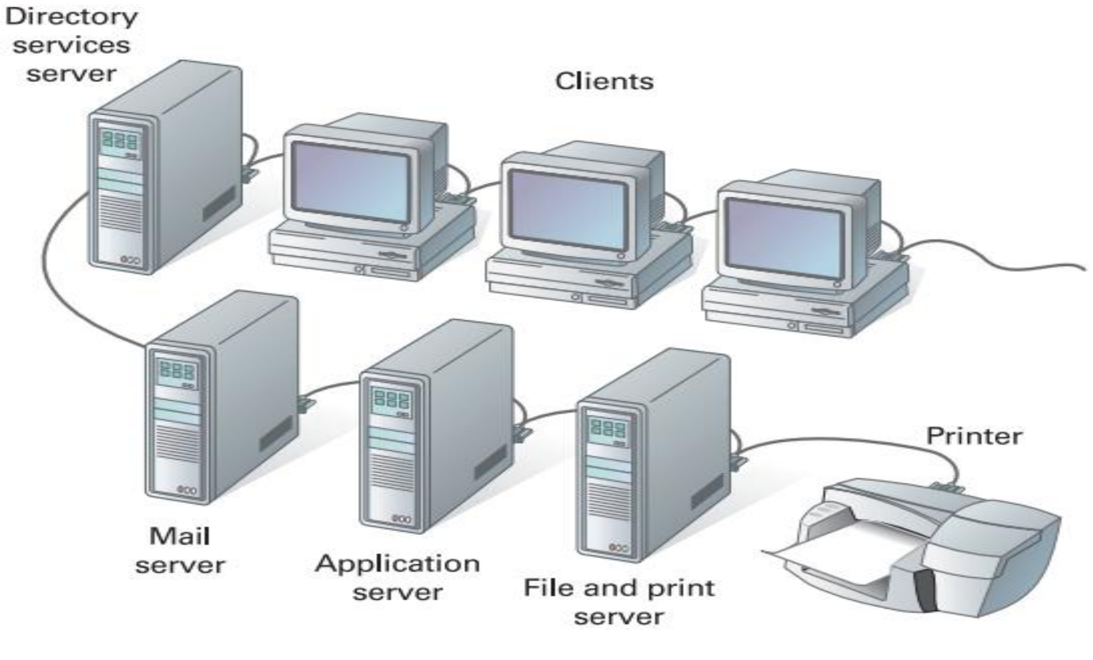


Figure 1.18: Types of servers

Application Server: An application server or an appserver is a component-based program that handles all application operations between users and backend applications or databases. It resides in the middle-tier of a server-centric architecture. It provides middleware services for security and state maintenance, along with data access and perseverance.An application server provides shared capabilities to software applications installed on client-server networks.The objective of an application server is to provide software abstractions for regularly used services.Some application servers also handle things like load-balancing and failover if the current application fails.

Email Server: An Email Server (also known as a **mail transport agent**, a **mail router** or an **Internet mailer**) is a server or a dedicated computer that controls and transfers e-mail over a network, mostly over the Internet. Anemail server receives e-mails from client computers and delivers them to other email servers. Anemail server also delivers e-mails to the client computers. The client computer is normally the computer where e-mails are drafted, send, received and read. For example a computer at home or in office. Mail server works concurrently with other programs to make up what is sometimes referred to as a messaging system. A messaging system incorporates all the applications necessary to keep e-mail moving as it should.An mail server usually consists of a storage spacewhere an email is stored for the users, along with set of user defined rules that determines how anemail server should react to the destination of a particular message, database consisting of user accounts which the email server recognizes and deals locally and communications modules those are components whichin facthandle the communication of messages to and from other mail servers and email clients.

File Server: A file server is a dedicated computer having central storage and management of data files. Such that other computers within the same network will be able to access the files. A file server allows users to share information within a network. Also, a program or mechanism that enables the required processes for file sharing can be called a file server.File servers are generallyoriginated in organization settings, such as company networks, today they are also used in schools, small organizations, and even at home networks.

Print Server: A software application, network device or dedicated computer that manages one or more printers within a network.The print server manages print requests and provides printer queue status information to end users and network administrators.Print servers are useful since theyallow users to print a job avoiding to move files from computer to computer before printing.Print servers usually supports one or more TCP/IP printing protocols. Common print protocols include:

- LPR/LPD (Line Printer Protocol)
- TELNET or stream
- IPP (Internet Print Protocol)
- Microsoft print protocol

Self-Test (Multiple Choice Questions)

Self-test

1. Fill in the blanks.
   a. In client server model users are called as ……………….
   b. The collaborative computing is also known as ……………….computing.
   c. In centralized computing network is done at …………………
2. Match the following

a. Network	a. Response
b. Client	b. Group of computers
c. Server	c. Request

3. Fill in the definitions for the following Functional relationshipsterms,
   - Client
   - Server
   - Peer-to-Peer (P2p)
   - Client-Server Network

1.6 Summary: In this chapter,it is explained that the old model of an individual computer serving all of the organization's computational need has been replaced by one in which the large no of separate but interconnected computers does the job. These systems are called as a computer network. A computer network is a collectionof more than one computer systems used for sharing services and interacting in some manner. At the end,it is shown that Computer networks are mainly divided into Local Area Network, Metropolitan area network, wide area network, wireless networks, Internetworks.

1.7 Exercise (short answer questions)

1. Writes Notes on (Draw diagrams when necessary)
   a. Types of networks
   b. Client Server Model
   c. Internetworks
2. Explain the centralize computing?
3. Explain in brief.
   a. Domain
   b. Workgroup

1.8 References

1.8.1 **Books**

Computer Networks: Andrew S. Tanenbaum

Networking Essentials: Emmett Dulaney

1.8.2 **Wikipedia**

http://en.wikipedia.org/wiki/Computer_networking

1.8.3 MOOCs

1.8.4 YouTube Videos

https://www.youtube.com/watch?v=mxK4cH6DJwo&list=PLftmDuo1-PWKJIApmovOsChz7a-bPKAZC

https://www.youtube.com/watch?v=R2mEK-LnaVk&list=PLoCUlAGhY8dL_glrT5IEORrcEIkuXk3vL

1.8.5 OER

Unit2 Network Topologies & Networking Devices

2.1 Learning Objectives

After successful completion of this unit, you will be able to:

- Understand and explain following terms:
  - **Topology**
  - **Media**
  - **Peer-To-Peer Network**
  - **Client - Server Network**
- Understand and explain Network Topology concepts
- Understand and handle different types of Topologies
- Understand and handle different Network Control Devices.
- Understand and explain how different devices are used to communicate in a network and in which conditions they are used

2.2 **Introduction:**Network topology describes the method used to do the physical wiring of the network. Common topologies include a bus, star, and ring. It is important to use the right topology. Each topology has its own strengths and weakness. Network architecture specifies the way in which computers participate in a network. A network consists of multiple computers that are connected by using some type of media or interface. Every computer has one or more interface devices like Network Interface Card (NIC) or a serial device for PPP networking. Computer are supported by network software that specifies the server or client functionality. Hardware that is used to transmit data over the network is called the media. For example, copper cable, fiber optic, or wireless transmission.

2.3 Network Topologies

2.3.1 Introduction: Network Topology refers to the layout of a network. It determines how different computers in a network are connected to each other and how do they communicate. It defines physical or logical arrangement of links in the network.

2.3.2 **Definition:** A network topology is the pattern in which nodes are connected to a network via links. **(Nodes: Computers, Printers, Switch or other devices)**

In fact topology is layout of computers, cables and other connected devices on a network. The term topology refers to the way a network is laid out either physical or logically two or more devices connect to a link or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (called nodes) to each other.

Topologies are either physical **(the physical layout of devices on a network)** or logical **(the way that the signals act on the network media, or the way that the data passes through the network from one device to the next)**

2.3.3 **Selection Criteria:**Topology determines the data paths that may be used between any pair of devices on the network.The selection of a Network Topology for a network cannot be done in isolation as it affects the choice of media and the access method used. Because it determines the strategy used in wiring a building for a network and deserves some careful study.

The following factors are considered while selecting a topology:

- Size (no. of nodes) of the system.
- The cost of the components and service required.
- Architecture of network.
- Cable type.
- Expandability of the network.
- The desired performance and reliability of entire system.
- Reliability
- Scalability
- Bandwidth capacity
- Ease of installation
- Ease of troubleshooting
- The delay involved in routing information from one node to another.
- Available hardware resources
- Applying invocation patterns
- Types of business processes that you plan to implement (interruptible versus non-interruptible)
- Individual scalability requirements
- Administrative effort involved

The Application, Remote Messaging, and Remote Support topology pattern is the preferred topology, but the choice finally depends upon users individual requirements.

2.3.4 **Types of Topology:** topology of a network is the geometric representation of the relationship of all the links and linking devices (called nodes) to each other.

There are two types of topologies-

1. Physical Topology
2. Logical Topology

Physical topology: The complete physical structure of transmission media is called physical topology. This refers to the layout of cabling, the location of nodes and interconnection between the nodes and cabling.

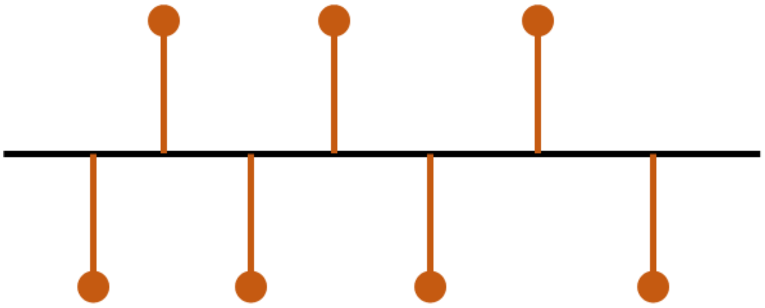
Logical Topology: The logical topology refers to how data is actually transferred on a network. This represents the way that data passes through the network from one device to another.

Different types of topologies are:

- Bus
- Ring
- Star
- Mesh
- Tree
- Hybrid

- **Bus Topology:** Bus topology is a network type in which every computer and network device is connected to a single cable. A single cable functions as a shared communication medium between devices connected with an interface connector. A device intending to communicate with another device in the network, sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message. When it has exactly two endpoints, then it is called Linear Bus topology.

  Symbol:



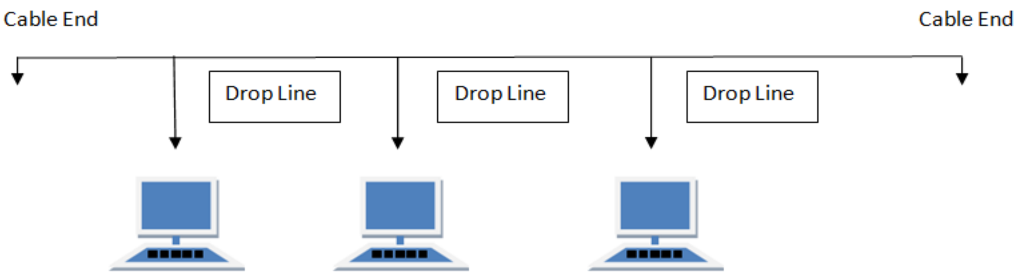


Figure 2.1: Bus Topology Network

Working: Computers on a bus topology network communicate by addressing data to a particular computer and sending out that data on the cable as electronic signals.

Sending the Signal: Network data in the form of electronic signals are sent to all the computers on the network. Only the computer whose address matches the address encoded in the original signal accepts the information, while all other computers reject the data. Only one computer at a time can send messages.

Since at a time only one computer can send data on a bus network, number of computers connected to the bus affect network performance. More computers there are on a bus, the more computers will be waiting in the queue to put data on the bus and, subsequently, the performance of the network will be slower.

Computers on a bus either transmit signal to other computers on the bus or listen for signal from other computers on the bus. They are not responsible for moving data from one computer to another. Subsequently, failure of one computer does not affect the rest of the network.

Signal Bounce: Since the signal, is sent over the entire bus, it travels from one end of the cable to the other. If the signal is permitted to travel continue uninterrupted, it will keep bouncing back and forth along the ends of the cable and restrict other computers from sending signals. So, the signal must be stopped after it has reached to the proper destination.

Terminator: To stop the bouncing of signal, a component called terminator is positioned at each end of the cable to absorb free signals. Terminator clears the cable by absorbing the signal so that other computers are able to send data.

Features of Bus Topology:

a. It transmits data only in one direction.
b. Every device is connected to a single cable

Advantages of Bus Topology

a. It is cost effective.
b. The cable required is least compared to other network topology.
c. Used in small networks.
d. It is easy to understand.
e. Easy to expand joining two cables together.

Disadvantages of Bus Topology

a. Cables fails, thenthe whole network fails.
b. If network traffic is heavy or nodes are more the performance of the network decreases.
c. Cable has a limited length.
d. It is slower than the ring topology.

- **Ring Topology:**The physical ring Topology is a circular loop of point-to-point links. It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Each device connects directly to the ring or indirectly through an interface device or drop cable. Every device has exactly two neighbors for communication purposes.

  Rings are used in high performance network. Messages travel through a ring in the same direction **(either clockwise or anticlockwise)**. Failure in any cable or device breaks the loop and take down the whole network.

  It has no beginning or end that needs to be terminated.In this topology, each device or node has a dedicated point to point line configuration with only two devices on either side of it.The signal is passed along the ring in one direction from one station to another until it reaches destination. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

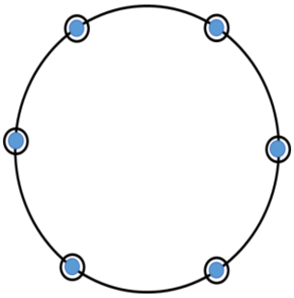
  There are two kinds of ring topologies:

  a. Single Ring
  b. Dual Ring

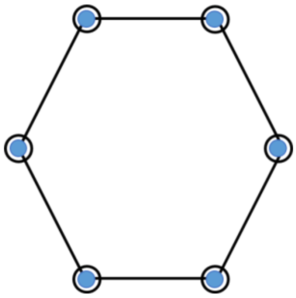
  Single Ring: In a single ring network, a single cable is shared by all the devices and data travel only in one direction. Each device waits for its turn and then transmits. When the data reaches its destination, another device can transmit.

  Dual ring: This topology uses two rings to send the data, each in a different direction. Thus allowing more packets to be sent over the network.

Symbol:



Or



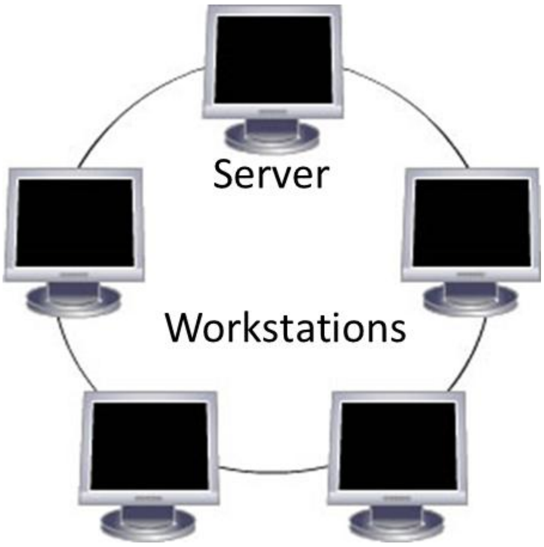


Figure 2.2: Simple ring network showing Logical Ring Topology

Working: In ring topology computers are connected to a single circle of cable. Unlike the bus topology, there are no terminating ends. Signals travel around the loop in one direction (**Clockwise or anticlockwise**) and pass through each computer that actsas a repeater to boost the signal and send it on to the next computer. Figure 2.2 shows the ring topology with one server and four workstations. The failure of one computer has an impact on the entire network.

Token Passing: One method of transmitting data around a ring is called token passing. (A token is a special series of bits that travels around a token-ring network. Each network has only one token.) The token is passed from computer to computer until it gets to a computer that has data to send. Figure 1.23 shows a token ring topology with the token. The sending computer modifies the token, puts an electronic address on the data, and sends it around the ring.

The message passes by each computer until it finds the one with an address that matches the address on the message. The receiving computer returns an acknowledge message to the sending computer shows that the data has been received successfully. On verification, the sending computer generates a new token and release it on the network. The token circulates within the ring until another workstation needs it to transfer data.

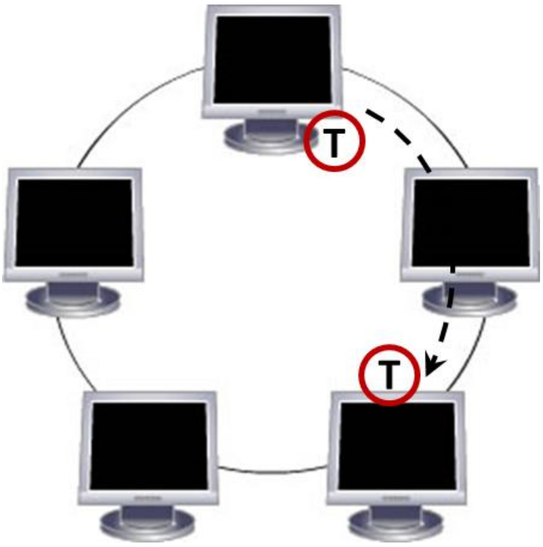


Figure 2.3: Computer is taking the token and passing it around the ring

Features of Ring Topology:

a. A number of repeaters are used in Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence, to prevent data loss repeaters are used in the network.

b. Transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

c. In Dual Ring Topology, two ring networks are formed, and data flow is in the opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.

d. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

a. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
b. Cheap to install and expand
c. Fault isolation is simplified, generally in a ring a signal is circulating at all time if any device does not receive a signal within the specified period. It can issue an alarm. An alarm alerts the network operator to the problem of its location.
d. Adding or deleting a device requires moving only two connections.
e. Time to send data is known, i.e. package delivery time is fixed and guaranteed because every PC has the token. No PC can have a monopoly on the network.
f. No data collisions.

Disadvantages of Ring Topology

a. Ring network requires more cable than a bus network.
b. Troubleshooting is difficult in a ring topology.
c. Adding or deleting the computers disturbs the network activity.
d. Failure of one computer disturbs the whole network.
e. Unidirectional traffic may be disadvantaged in a simple ring. A break in the ring can disable the entire network; using dual ring can solve the weakness.

- **Star Topology:**In Star Topology all nodes are individually connected to a central connection point, like a hub or a switch.This hub or switch is the central node and all others nodes are connected to the central node.Each node has a dedicated point-to-point link to the central hub. There is no direct link between these nodes and thesenodes communicate through central controller only.

  This approach avoids troublesome collisions and keeps the lines of communications open and free from traffic.Signals are transmitted from the sending node through the hub to all nodes on the network.Star topology is also known as a star network.

  Symbol:

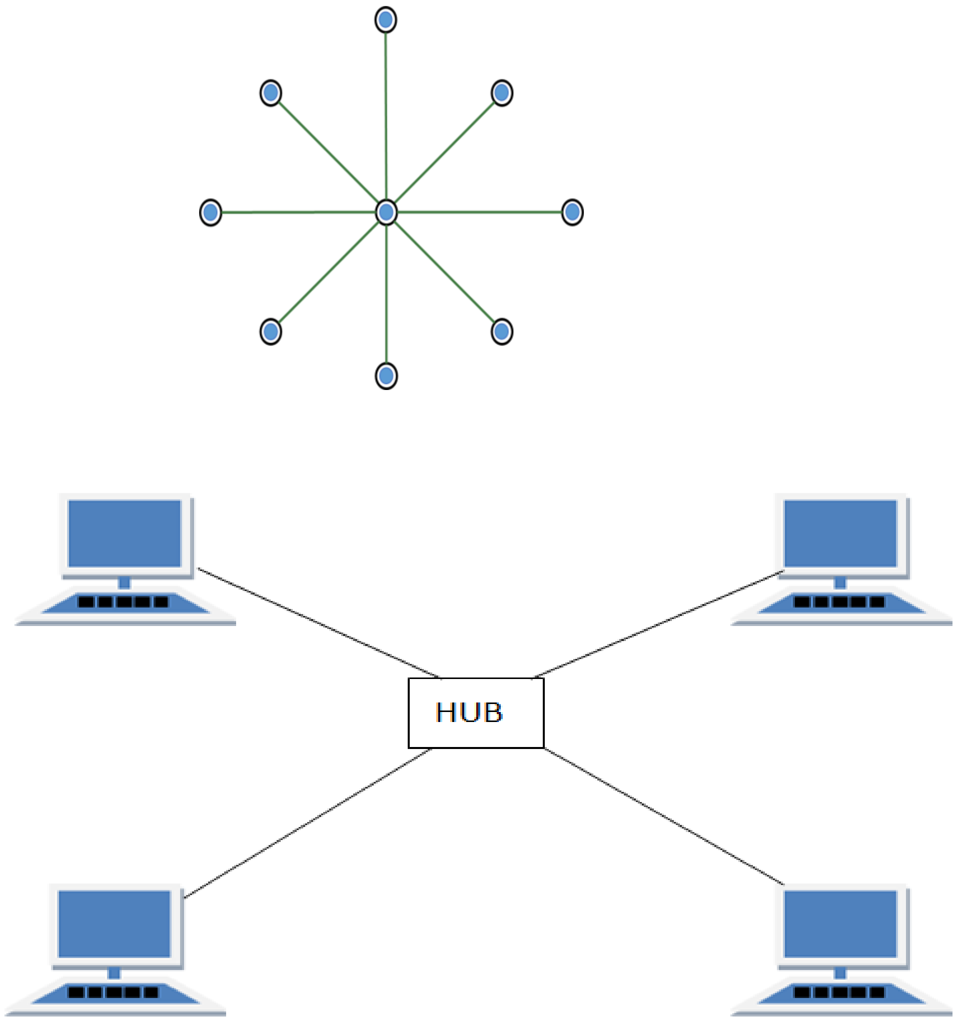


Figure 2.4: Star Topology Network

Working: Star network consists of one central switch, hub or computer which acts as a router to transmit messages.The routing function is performed by the central switch, hub or computer whichcentrally controls communication between any two nodes by creatinga logical path between them. It means that if one node wants to send data to another node, sending node sends the data to the controller & this controller then sends the data to receiving node.

An active hub or switch regenerates the electrical signal and sends it to all the nodes connected to it. This type of hub or switch is often called a multipoint repeater.

Features of Star Topology

a. Every node has its own dedicated connection to the hub.
b. Hub acts as a repeater for data flow.
c. Can be used with twisted pair, Optical Fiber or coaxial cable.

Advantages of Star Topology

a. Fast performance with few nodes and low network traffic.
b. Hub can be upgraded easily.
c. Easy to troubleshoot.
d. Easy to setup and modify.
e. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

a. Installation cost is high.
b. Highly expensive to use.
c. If central hub or switch fails then the whole network is stopped because all the nodes are depended on it.
d. Performance is based on the capacity of hub or switch

- **Mesh Topology:**All nodes in mesh topology have a point-to-point connection to other nodes or devices. All the nodes in mesh topology are connected to each other. Each node has a dedicated point to point link to every other node as shown in figure 2.5. Dedicated link carries the traffic only between two nodes it connects. There are multiple paths between two nodes of the network. If one path is failed, still the other path can be used.

Types of Mesh Topology

1. **Partial Mesh Topology:** In this type some systems are connected in similarwaylike mesh topology but some of the nodes are only connected to two to three nodes.
2. **Full Mesh Topology:**In this type each and every nodes are connected to each other.

Fully connected mesh network has **n (n-1)/2** physical connections to link nodes or devices.To achievethis every device on the network must have **(n-1)** output ports since every device requires an interface for every other on the network.

Symbol:

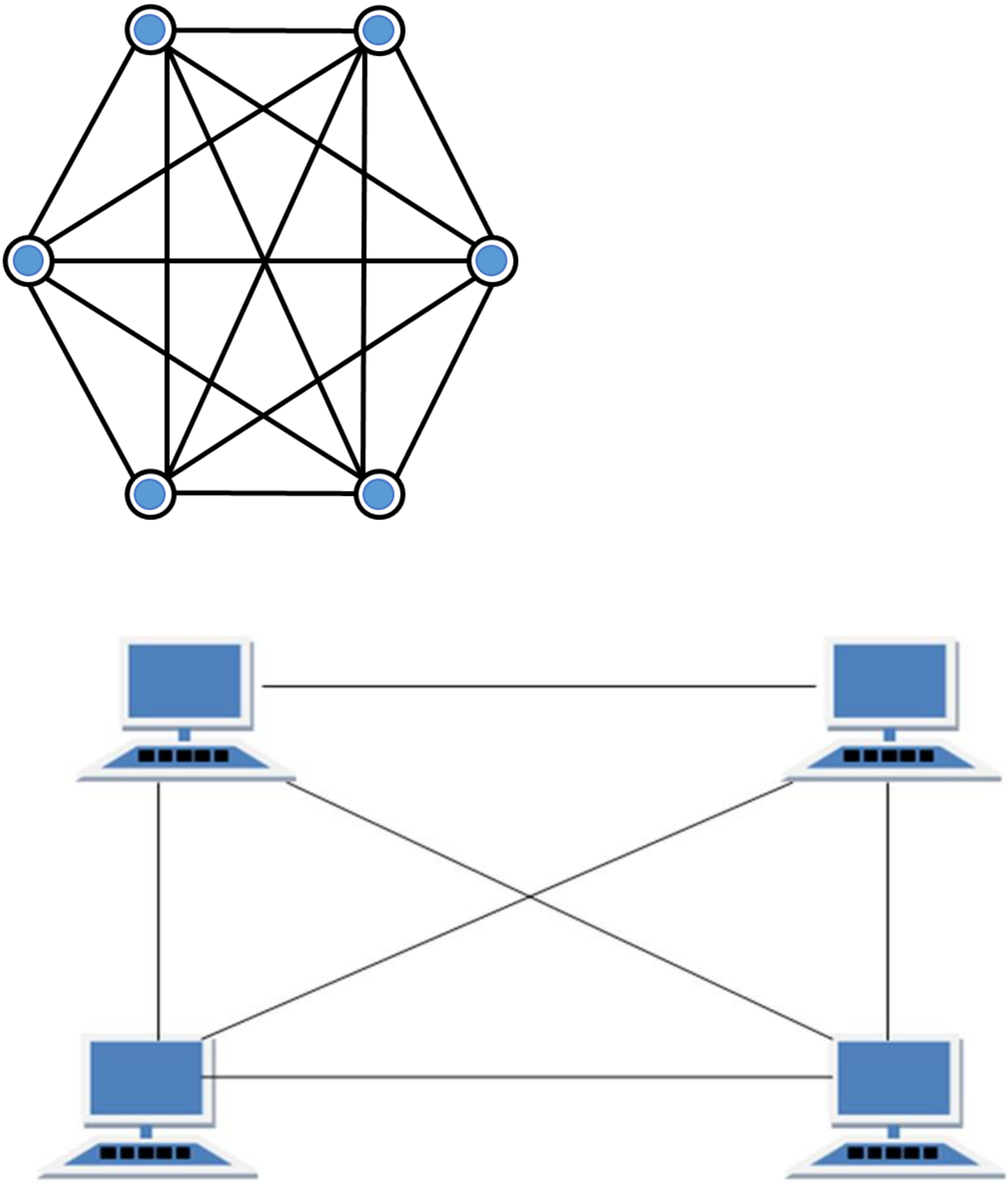


Figure 2.5: Mesh Network Topology

Working: Mesh topology network provides excellent redundancy and reliability.

There are two techniques to transmit data over the Mesh Topology:

1. Routing
2. Flooding

Routing: In routing, the nodes uses a routing logic, as per the network conditions. Routing logic is used to direct the data to reach the destination using the shortest distance. Also, routing logic having information about the broken links, uses it to avoid those nodes etc. Routing logic can also be used to re-configure the failed nodes.

Flooding: In flooding, no routing logic is used, same data is transmitted to all the network nodes. Such network is robust, and has more chances to lose the data. Also it leads to unwanted load over the network.

Features of Mesh Topology:

1. Fully connected.
2. Robust.
3. Unmanageable beyond a very small number of devices.
4. Not flexible.

Advantages of Mesh Topology:

1. Each dedicated linkcarries its own data load.
2. It is robust, i.e. failure of one link doesn’t affects the entire network.
3. Fault diagnosis is easy.
4. Provides good security and privacy, as every transmitted message travels along a dedicated line.
5. Reliable as compared to other topologies.
6. Heavy traffic data can be routed avoiding the busy root.

Disadvantages of Mesh Topology:

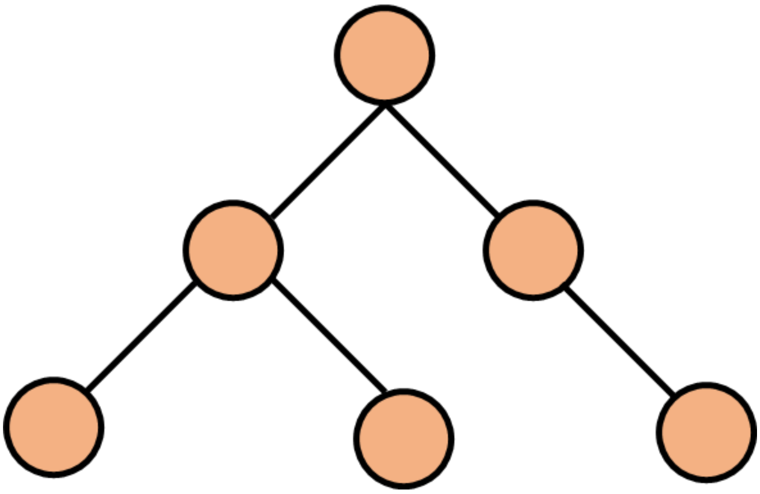
1. Installation and configuration is difficult.
2. Requires a lot of connection.
3. Cabling cost is more.
4. Very expensive.
5. Bulk wiring is required.
6. Difficult to install and reconfigure.

- **Tree Topology:**Also known as **Hierarchical Topology**. In this topology a central or root node is placed at the top level of the hierarchy. This root node is connected to one or more other nodes those are one level lower in the hierarchy i.e., at second level. The root node also connected one or more other nodes that are again one more level lower in the hierarchy, i.e., the third level.

  In this way root node and all other nodes are connected to it forming a hierarchy. Tree Topologyat least have up to three levels to the hierarchy. Hierarchy of the tree is symmetrical.Each node in the hierarchical network have a specific fixed number of‘f’ nodes connected to it at the next lower level in the hierarchy.The number ‘f’ is referred as the**Branching Factor** of the hierarchical tree.

Tree topology combines characteristics of linear bus and star topologies.Tree topologyis valued for its scalability and accessibility for troubleshooting.Each node this topology has point-to-point connection with each adjacent node on its below level. All secondary nodes have point-to-point connection to the third levelnearby nodes in their jurisdiction.Primary node has a point-to-point connection to each secondary node. These systems connections appear similar to a tree like structure.

Symbol:



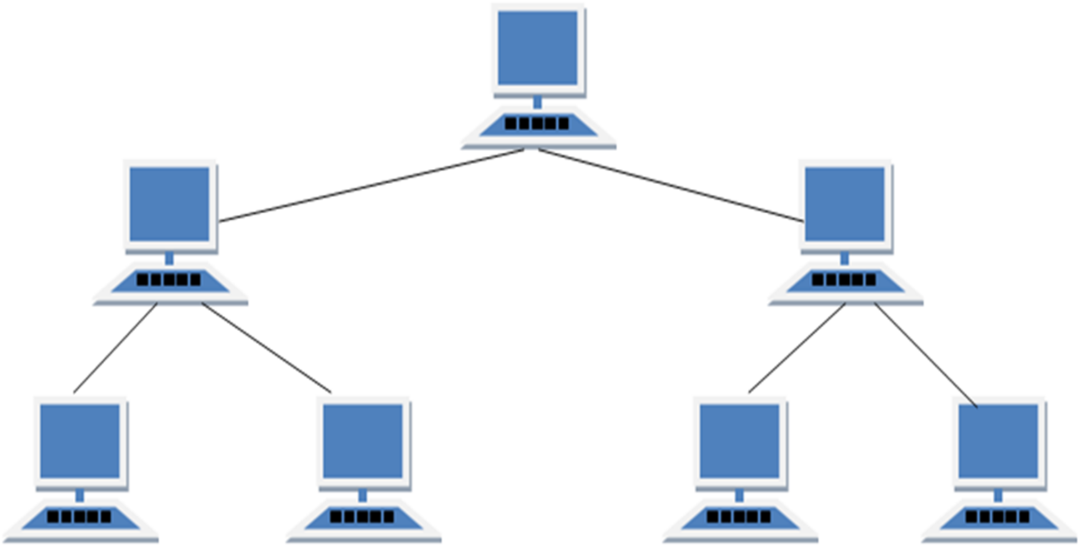


Figure 2.6: Tree (Hierarchical) Network Topology

Working: In tree topology network, one central hub and multiple secondary hubs are used. The central hub is an active hub. It regenerates the received signals of data. The secondary hubs are passive hubs. Each passive hub controls the nodes directly connected to it. Data exchanged to other devices connected to the same or other secondary hubs is done through the central hub. The secondary hub also actslike active hub if another secondary hub is directly connected to it.

Cable TV network is best example of tree topology. In this the main cable is divided into branches and each branch is further divided into smaller branches and so on. A hub is used every time when a new branch is created.

Features of Tree Topology

1. Form a tree network
2. Ideal if workstations are located in groups.
3. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Allows more devices to be connected to the central Hub.
3. Expansion of nodes is possible and easy.
4. Easily managed and maintained.
5. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. More expensive.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

- **Hybrid topology:**A hybrid topology is a network topology which uses two or more other network topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

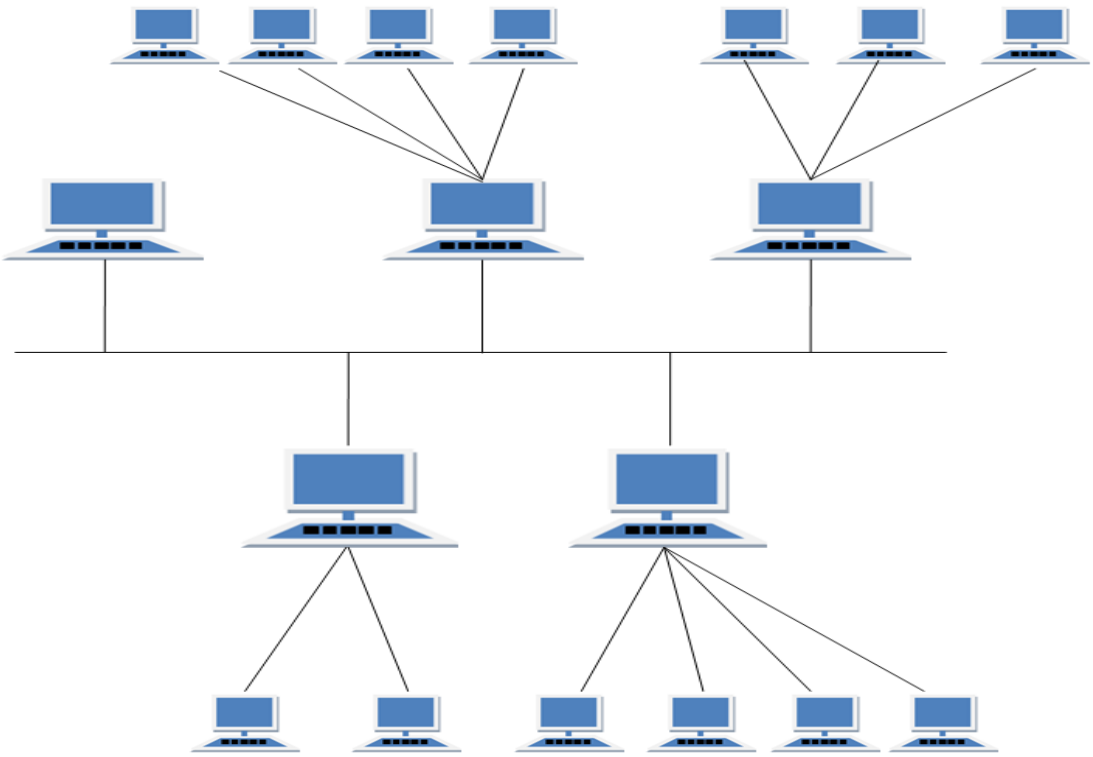


Figure 2.7: Hybrid Network Topology

Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and troubleshooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

2.3.5 Self-Test (Multiple Choice Questions)

2.3.6 Self-test question

1. Fill in the blanks.

- Network professionals use the term _________ to refer to the network's physical layout.
- The four basic topologies are the _______, ________, ________, and _________ topologies.
- In a bus topology, all the computers are connected in a series. To stop the signals from bouncing, it is important that a ________ be connected to each end of the cable.
- In a ________ topology all segments are connected to a centralized component called a __________.
- In a ________ topology, a break anywhere in the cable will cause the entire network to go down.
- The most reliable as well as the most expensive topology to install is the _______ topology.
- A ring topology passes a ________ from one segment to another. In order for a computer to place data on the network, the computer must be in possession of the _______.

2. What is topology?
3. Define:Network topologies
   a. Ring
   b. Bus
   c. Star
   d. Tree
4. Give advantages and disadvantages of the following topologies
   a. Ring
   b. Bus
   c. Star
   d. Tree

2.4 **Network Control / Connecting Devices:**Network control devices are the physical entities connected to a network. Basic network devices are: Computers either a PC or a Server, Connectors, Hub, Repeater, Bridges, Switches, Router, Gateway, Modem, Network interface cards (NICs), Wireless access points (WAPs), Printers and Modems.

These devices are classified into two types

- **End User Devices:** Include computers, printers, scanners, and other devices that provide services.
- **Network devices:** Include all devices that connects the end-user devices to communicate.End user devices that provide users with a connection to the network are also called hosts.

2.4.1 **Need of Network Control devices:**Network Control devices are used to expand a single network without breaking it into new pass or connecting it through another different network. All networks require devices to provide connectivity and functionality.

Network Devices.

- Allow a greater number of nodes to be connected to the network.
- Extend the distance over which a network can extend.
- Localize traffic on the network.
- Can merge existing networks.
- Isolate network problems so that they can be diagnosed more easily.

2.4.2 **Role of Network Control devices in a Network:** Network Control Devices operate at different layers of TCP/ IP model.Network control devices are categorized into five different categories based on the layer in which they operate in anetwork.

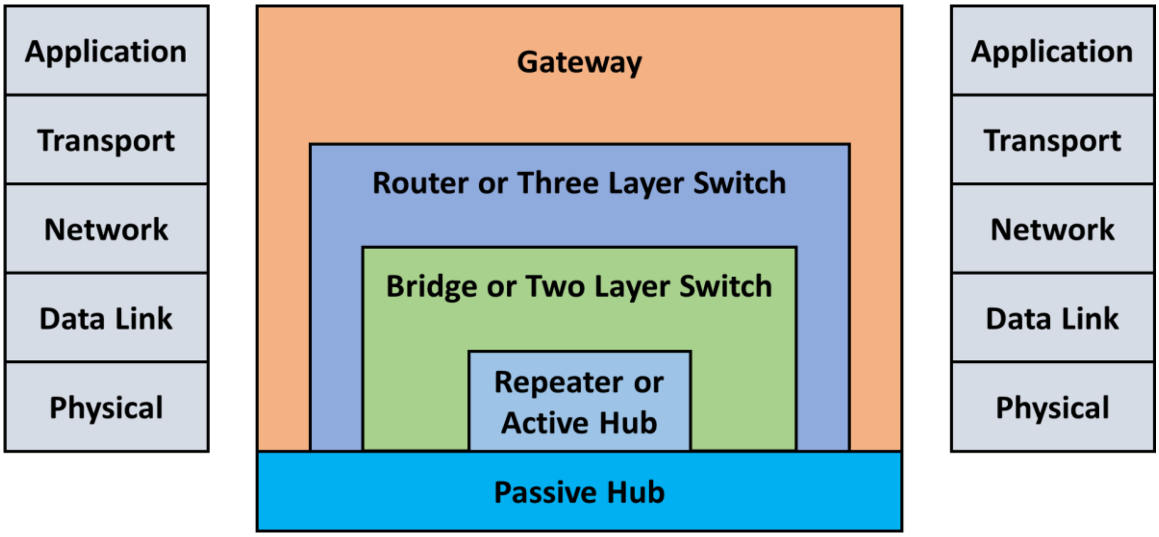


Figure 2.8 Network Control Devices

The five categories contain devices which can be defined as

- Operating below the Physical Layer.**(Ex. Passive Hub).**
- Operating at the Physical Layer **(Ex. Repeater or Active Hub).**
- Operating at the Physical and Data Link Layers **(Ex. Bridge or Two – Layer Switch).**
- Operating at the physical, data link, and network layers **(Ex. Router orThree – LayerSwitch).**
- Operating at all five layers **(Ex. Gateway).**

Usually some of following Network Control Devices are used to setup a Network:

- Connectors
- Hubs
- Repeaters

- Bridges
- Switches
- Routers
- Modem

2.4.3 Network Control Devices:

- **Connectors:** It is device that provides an entry pointat the end segment of cabling, for networking devices like computers, switches, hubs, and routers. Connectors can be classified according to its physical appearance and coupling properties.

  For example:

  Jacks and plugs are male connectors andSockets and Ports are female connectors. Also they can be classified by their different pinning configurations, such as DB9 and DB15 connectors that have 9 and 15 pins, respectively. In addition, connectors are also classified by the kind of electrical interfaces they support.

  Examples of different types of connectors include

  - Connectors for serial interfaces, such as RS-232 and V.35
  - Ethernet connectors, such as RJ-45 and BNC connectors
  - Fiber-optic cabling connectors, such as SC and ST connectors

  There are several of types of connectors used in networking, and the networking professional musthave to be familiar with many of them.

  - **Connectors are of different type such as:**
    1. Twisted Pair cable
    2. Co-axial Cable
    3. Fiber optic cable.

  - **Connectors are type such as:**
    1. Jacks
    2. Plugs
    3. Sockets and ports

  Example:

  - RS232 and V35 for serial interface
  - RJ45 and BNC connectors for Ethernet.
  - SC or ST connectors for fiber optic

BNC Connector:(Bayonet Neill Concelman) connector, sometimes also called as**British Naval Connectoror Bayonet Nut Connector**. It is a type of connector that is used with coaxial cables such as the RG-58 A/U cable used with the 10Base-2 Ethernet system. Basic BNC connector is a male type mounted at each end of a cable. BNC connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female connector.

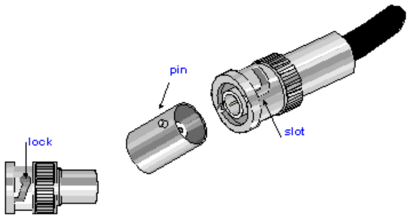


Figure 2.9: BNC Connector

BNC T-connectors (used with the 10Base-2 system) are female devices for connecting two cables to a network interface card (NIC). A BNC barrel connector allows connecting two cables together.

BNC connectors can also be used to connect some monitors, which increases the accuracy of the signals sent from the video adapter.

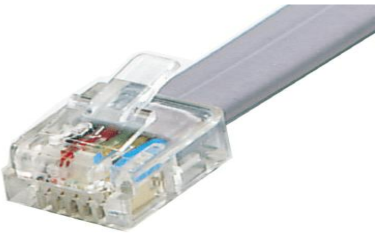


Figure 2.10: RJ – 11 Connector

RJ-11 (Registered Jack):RJ-11 is a 6-position 2 – conductortelephone connector/jack (6P2C) with 4 positions unused. RJ-11 is commonly used to connect the telephone handset to the base unit.RJ-11can also be used to connect LANs.

F-Type:F connector is a coaxial RF connector commonly used for cable television and universally for

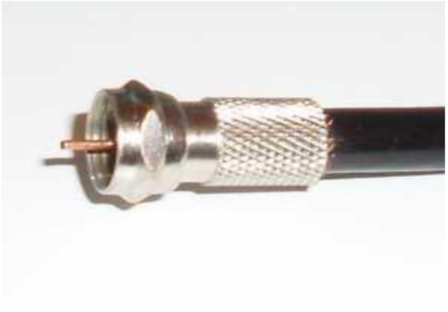


Figure 2.11: F – Type Connector

satellite television and cable modems.

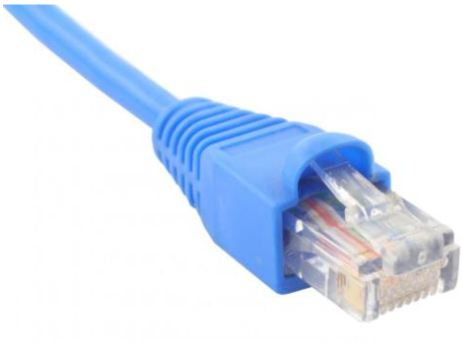


Figure 2.12: RJ – 45 Connector

RJ – 45:Registered Jack – 45is a most common twisted-pair connector. RJ - 45 is an 8-position, 8-contact (8P8C) modular plug commonly used for Ethernet networking.RJ – 45 connectors look similar to the ubiquitous RJ-11 connectors, but is slightly wider. RJ-45s can be used to connect some types of telephone equipment.

USB (Universal Serial Bus): Universal Serial Bus, or USB, is a computer standard designed to eliminate the guesswork in connecting peripherals to a PC. It is expected to replace serial and parallel ports. A single USB port can be used to connect up to 127 peripheral devices, such as mice, modems, keyboards, digital cameras, printers,

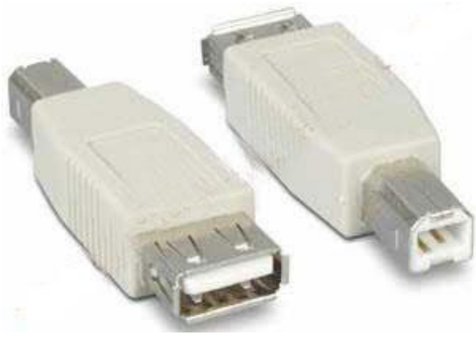


Figure 2.12: USB Connector

scanners, MP3 players and many more. USB also supports Plug-and-Play installation and hot plugging.

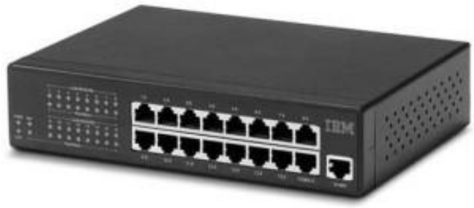


Figure 2.13: HUB

- Hub: Hub works at the physical layer of the OSI model.Hub is the most basic networking device that connects multiple computers or other network devices together. Hub is a device that splits a network connection into multiple computers. It is like a distribution center. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN cansee all packets.

Types of Hub: On the basis of its working functionality Hubs are categorized into three types:

a. **Passive Hub**
b. **Active Hub**
c. **Intelligent Hub**

Passive Hub: They do not have ability to amplify or regenerate the signal of incoming packets before broadcasting them out to the network. They are just used for creating a connection between various devices. Passive hub only receives signal and then forward it to multiple devices.

Active Hub: They does have the ability to amplify or regenerate the signal of incoming packets before broadcasting them out to the network. They not only amplifies the incoming signal but also forward it to multiple devices. It is also known as multiport repeater. It upgrades the properties of incoming signal before sending them to destination.

Intelligent Hub: This adds extra features to an active hub. It is capable to perform tasks of both Active and Passive hubs. It also performs other tasks like Bridging and routing.Intelligent Ethernet hubs also possesses remote management capabilities.

Applications of Hub: Networking Hubsareusuallyused networking connectivity device that have many advantages over other connectivity devices. Some Applications of Hub are as given below:

i. Hubs are used to create small home networks.
ii. Hubs are used to monitor the networks.
iii. Hubs are used at various places for connectivity.
iv. It makes one device or peripheral available throughout the whole network.

Advantages:

- A hub allows you connect clients to share and conversations with a network protocol analyzer.
- A hub also can modulate signal of the cable, if needed.
- Using hub save money because switches are costly then hub.

Hub Disadvantages:

- Hub can’t control traffic of data. Cause it receive all attachment post.
- Hubs have limited port to connect client, so it is not suitable for large network.
- It works as a query system. When NIC send a work to the hub then hub make this work pending and process one by one. So it’s time consuming.

- **Repeater:**Repeater is an electronic device that operates at the physical layer. Repeater regenerates the incoming signal over the same network before it becomes too weak or corrupted. So that the signal can be transmitted at maximum length in the network. Repeaters do not amplify the signal they just copy the signal bit by bit and regenerate it at the original strength, when the signal becomes weak. Repeaters are used to increase the usable length of the cable. Repeaters are most commonly associated with coaxial network configurations. Repeaters connects the segments that have the same access method. (CSMA/CD, Token Passing, Polling, etc.)Repeater cannot do the intelligent routing like bridges and routers.

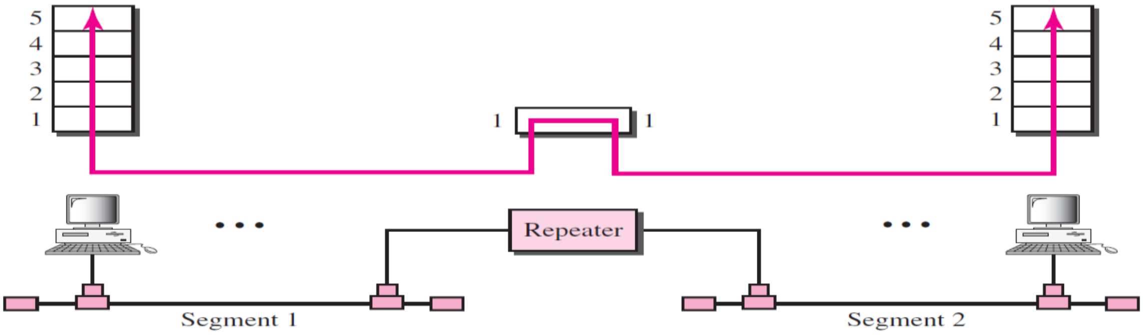
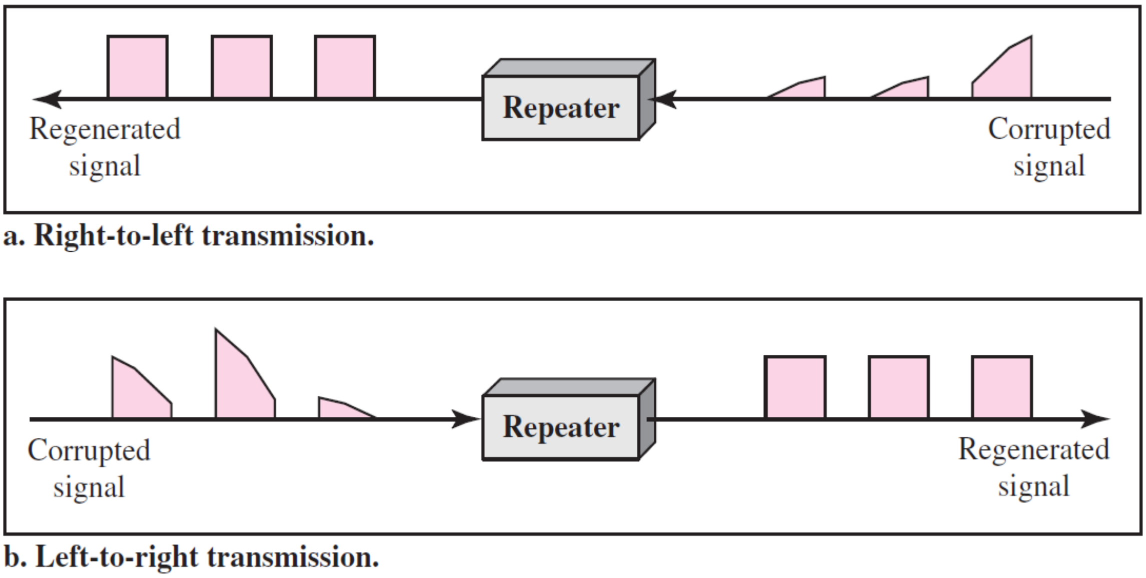


Figure 2.14:Repeater connecting two segments of a LAN

A repeater does not actually connect two LANs, rather it just connects two segments of thesame LAN. The segments connected are the part of the same single LAN. Repeater is nota device used to connect two different LANs of different protocols.

Functionality:10Base5 Ethernet cable has length restriction. Transmission length of the cable is limited up – to500 m.To extend this length, the cable is divided into segments and the repeaters installed between these segments.

Repeater acts as a two-port node, and operates only in the physicallayer. When a signal is received by repeater from any port it simply regenerates the signal and forwards it tothe other port. Figure 2.15 shows the functionality of a repeater.



a. Right-to-left transmission.

b. Left-to-right transmission.

Figure 2.15: Functionality of a Repeater.

Advantages

- Repeaters increase the usable distance of the network.
- Repeaters have little impact on network performance because they don't do any packet processing.
- Repeaters can connect networks using different physical media.

Disadvantages

- Repeaters cannot connect different network architectures.
- Repeaters do not reduce network traffic.
- The number of repeaters must be limited.
- Repeaters do not segment the network.
- Too many repeaters on a network create noise on the wire and increase the likelihood of packet collisions.
- Devices that are separated only by a repeater are part of the same collision domain.

- **Bridges:** It operates in both the Physical and the Data Link Layer. It regenerates the received signal as a Physical Layer device.And as a Data Link Layer device, it checks the Physical (MAC) Addresses (of both source and destination) contained in the frame.Bridges are networking devices used connect networksworking on the same protocol.It has a single input and single output port, thus making it a 2 port device.

  Bridge has filtering capability, it checks the destination address of a frame anddecideswhether frame should be forwarded or dropped. If the frame is to be forwarded, thedecision must specify the port. A bridge has a table that maps addresses to ports and used in filtering decisions.

  Working of Bridge: Bridges work at the Media Access Control Sub-layer ofthe OSI model. Routing table is built to record the segment no. ofaddress. If destination address and source address are in the same segment it decides to stop transmit. Otherwise, forwards it to the other segment

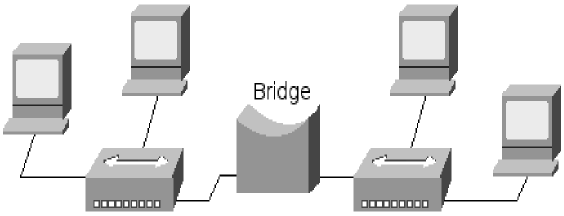


Figure 2.16: Bridge

Types of Bridges:

There are mainly three types in which bridges can be characterized:

Transparent Bridge: As the name signifies, it appears to be transparent for the other devices on the network. The other devices are ignorant of its existence. It only blocks or forwards the data as per the MAC address.

Source Route Bridge: It derives its name from the fact that the path which packet takes through the network is implanted within the packet. It is mainly used in Token ring networks.

Translational Bridge: The process of conversion takes place via Translational Bridge. It converts the data format of one networking to another. For instance Token ring to Ethernet and vice versa.

Advantages

- Bridges can extend a network by acting as a repeater
- Bridges can reduce network traffic on a segment by subdividing network communications
- Bridges increase the available bandwidth to individual nodes because fewer nodes share a collision domain
- Bridges reduce collisions
- Some bridges connect networks using different media types and architectures.

Disadvantages

- Does not limit the scope of broadcasts
- Does not scale to extremely large networks
- Buffering introduces store and forward delays - on average traffic destined for bridge will be related to the number of stations on the rest of the LAN
- Bridging of different MAC protocols introduces errors

- Because bridges do more than repeaters by viewing MAC addresses, the extra processing makes them slower than repeaters
- Bridges are more expensive than repeaters

- **Switch:**Since switches can operate at one or more OSI layers, including physical, data link, network, or transport layer,also known as a multilayer switch.Switch much appears like a hub.Switches are very efficient than hubs and are used widely in today's network environments. Switch is a high-speed device that receives incoming data packets and redirects them to their destination on a LAN.A switchcreates an electronic tunnel between source and destination ports so that no other traffic can enter for some time which end in communication without collisions.

  Functionality: Alike hub switch does not transmits the data to all the ports on the device. Rather switch transfers data only to that port to which destination device is connected. A switch does so by having an in-built learning of the MAC address of the devices connected to it. Since the transmission of data signals are well defined in a switch hence the network performance is consequently enhanced. Switches operate in full-duplex mode where devices can send and receive data from the switch at the simultaneously unlike in half-duplex mode. The transmission speed in switches is double than in Ethernet hub transferring a 20Mbps connection into 30Mbps and a 200Mbps connection to become 300Mbps.

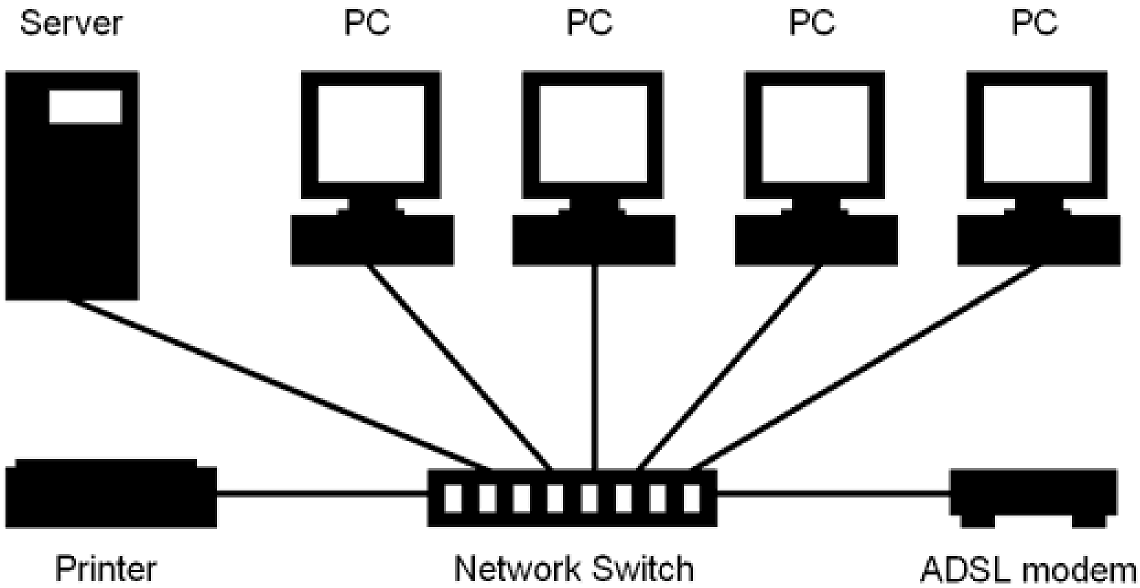


Figure 2.17: Switch

Switches data transmission methods:

Cut-through transmission: It allows the packets to be forwarded as soon as they are received. The method is prompt and quick but the possibility of error checking gets overlooked in such kind of packet data transmission.

Store and forward: In this switching environment the entire packet are received and 'checked' before being forwarded ahead. The errors are thus eliminated before being propagated further. The downside of this process is that error checking takes relatively longer time consequently making it a bit slower in processing and delivering.

Fragment Free: In a fragment free switching environment, a greater part of the packet is examined so that the switch can determine whether the packet has been caught up in a collision. After the collision status is determined, the packet is forwarded.

Advantages:

- Switches increase available network bandwidth
- Switches reduce the workload on individual computers
- Switches increase network performance
- Networks that include switches experience fewer frame collisions because switches create collision domains for each connection (a process called micro segmentation)
- Switches connect directly to workstations.

Disadvantages:

- Not as good as a router in limiting Broadcasts
- Communication b/w VLAN's need interVLAN routing [Router],but these days there are a number of Multilayer switchesavailable in the market.
- Handling Multicast packets needs quite a bit ofconfiguration & proper designing.
- At times switches when in Promiscuous mode is an opening for Security attacks [Spoofing IP address or capturingEthernet Frames using ethereal]

- **Router:** Router operates at Network Layer of OSI Model. A router is hardware device designed to receive, analyze and move incoming packets to another

Figure 2.18: Router

network. It may also be used to convert the packets to another network interface, drop them, and perform other actions relating to a network.A router has a lot more capabilities than other network devices, such as a hub or a switch that are only able to perform basic network functions.Routers can analyze the data being sent over a network, change how it is packaged, and send it to another network or over a different network. Routers are commonly used in home networks to share a single Internet connection between multiple computers.

A router is connects networks, like two LANs or WANs or a LAN and its ISP's network. Routers are located at gatewayswhere two or more networks connect.

Functionality: When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined, it searches in its routing table to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another router. Router determines the best route for the data to continue its journey.

Unlike bridges and switches, those uses the hardware-configured MAC address to determinethe destination of the data, routers use the software-configured network address to make decisions.

Routing tables play a very important role in helping the router to make a decision. Routing table are always updated and complete.

The two ways through which a router can receive information are:

- **Static Routing**
- **Dynamic Routing**

Static Routing: In static routing, the routing information is fed into the routing tables manually. It does not only become a time-taking task but gets prone to errors as well. The manual updating is also required in case of statically configured routers when change in the topology of the network or in the layout takes place. Thus static routing is feasible for tinniest environments with minimum of one or two routers.

Dynamic Routing: For larger environment dynamic routing proves to be the practical solution. The process involves use of peculiar routing protocols to hold communication. The purpose of these protocols is to enable the other routers to transfer information about to other routers, so that the other routers can build their own routing tables

Advantages

- Reduce network traffic by creating collision domains.
- Reduce network traffic by creating broadcast domains
- Able to function on LAN & WAN.
- It can connects different media & architectures.
- Capable to determine best path/route for data across an internetwork using dynamic routing techniques to reachthe destination.
- Router can filter the broadcasts.
- Routers can connect different network architectures, such as Ethernet and Token Ring

Disadvantage

- Highly expensive than Hub, Bridge & Switch.
- Works only with routable protocol.
- Dynamic router communications (inter-router communication) causes additional network traffic.
- Routing updates consume bandwidth.
- Slower than bridges or repeaters because they must analyze a data transmission from the Physical to the Network layer.
- Increase latency due to greater degree of packet filtering.
- Repeaters and bridges only need to read two layers of information: the Data Link and Physical.

- **Gateway:** A gateway is aninternetworking system capable of connecting two networks that use different protocols.In fact gateway is any device, system, or software application that can interpret data from one format to another. The main feature of a gateway isthat it converts only the format of the data, not the data.Gateway might be installed in some other device to add its functionality into another.

  Gateways works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also known as protocol converters and can operate at any network layer. Generally Gateways are more complex than switch or router.

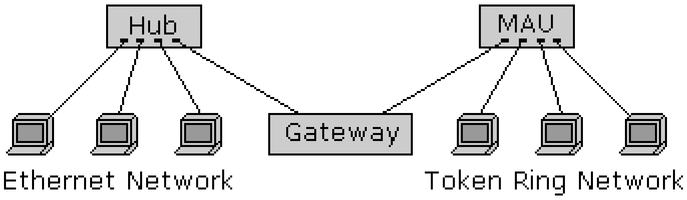


Figure 2.19: Gateways

Advantages

- Used to expand the network.
- Gateway is a server so it provides some security.

- We can connect two different types of networks.
- Protocol conversion is done.
- Effectively handles the traffic problems.
- Providesa connections between internal network and external network.
- Direct linking' b/w internal & external hosts are denied.
- User level authentication or protection is supported.

Disadvantages:

- Not an intellectual equipment.
- Not an intelligent device.
- So noise prevention is not done.
- Protocol conversion is done so transmission rate is slower.
- Somewhat hard to handle, requires the 'internal' user to know about them.
- Never strains out the 'data'. & it is costly.
- Possible kind of linking cannot be supported.

- **Modem (Modulation – Demodulation):**It is short for modulator-demodulator. A modem is a device or program used to transmit data over a telephone cable. Information is stored digitally on the computer. On other hand the information transmitted over telephone lines is transmitted in the form of analog signal. A modem converts the information from digital to analog while transmitting and analog to digital when receiving.

  Modems are available as internal devices that plug into expansion slots in a system; externaldevices that plug into serial or USB ports; PCMCIA cards designed for use in laptops; and specializeddevices designed for use in systems such as handheld computers.

  There are two types of Modem:

  - **Internal Modem:**The internal modem contains its own universal asynchronous receiver/transmitter (UART). The UART work here logically as serial port. A modulator circuit converts the serial digital data from the computer into analog signals to be transmitted over telephone line. The analog signal is then coupled to the telephone line using a circuit very similar to that used by ordinary telephone to couple voice signals. Then this analog signal passes to the telephone line through telephone jack (RJ-11 connector socket).

    On the receiver side, serial signals received from telephone line. The telephone interface separate received signals and passes them to demodulator. The demodulator converts analog signals into digital form and send this serial data to UART. The UART convert serial bit data into parallel byte and placed on the system's data bus. Besides combining and separating modulated audio data, the telephone interface generates the Dual-Tone-Multi-Frequency (DTMF) dialling signals needed to reach a remote modem. When a remote modem dials in the telephone interface defects the incoming signals and alerts the UART to begin negotiating a connection.

Finally the telephone interface drives a small speaker during find stages of modem operation. The speaker is used to hear a dial tone, dialling signals and audio negotiation between the two modems. Once a connection is established, the speaker is usually disabled. A controller circuit manages the overall operation of the modem. Generally it is used to manage modem between in control and data operating modes The NVRAM (Non Volatile RAM) it is used to store modem parameters

- **External Modem:**An external modem is similar to the internal modem in that it also allows access to the Internet, but unlike the internal modem, the external modem sits outside the computer. The external modem can be used when a computer is unable to fit an internal modem inside of it. The modem typically connects to the computer via a serial or USB cable, and is usually powered by an external source, rather than the computer.

  The external modem does not include built in UART. It uses existing serial port alreadyconfigured in the PC.A 9 pin (DB9) or 25 pin serial cables connects the PC serial port to the modem. Thus CPUneed not be opened during modem installation.

  A modulator circuit converts serial data into audio signal.The modulated audio signal is coupled to the Telephone lines by telephone interface.Audio signal is passing through RJ 11 type connector at the rear of the modem to thetelephone lines where signal receives from the telephone lines must be translated back intoserial data.

  The signal receives from telephone lines are converted into digital information usingdemodulator.The controller circuit manages the overall operation of the modem by switching the modembetween its control and data operating mode.

  During power loss or reset condition default modem parameters can be loaded from NVRAM. Permanent changes to modem parameters are stored in NVRAM.External modems avoid hardware conflicts such as (conflict of I/O address lines and that ofinterrupt lines) the external modem setup is faster and easier than internal modems.

In the external modem the status of serial communication can be checked from the signalstatus LEDs.

2.4.4 **Self-Test (Multiple Choice Questions)**

2.4.5 Self-test question

2.5 Network software

2.5.1 **NIC Device Driver**: Device Driver or simply a Driver is a computer program used to operate or control a particular device attached to a computer. Driver is a software that provides an interface to hardware devices and enables operating systems or other computer programs to access hardware functions without needing to know precise details of the hardware being used.

Network Interface Card (NIC) drivers are computerized instructions and information required for a NIC card to be operational when it is installed on or connected to a computer.Network adapters or hardware cards, also known as network interface cards, or NICs are inserted in a PCI slot, or USB port of the computer.

Nowadays many computer motherboardshave a build-in network adapter.Drivers for such networks adaptors are installed automatically by the latest operating systems like Windows 7, Windows 8, Windows 8.1 and Windows 10. But sometimes it is needed to install the driver before it can work.

To install NIC driver manually driver CD is needed and if CD is not available or lost those drivers can be downloaded from the manufacturer’s website over the internet.

Steps to verify and install NIC driver:

- Click Start and click Control Panel.
- In Category view, click Hardware and Sound, and then, under Devices and Printers, click the Device Manager link.
- From the Device Manager window displayed, double-click on Network Adapters to display the network adapter on the computer.
- If the NIC is visible and it doesn't have a problem icon (an exclamation mark), operating systemassumes that the NIC driver is installed and running properly.
- Double-click the device, toview the device status, if the device is working properly or not.
- If NIC is having a problem icon, double-click NIC.

- Mostly a message is displayed about device status that a driver is not installed.
- NIC in the Device Manager window is not visible, click the action menu, and click the add legacy hardware option.
- When Add Hardware Wizard window is displayed, click Next button to continue.
- Select the option install the hardware that “I manually select from a list (Advanced)” and click Next button.
- From the window displayed, scroll down and double-click on Network adapters in the Common hardware types list. A list of network adapters appears. If the NIC is there on the list, Windows will found and install the driver for it.
- Now click on Have Disk button. Then, click Browse button to locate the appropriate drive or folder for the NIC driver, and click Open.
- The driver path is displayed on the Install from Disk window, click OK, and click Next button to continue. When told that the device will be installed, click next again.
- A message stating that “The driver you are about to install does not have a Microsoft digital signature” may be visible. But, Click Yes to continue install it.
- When finish, click Finish.

2.5.2 **Client-Server Architecture:**Client-server architecture is a network architecture in which many computers requesting services or resources on the network are clients and one or more computer providing services or resources is a server. Servers are powerful computers or processes dedicated to managing disk drives (file servers), printers (print servers), or network traffic (network servers). Clients are PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.

- **DHCP:Dynamic Host Configuration Protocol (DHCP)** is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

  Figure 2.20 shows the basic steps that occur when a DHCP client requests an IP address from a DHCP Server. The DHCP client broadcasts a DHCPDISCOVER message to locate a Cisco IOS DHCP Server. A DHCP Server offers configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a DHCPOFFER unicast message.

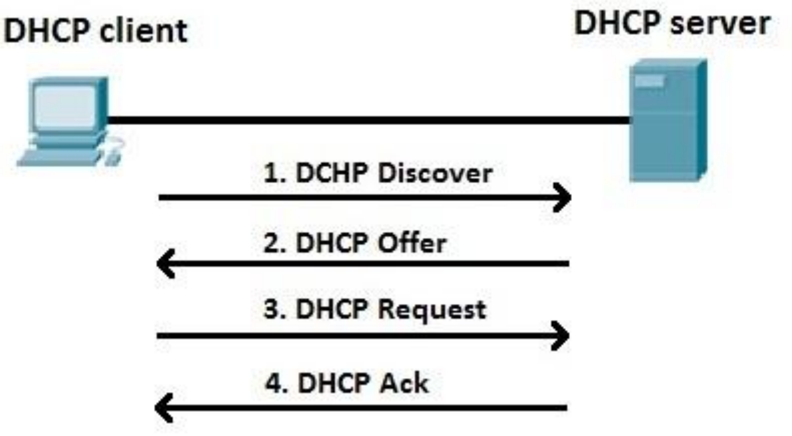


Figure 2.20: DHCP Request for an IP Address from a DHCP Server

Benefits of DHCP

DHCP Server service provides the following benefits:

- **Reliable IP address configuration:** DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.
- **Reduced network administration:** DHCP includes the following features to reduce network administration:
  - Centralized and automated TCP/IP configuration.
  - The ability to define TCP/IP configurations from a central location.
  - The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
  - The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.

DHCP provides configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP Server to a host and a mechanism for allocating network addresses to hosts. DHCP is built on a client/server model, where designated DHCP Server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. By default, Cisco routers running Cisco IOS software include DHCP server and relay agent software.

DHCP supports three mechanisms for IP address allocation:

- **Automatic allocation:** DHCP assigns a permanent IP address to a client.

- **Dynamic allocation:** DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address).
- **Manual allocation:** The network administrator assigns an IP address to a client and DHCP is used simply to convey the assigned address to the client.

The format of DHCP messages is based on the format of Bootstrap Protocol (BOOTP) messages, which ensures support for BOOTP relay agent functionality and interoperability between BOOTP clients and DHCP Servers. BOOTP relay agents eliminate the need for deploying a DHCP Server on each physical network segment.

DHCP Server Optional Parameters

Command options	**Description**
domain-name	Specifies the domain name for the DHCP clients.
domain-name-servers	Specifies the Domain Name System (DNS) IP servers that are available to the DHCP clients.
merit-dump	Specifies the path name of a file into which the client’s core image should be placed in the event that the client crashes (the DHCP application issues an exception in case of errors such as division by zero).
root-path	Specifies the name of the path that contains the client’s root filesystem in NFS notation.
router	Adds the default router and gateway for the DHCP clients.
subnet-mask	Defines the subnet mask for the network.
broadcast-address	Defines a broadcast address for the network.
wins-server	Defines the NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft DHCP clients.

log-servers	Defines a list of log servers available to the client.
bootstrap-server	Specifies the IP address of the bootstrap server (the command fills the "siaddr" field in the DHCP packet).

DHCP Server CLI Commands

Command	**Description**
dbexpire command	Specifies how long, in seconds, the DHCP server should wait before aborting a database transfer.
ip dhcp-server arp-ping-timeout	Specifies the time (in seconds) the server will wait for a response to an arp-ping packet before deleting the client from the binding database. The minimum setting is 5 seconds and the maximum time is 30 seconds. NOTE Do not alter the default value unless it is necessary. Increasing the value of this timer may increase the time to get console access after a reboot.
clear ip dhcp-server binding	Deletes a specific, or all leases from the binding database.
ip dhcp-server enable	Enables the DHCP server feature.
no ip dhcp-server mgmt	Disables DHCP server on the management port.
ip dhcp-server pool	Switches to pool configuration mode (config-dhcp-name# prompt) and creates an address pool.
ip dhcp-server relay-agent-echo enable	Enables relay agent echo (Option 82).
ip dhcp-server	Specifies the IP address of the selected DHCP server.
show ip dhcp-server binding	Displays a specific lease entry, or all lease entries.
show ip dhcp-server	Displays a specific address pool or all address pools.

show ip dhcp-server flash	Displays the lease binding database that is stored in flash memory.
show ip dhcp-server summary	Displays a summary of active leases, deployed address pools, undeployed address pools, and server uptime.
bootfile	Specifies a boot image to be used by the client.
deploy	Deploys an address pool configuration to the server.
dhcp-default-router	Specifies the IP address of the default router or routers for a client.
dns-server	Specifies the IP addresses of a DNS server or servers available to the client.
domain-name	Configures the domain name for the client.
lease	Specifies the lease duration for an address pool. The default is a one-day lease.
excluded-address	Specifies an address or range of addresses to be excluded from the address pool.
netbios-name-server	Specifies the IP address of a NetBIOS WINS server or servers that are available to Microsoft DHCP clients.
network	Configures the subnet network and mask of the DHCP address pool.
next-bootstrap-server	Configures the IP address of the next server to be used for startup by the client.
tftp -server	Configures the address or name of the TFTP server available to the client.
vendor-class	Specifies the vendor type and configuration value for the DHCP client.

- **TELNET:**TCP protocol is used to connect the remote computers, the TELNETprotocol makes it possible to use them. The TELNET protocol offers a user the possibility toconnect and log on to any other hosts in the network from user's own computer by offering aremote log on capability. TELNET is the first TCP/IP application which is still widely used as a terminal emulator. Now a days, when the applications are more and moreequipped with the graphical user interface, the terminal-based applications are becomingminority among the applications, the TELNET has found its future as a toolkit lying belowseveral client/server software. E.g. FTP, SMTP, SNMP, NNTP and HTTP are more or lessdependent on the TELNET protocol.

Telnet Model: For the connections, TELNET uses the TCP protocol. The TELNET service is offered in the host machine's TCP port 23. The user at the terminal interacts with the local telnet client. The TELNET client acts as a terminal accepting any keystrokes from the keyboard, interpreting them and displaying the output on the screen. The client on the computer makes the TCP connection to the host machine's port 23 where the TELNET server answers. The TELNET server interacts with applications in the host machine and assists in the terminal emulation.

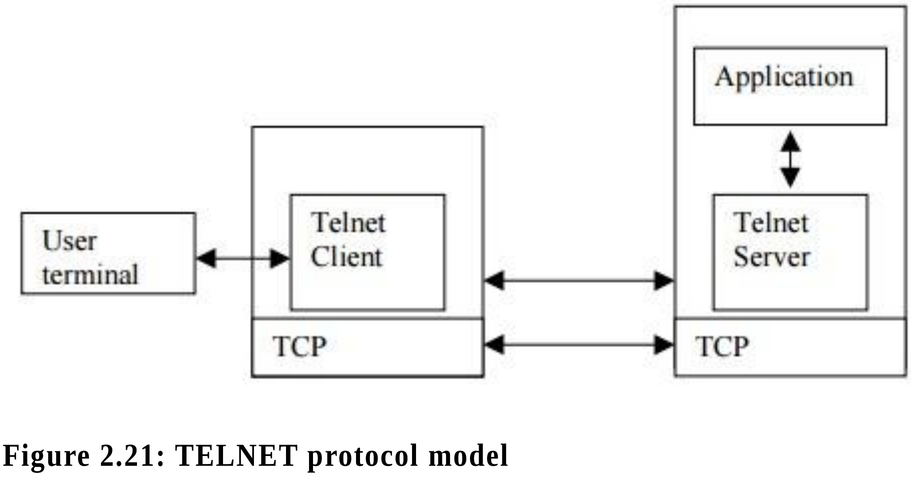


Figure 2.21: TELNET protocol model

As the connection is setup, the both ends of the TELNET connection are assumed to be originated and terminated at the network virtual terminal

(NVT). The NVT is a network wide terminal which is host independent so that both the server and the client in the connection may not need to keep any information about each other's terminal's characteristics as both sees each other as a NVT terminal. As there are several types of terminals, which may be able to provide additional services from those provided by the NVT, the TELNET protocol contains a negotiation method for the user and the server to negotiate changes to the terminal provided in the NVT. Typically the client and the server stays in the NVT just as long as it takes to negotiate some terminal type to be emulated.

Options

The TELNET has a set of options and these options can be negotiated through a simple protocol inside the TELNET. The negotiation protocol contains commands DO, WILL, WON'T and DON'T. Following examples present the accepted command sequences:

DO (sender wants receiver to enable the option)

WILL (receiver acknowledges)

DO (sender wants receiver to enable the option)

WON'T (receiver will not acknowledge the request)

WILL (sender wants to enable the option)

DO (receiver gives permission)

WILL (sender wants to enable the option)

DON'T (receiver does not give permission to do so)

WON´T (sender wants to disable option)

DON'T (receiver has to answer OK)

DON'T (sender wants receiver to disable option)

WON'T (receiver must say OK)

Mostly the options are used in the beginning of the connection to setup a desired set of options for the TELNET. In some cases the options are changed during the session. The key option to be negotiated is the terminal type.

The symmetry in the negotiation protocol indicates that some loops are possible.Without any further restrictions, the following sequence could take place:

DO TERMINAL TYPE VT100

WILL TERMINAL TYPE VT100

DO TERMINAL TYPE VT100

…

1. For this situation and similar situations the protocol introduces set of rules: 1. Parties may only request a change in the option (this rule overcomes previous problem)
2. If a party receives a request enter some mode that it is already in, the request should not be acknowledged
3. If the option affects the way, how the data is processed, the command must be inserted in the data stream exactly in the place where it is desired to take effect.
4. The rejected request should not be repeated until something changes in the operating environment E.G. the process runs other program or other user command is executed.

The options are set through TELNET commands. To indicate that the next byte is a command byte, the IAC (interpret as command) byte (0xFF) is sent. The data byte 0xFF is sent as two consecutive 0xFF bytes.

The option negotiation requires 3 bytes: IAC, request (WILL, WON'T, DO, DON'T) and the option ID byte to be enabled or disabled. The negotiations are either symmetrical or nonsymmetrical. With a symmetrical option both sides may start the negotiation sequence. A nonsymmetrical option is always requested by the other part. As an example of a nonsymmetrical option can be the linemode option, which can only be requested by the client.

The negotiation may require sub option negotiations. These negotiations take place when the option does not have only two modes: enable and disable. An example for such a sub negotiation is a terminal type negotiation. The Terminal type option is first enabled with a normal 3 byte negotiation:

IAC, WILL, 24 (24 = terminal type)

Server responds hopefully:

IAC, DO, 24

The server then asks the terminal type of the client:

IAC, SB, 24, 1, IAC, SE

(SB = suboption, 24 = suboption terminal type, 1 = sent your terminal type,SE = suboptionend)

Client responds:

IAC, SB, 24, 0, ‘V′, ′T′, ‘1’, ‘0’, ‘0’, IAC, SE

(0 = my terminal type, string VT100)

TELNET commands:

Name	Code	Description
EOF	236	End of file
SUSP	237	Suspend process
ABORT	238	Abort process
EOR	239	End of record
SE	240	Suboption end
NOP	241	No operation
DM	242	Data mark
BRK	243	Break
IP	244	Interrupt process
AO	245	Abort output
AYT	246	Are you there
EC	247	Escape character
EL	248	Erase line
GA	249	Go ahead
SB	250	Suboption
WILL	251	Option negotiation
WONT	252	Option negotiation
DO	253	Option negotiation
DONT	254	Option negotiation

IAC	255	Interpret as command

Telnet syntax

```
telnet [host [port]]
```

host	Specifies the hostname or IP address of the remote computer.
port	Specifies the port number or service name.

Examples

```
telnet ycmou.digitaluniversity.ac
```

Telnet to the **ycmou.digitaluniversity.ac**

- **FTP:File Transfer Protocol (FTP)** is for copying files between two computer systems over the TCP connection. The FTP overcomes the difficulties of various file systems that is used in the network. Various types of file systems creates problems about:
  - The file names conversion process
  - The directories utilization process
  - The file access under restrictions process
  - The data and the text representation process in the files

In case of FTP, the user exchange information with a user interface in the local FTP client process. A control connection is made by the local FTP client process to the remote server’s FTP server protocol. FTP server protocol can be located in the TCP port 21. The local FTP client is taken as a protocol interpreter that interprets the user commands to the acronyms which is used between the client and the server protocol. The control connection is fundamentally a general TELNET’s NVT session. The control connection is used very simply: The client transmit commands across the control connection to the server. The message is replied by the server in accordance with the server protocol.

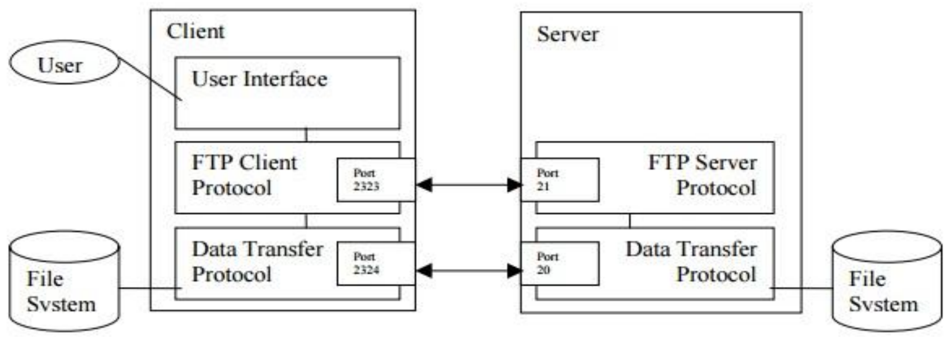


Figure 2.22: FTP protocol model

If the user asks for a data transfer, particular data connection is initiated between the server and the client and the files are transmitted through this link. Separate data transfer process is developed for the server and the client. The data connection persists until the command that it was made for is executed. Other different FTP commands that need a data connection a new connection is made.

The data connection is usually used for three purposes:

- To send a file from the client to the server
- For receiving a file from the server
- For receiving listings of files or directories from the server

The FTP overcomes the problem of different file systems used in thenetwork. The different types of file systems introduces problems in how:

- The file names are converted
- The directories are used
- The files are accessed under restrictions
- The data and the text are represented in the files.

FTP commands

Command type	Command	Parameters	Description
Access	USER	UserId	Identify user
	PASS	Password	Provide password
	ACCT	AccountId	Provide account
	REIN	-	Reinitialize start state
	QUIT	-	Logout

Command type	**Command**	**Parameters**	**Description**
	ABOR	-	Abort previous command
File mngt	CWD	Dir name	Change directory
	CDUP	-	Change to parent directory
	DELE	Filename	Delete file
	LIST	Dir name	List information about files
	MKD	Dir name	Make a directory
	NLST	Dir name	List the files in the directory
	PWD	-	Print the name of the working directory
	RMD	Dir name	Remove directory
	RNFR	Filename	Identify file to be renamed
	RNTO	Filename	Rename the file
	SMNT	Filename	Mount a different file system
Data format	TYPE	A(scii),E(bcdic),I(mage),N(nonprint),T(elnet),C(ASA)	Identify the data type for the transfer
	STRU	F(ile),R(ecord)	Organization of the file
	MODE	S(tream),B(lock),C(ompressed)	Transmission format
File transfer	ALLO	No. of bytes	Allocate storage for data
	APPE	Filenames	Append local file to remote file
	PASV	-	
	PORT	IP Addr+port	Identify IP address and port for data connection
	REST	Marker value	Identify restart marker
	RETR	Filename	Get a file
	STOR	Filename	Put a file
	STOU	Filename	Store unique: version of the file with unique name
Misc	HELP	-	Information about server implementation
	NOOP	-	Ask server to return an OK reply
	SITE	-	Server specific subcommands

Command type	Command	Parameters	Description
	SYST	-	Identify servers operating system
	STAT	-	Connection status request

2.5.3 **Solved Problems**

2.5.4 Solved problem

2.5.5 **Self-Test (Multiple Choice Questions)**

2.5.6 Self-test question

2.6 Summary

2.7 Exercise (short answer questions)

2.8 References

Books

Wikipedia

MOOCs

YouTube Videos

OER

Unit3: Transmission Media

1.9 **Learning Objectives:**To introduce common computer network transmission media, to enable users to identify installed transmission media, and to choose the appropriate transmission media for a given situation.

After successful completion of this unit, you will be able to:

- Develop the concepts of basic theory and operation of analog communication systems, transmission line and fibre optic theory
- Identify types of networks using different transmission media and compare features and operational aspects of transmission media.
- Define the term "transmission media" as it relates to computer networks
- Give an overview of the main types of media used in local area networks
- List and describe common transmission media
- Identify and describe the characteristics of each medium and compare them in terms of cost, ease of installation, capacity, attenuation, and immunity from interference
- Identify the public network services that expand the capabilities of private networks

- Identify the appropriate transmission media for particular business objectives
- Identify the various forms of connectivity hardware and describe their functions
- Choose the appropriate connectivity devices to fulfil particular network criteria
- Describe the primary types and uses of twisted-pair cables
- Describe the primary types and uses of coaxial cables
- Describe the primary types and uses of fibre-optic cables
- Describe the primary types and uses of wireless media
- Compare and contrast the primary types and uses of different media, m

1.10 **Transmission Media (Introduction):** Transmission media is a link that carries the information from sender to receiver. An electrical signal is in the form of current. An electromagnetic signal is series of electromagnetic energy pulses at various frequencies.Data is transmitted normally in the form of electrical or electromagnetic signals.Signals are transmitted in the form of electromagnetic energy from one device to another.Electromagnetic signals travel through vacuum, air or other transmission medium to travel from one point toanother point.

Electromagnetic energy includes power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.

Transmission media is also known as**Communication Channel.**

1.10.1 **Need of Transmission Media:** Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication Networks OSI Seven layer model is dedicated to the transmission media.

Transmission media is needed:

1. For data transmission.
2. To transmit data safely.
3. As transmission media decides the path of data to be transmitted between computers.

1.10.2 **Selection Criteria:**Different Medias have different properties like bandwidth, delay, cost and ease of installation and maintenance. The data transmission capabilities of various Media vary depending upon the various factors.

Following factors are to be considered while choosing Transmission Medium

- Type of Media
- Transmission Rate

- Flexibility
- Radiation
- Bandwidth
- Cost and Ease of Installation
- Reliability
- Resistance to Environmental Conditions
- Noise Absorption
- Attenuation
- Distances
- Number of receivers
- Transition media
- Topology used
- Transmission Protocol
- Connections of nodes vis
- Electrical network segment can be connected

Self-Test (Multiple Choice Questions)

Self-test question

1.11 **Types of Transmission Media:** Transmission media is broadly classified into two groups.

1. **Wired or Guided Media or Bound Transmission Media**
2. **Wireless or Unguided Media or Unbound Transmission Media**

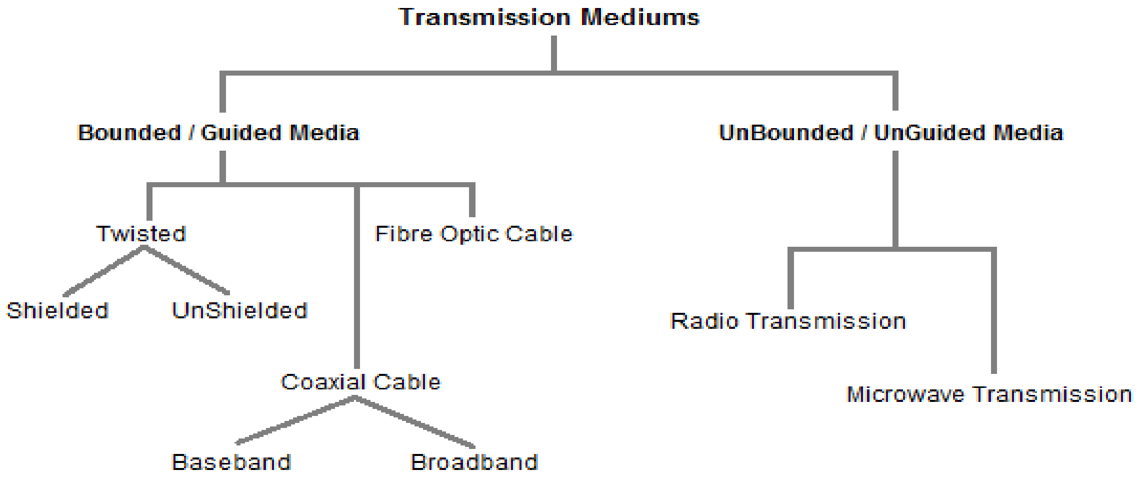


Figure 3.1: Transmission Mediums

1.11.1 **Guided Media:**It uses physical links, such as coaxial or fibre optic cables, to transmit data to the desired connection. Most cables are made of copper and bound by some form of jacket material. Because they are tangible, this type of media is limited to a fixed location. Popular bound transmission media in use are twisted pair cable, co-axial cable and fibre optical cable. Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost etc.

1.11.1.1 **Cable Characteristics:**Following characteristics are to be considered while choosing cable.

- **Cable Type:** It is the type of cable to be used for networking. Like **(UTP, STP Coaxial or Fibre Optic)**
- **Bandwidth:**The bandwidth of a communication system is the highest frequency range that it uses.
- **Data Transfer Rate:** The actual data throughput of a cable, after applying encoding and compression schemes to more efficiently use the bandwidth of the cable.
- **Cable Cost:** Cost required to purchase the cable.
- **Installation Cost:** Cost required to install the cable in the network.
- **Electro – Magnetic Interference Sensitivity:** It shows the capacity of cable to tolerate electromagnetic interference.

1.11.1.2 Types of Cable: Guided media is further categorized in three Types.

- **Twisted Pair Cable**
- **Coaxial Cable**
- **Fibre Optics Cable**

- **Twisted Pair Cable:** Twisted paircable consists of coppercore wires surrounded by an insulator. Two wires are twisted together to form a pair, and the pair forms a balanced circuit, so that voltages in each pair have the same amplitude but are opposite in phase. The twisting protects against **Electromagnetic Interference(EMI)**and **Radio Frequency Interference(RFI)**.

  A typical cable has multiple twisted pairs, each color-coded to differentiate it from other pairs. **UTP (unshielded twisted-pair)** has been used in the telephone network and is commonly used for data networking. **STP (shielded twisted-pair)** cable has a foil shield around the wire pairs in a cable to provide superior immunity to RFI.

Why twisted pair?

Purpose of twisting the wire is to reduce the electrical interference from the similar pairs in surroundings. The performance of the wire improves with the increase in the number of twist per foot.

If the two wires are parallel, then the electromagnetic interference from the devices such as motor can create a noise or interference on the wire that is closer to the source of noise. This results in high voltage level in one wire than the other as shown in **figure 3.2.**This further leads to uneven load and damaged signal and there will be difference at the receiver side.

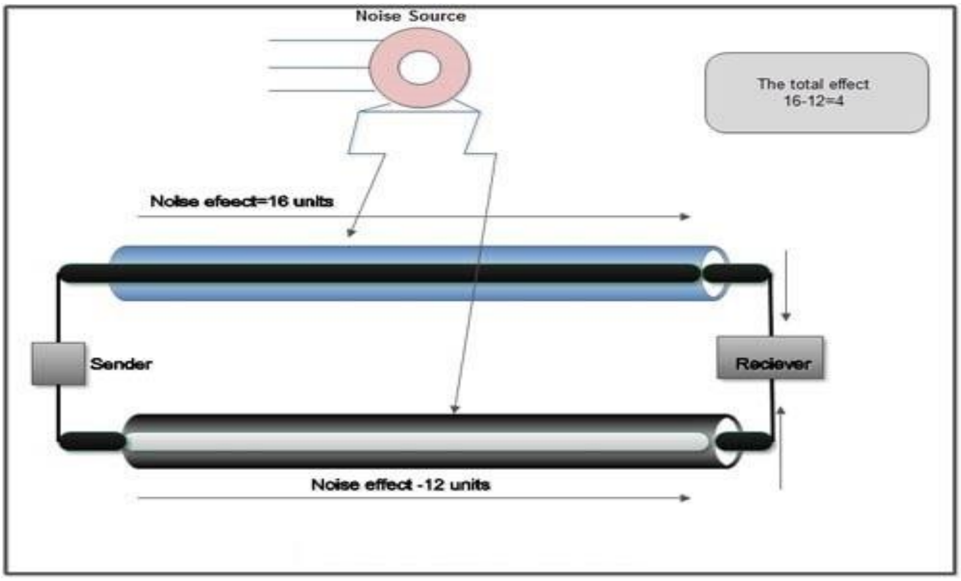


Figure 3.2: Effect of Noise on Parallel Pair Cables

If two wires are twisted, then the cumulative effect of the interference on both the wires is equal. In twisted pair each wire is closer to the noise source for half of the time and farther away for the other half i.e. in one twist one wire is closer to the noise source and the other is farther; in next twist the reverse is true.

So there will be no difference at the receiver side as unwanted signals are cancelled out, as shown in **figure 3.3.**

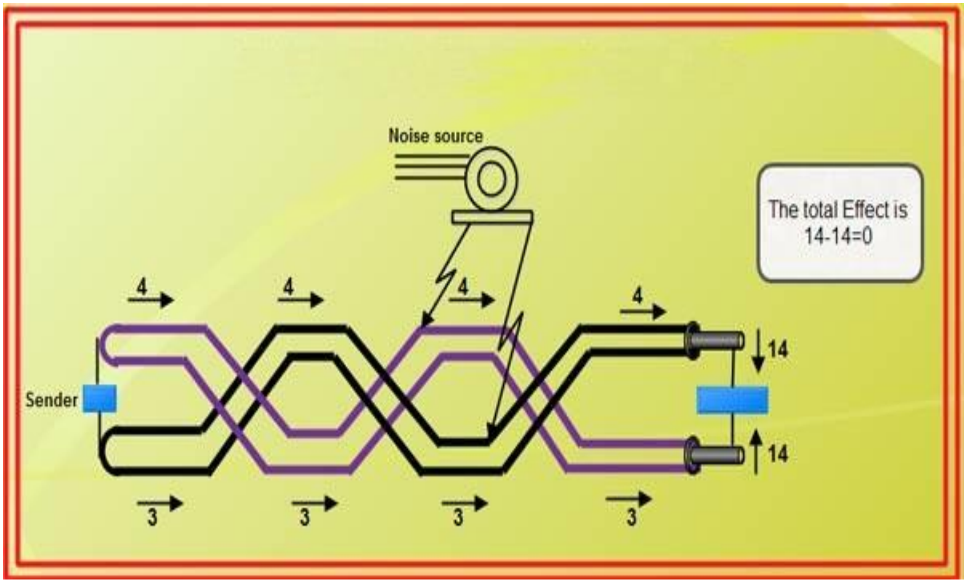


Figure 3.3 Effect of noise on twisted pair

There are two basic types of twisted-pair cable:

- **Unshielded Twisted Pair (UTP):**UTP cable is a medium that is composed of pairs of wires as shown in figure 3.4. UTP cable is used in a different types of networks. Each of the eight individual copper wires in UTP cable \is covered by an insulating material. In addition, the wires in each pair are twisted around each other.UTP cable often is installed using a Registered Jack 45 (RJ-45) connector. The RJ-45 is an eight-wire connector used commonly to connect computers onto a local-area network (LAN), especially Ethernets.

There are seven different types of UTP categories:

- Category 1: Used in telephone communications. Not used for transmitting data.
- Category 2: Used in Token Ring networks, Transmits data at speeds up to 4 megabits per second (Mbps).
- Category 3: Used in Token Ring and 10BASE-T networks,Transmits data at speeds up to 10 Mbps.
- Category 4: Used in Token Ring networks,Transmits data at speeds up to 16 Mbps.
- Category 5: Used in Ethernet, Fast Ethernet and Token Ring, Transmits data at speeds up to 100 Mbps.
- Category 5e: Used in Ethernet, Fast Ethernet and Gigabit Ethernet, Transmits data at speeds up to 1000Mbps (1 gigabit per second [Gbps]).
- Category 6: Used in Gigabit Ethernet and 10G Ethernet, Transmits data at speeds up to 10 Gbps.

UTP-CAT5e is the most popular UTP cable for networking.

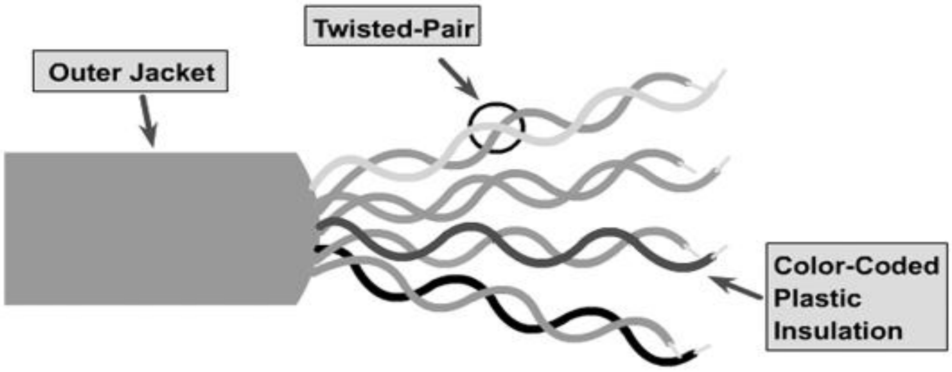


Figure 3.4: Unshielded Twisted-Pair Cable

Features of UTP cable:

- Physical Features: Typically uses eight wires grouped in four pairs, each composed of a solid-coloured and a stripped wire.
- Speed and throughput—1 to 1000 Mbps
- Average cost per node: less expensive
- Media and connector size: Small
- Maximum Cable Length: 100 m (short)

Advantages:

- Installation is easy
- Highly Flexible
- Very Cheap
- HaveHigh Speed Capacity
- 100-meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.
- Most compatible cabling, used in most of networking systems and need not require grounding.

Disadvantages:

- Low Bandwidth as compared to Coaxial Cable
- More prone to EMI interference.

- **Shielded Twisted Pair (STP):**STP is similar to UTP except with each pair covered by an additional copper braid jacket or foil wrapping. This shielding helps protect the signals on the cables from external interference.STP cable combines the techniques of shielding, cancellation, and wire twisting. Each pair of wires is wrapped in a metallic foil as shown in figure 3.5. The four pairs of wires then are wrapped in an overall metallic braid or foil, usually 150-ohm cable. As specified for use in Ethernet network installations, STP reduces electrical noise both within the cable and from outside the cable. Usually STP is installed with STP data connector thatis specially designed for the STP cable. STP cabling may also use the same RJ connectors used by UTP.

ThoughSTP provides better interference prevention than UTP, but it is more expensive and difficult to install. Since it is expensive and have difficulty with termination, STP is hardly used in Ethernet networks.

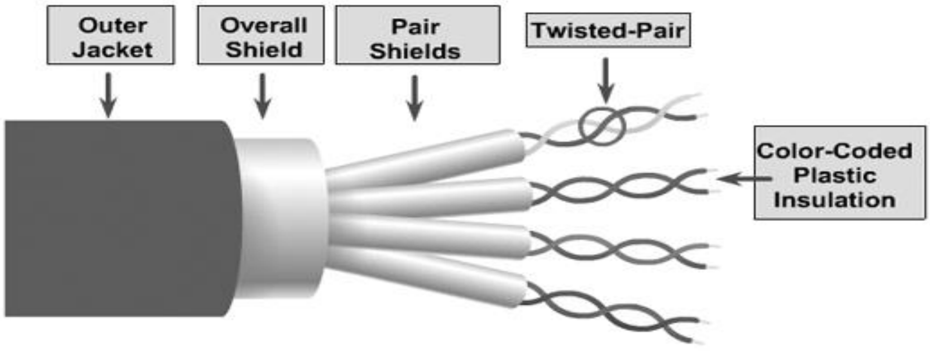


Figure 3.5: Shielded Twisted-Pair Cable

Features of STP cable:

- Speed and throughput: 10 to 100 Mbps
- Average cost per node: Moderately expensive
- Media and connector size: Medium to large
- Maximum cable length: 100 m (short)

STP cabling includes metal shielding over each individual pair of copper wires. This type of shielding protects cable from external EMI (electromagnetic interferences). STP cabling is used with token ring networks.

Advantages:

- Metal shield protects wires from radio and electromagnetic interference.
- This enhances dependability and boosts data transmission speeds at locationswhere EMI level is high.
- Installation is easy
- Performance is satisfactory
- Can used for both, Analog and Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair

Disadvantages:

- Difficult to manufacture
- Quite Heavy than UTP
- Very Expensive than UTP

- **Co-axial Cable:**Coaxial cable consists of a hollow outer cylindrical conductor that surrounds a single inner wire made of two conducting elements as shown in figure 3.6. One of these elements, located in the centre of the cable, is a copper conductor. Surrounding the copper conductor is a layer of flexible insulation. Over this insulating material is a woven copper braid or metallic foil that acts both as the second wire in the circuit and as a shield for the inner conductor. This second layer helps inthe reduction of outside interference.

  Coaxial cabling is the primary type of cabling used by the cable television industry and is also widely used for computer networks, such as Ethernet.Coaxial cable supports data transfer speeds up to 10 to 100 Mbps and is relatively inexpensive, it is more costly than UTP on a per-unit length.The most common connectors used with Thinnet are BNC connectors.

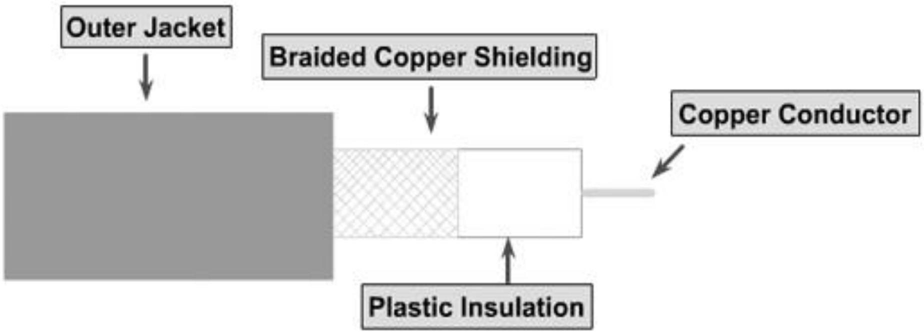


Figure 3.6: Coaxial Cable

Features of coaxial cables:

- Speed and throughput: 10 to 100 Mbps
- Average cost per node: Inexpensive
- Media and connector size: Medium
- Maximum cable length: 500 m (medium)
- It provides better immunity than twisted pair.
- This cable is able to transmit data at higher rates.

Other Properties of Coaxial Cable

- **Gauge:** Gauge of coaxial cable is thicker than the twisted pair.

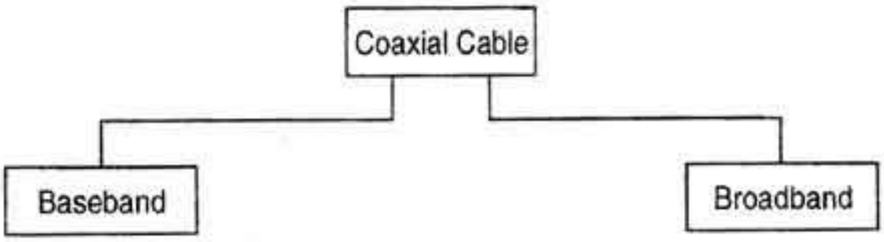
- **Configuration:** Coaxial cables consist of a single, two-conductor wire, with a centre conductor and an outer shield (conductor), which is of solid metal
- **Bandwidth:** Very significant bandwidth, hence used in high capacity applications, such as data and image transmission.
- **Error:** Due to the outer shielding performance of Coaxial cable is exceptionally fine.
- **Distance:** Not as limited as UTP, amplifiers or other intermediate devices can be used to extend high frequency transmissions over long distances.
- **Security:** Coaxial cable is integrally quite secure, it is not easy to place physical taps on coaxial cable. Radiation of energy is also very least so intercepting it is not that easy.
- **Cost:** The acquisition, deployment, and rearrangement costs of coaxial cables are very high, as compared with UTP.

Applications of coaxial cables:

Coaxial cable's superior performance characteristics make it the popular medium in many short hauls, bandwidth-intensive data applications.Coaxial cable is a widely used type of wire used for carrying a wide range of transmissions from source to device. Coaxial cable is mostly use in:

- Analog telephone networks.
- Digital telephone network.
- Cable TV
- Traditional Ethernet LANs
- Digital transmission
- Thick Ethernet

There are two types of Coaxial cables:



- **Baseband:**A baseband coaxial cable transmits a single signal at a time at very high speed. A broadband coaxial cable can transmit many simultaneous signals using different frequencies. A baseband cable is mainly used for LANs.

Baseband coaxial cable supports frequency range of a-4kHz and are used for digital signalling.**50 ohm (Ω)**Baseband coaxial cables are used for digital transmission.

- Broadband: **75 ohm (Ω)**Broadband coaxial cables are used for analog transmission.It can transmits several simultaneous signal at different frequencies. Covers large area as compared to Baseband Coaxial Cable. Since it is used for large area, it requires amplifiers which are unidirectional.

Coaxial Cable Limitations:

- High installation cost
- High maintenance cost.

Advantages of Coaxial Cables

- It can be used for both analog and digital transmission.
- It offers higher bandwidth as compared to twisted pair cable and can span longer distances.
- Because of better shielding in coaxial cable, loss of signal or attenuation is less.
- Better shielding also offers good noise immunity.
- It is relatively inexpensive as compared to optical fibres.
- It has lower error rates as compared to twisted pair.
- It is not as easy to tap as twisted pair because copper wire is contained in plastic jacket.

Disadvantages of Coaxial Cables

- It is usually more expensive than twisted pair.

- Fibre Optics Cable: An optical fibre is a thin (2 to 125 µm), flexible medium capable of guiding an optical ray. Various glasses and plastics can be used to make optical fibres. The lowest losses have been obtained using fibres of ultrapure fused silica. Ultrapure fibre is difficult to manufacture; higher-loss multicomponent glass fibres are more economical and still provide good performance. Plastic fibre is even less costly and can be used for short-haul links, for which moderately high losses are acceptable.

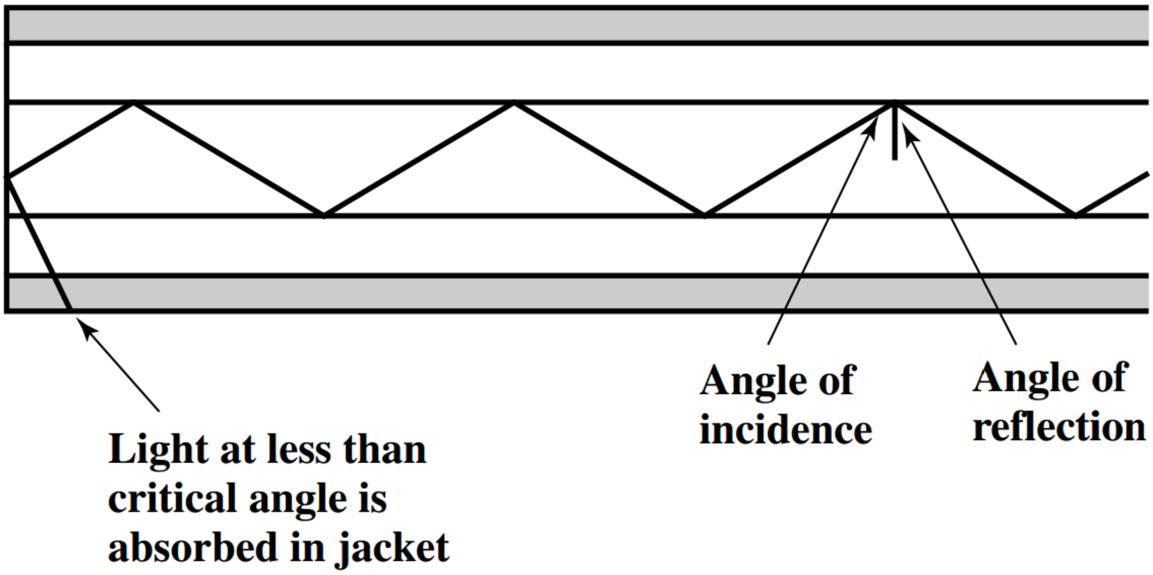


Figure 3.7Optical Fibre

An optical fibre cable has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket as shown in Figure 3.7. The core is the innermost section and consists of one or more very thin strands, or fibres, made of glass or plastic; the core has a diameter in the range of 8 to Each fibre is surrounded by its own cladding, a glass or plastic coating that has optical properties different from those of the core. The interface between the core and cladding acts as a reflector to confine light that would otherwise escape the core. The outermost layer, surrounding one or a bundle of cladded fibres, is the jacket. The jacket is composed of plastic and other material layered to protect against moisture, abrasion, crushing, and other environmental dangers.

Applications one of the most significant technological breakthroughs in data transmission has been the development of practical fibre optic communications systems. Optical fibre already enjoys considerable use in long-distance telecommunications, and its use in military applications is growing. The continuing improvements in performance and decline in prices, together with the inherent advantages of optical fibre, have made it increasingly attractive for local area networking.

The following characteristics distinguish optical fibre from twisted pair or coaxial cable:

- **Greater Capacity:** The potential bandwidth, and hence data rate, of optical fibre is immense; data rates of hundreds of Gbps over tens of kilometres have been demonstrated. Compare this to the practical maximum of hundreds of Mbps over about 1 km for coaxial cable and just a few Mbps over 1 km or up to 100 Mbps to 1 Gbps over a few tens of meters for twisted pair.

- **Smaller Size and Lighter Weight:** Optical fibres are considerably thinner than coaxial cable or bundled twisted-pair cable—at least an order of magnitude thinner for comparable information transmission capacity. For cramped conduits in buildings and underground along public rights-of-way, the advantage of small size is considerable. The corresponding reduction in weight reduces structural support requirements.
- **Lower Attenuation:** Attenuation is significantly lower for optical fibre than for coaxial cable or twisted pair and is constant over a wide range.
- **Electromagnetic Isolation:** Optical fibre systems are not affected by external electromagnetic fields. Thus the system is not vulnerable to interference, impulse noise, or crosstalk. By the same token, fibres do not radiate energy, so there is little interference with other equipment and there is a high degree of security from eavesdropping. In addition, fibre is inherently difficult to tap.
- **Greater Repeater Spacing:** Fewer repeaters mean lower cost and fewer sources of error. The performance of optical fibre systems from this point of view has been steadily improving. Repeater spacing in the tens of kilometres for optical fibre is common, and repeater spacing's of hundreds of kilometres have been demonstrated. Coaxial and twisted-pair systems generally have repeaters every few kilometres.

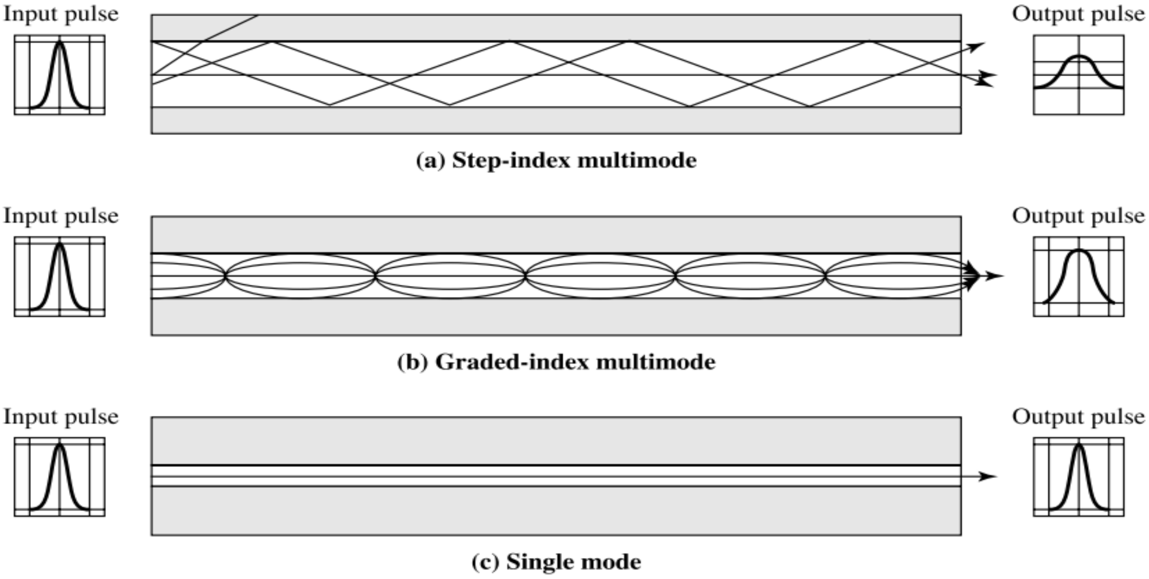
Five basic categories of application have become important for optical fibre:

- Long-haul trunks
- Metropolitan trunks
- Rural exchange trunks
- Subscriber loops
- Local area networks

Transmission Characteristics:

Optical fibre transmits a signal-encoded beam of light by means of total internalreflection.Total internal reflection can occur in any transparent medium that hasa higher index of refraction than the surrounding medium. In effect, the optical fibreacts as a waveguide for frequencies in the range of about to this coversportions of the infrared and visible spectra.

Figure 3.8 shows the principle of optical fibre transmission. Light from asource enters the cylindrical glass or plastic core. Rays at shallow angles are reflectedand propagated along the fibre; other rays are absorbed by the surroundingmaterial. This form of propagation is called step-index multimode, referring to thevariety of angles that will reflect.



(a) Step-index multimode

(b) Graded-index multimode

(c) Single mode

Figure 3.8: Optical Fibre Transmission Modes

With multimode transmission, multiple propagationpaths exist, each with a different path length and hence time to traverse the fibre. This causes signal elements (light pulses) to spread out in time, which limitsthe rate at which data can be accurately received. Put another way, the need to leavespacing between the pulses limits data rate.

This type of fibre is best suited for transmissionover very short distances. When the fibre core radius is reduced, fewer angleswill reflect. By reducing the radius of the core to the order of a wavelength, onlya single angle or mode can pass: the axial ray. This **single-mode** propagation providessuperior performance for the following reason. Because there is a single transmissionpath with single-mode transmission, the distortion found in multimodecannot occur. Single-mode is typically used for long-distance applications, includingtelephone and cable television. Finally, by varying the index of refraction of thecore, a third type of transmission, known as **graded-index multimode**, is possible.

This type is intermediate between the other two in characteristics. The higher refractiveindex (discussed subsequently) at the centre makes the light rays movingdown the axis advance more slowly than those near the cladding. Rather than zigzaggingoff the cladding, light in the core curves helically because of the gradedindex, reducing its travel distance. The shortened path and higher speed allows lightat the periphery to arrive at a receiver at about the same time as the straight rays inthe core axis. Graded-index fibres are often used in local area networks.

Two different types of light source are used in fibre optic systems: the lightemittingdiode (LED) and the injection laser diode (ILD). Both are semiconductordevices that emit a beam of light when a voltage is applied. The LED is less costly,operates over a greater temperature range, and has a longer operational life. TheILD, which operates on the laser principle, is more efficient and can sustain greaterdata rates.

Advantages:

- **Extremely High Bandwidth:**Fibre optic cables have a much greater bandwidth than metal cables.No other cable-based data transmission medium provides the bandwidth like it.
- **Easy to AdjustIncreasing Bandwidth:**Characteristics of Fibre cable enable dynamic network bandwidth provisioning to provide for data traffic spikes and lulls.
- **Good Resistance to Electromagnetic Interference:**Fibre has a very low rate of bit error hence it is highly resistive to electromagnetic interference. Mostlyfibre-optic transmission is noise free.
- **Flexibility:**Optical fibre has greater tensile strength than copper or steel fibres of the same diameter. It has good flexibility, it bends easily and resists most corrosive elements thosestrikes copper cable.
- **Able to detect Cable Damage and provide Secure Transmissions:**It provides an verysecure transmission medium, since there is not any possibilityof detection of data transmission "listening in" or "leaking" through the cable, like traditional media. Any damage due to splices in the cable can be easily detected by continuous monitoring an optical network and by preciselymeasuring the time to take the light to reflect down the Fibre.
- **Low Signal Loss:**An optical fibre offers low signal loss. This allows for longer transmission distances. When high frequency signal are broadcastedthrough convention coaxial cable,it loss half of its power only after a few hundred meters whereas the optical Fibre loss the sauce amount of power in 15 km or more. Thus repeater is required at very long distance.
- **High Transmission Rate:** The transmission rate of optical Fibre is 10 GB/sec whereas coaxial cable is 1 GB/sec.

- **Saves Time:**Since it is small in size and light in weight and have large flexibility, it havenumerous of advantages over copper wires at the time of installation. Since it is easy to install and have good compatibility with digital technology it saves time.
- **Saves Steps:**Sinceit possess no electrical conductivity, so grounding and protection are not required.
- **Provides Safe Transmission:**Since no leakage of any light, hence the transmission is secure and cannot be disturbed.
- **Good ability towork in Special Atmospheres:**Sinceit possess no electrical signals, thusno possibility of shock or other hazards. It makes optical Fibres suitable and sustainable to work in fieryatmospheres.
- **Portability:**Because of light weight and small size of the cable it has good capability of carrying a large number of signals.

Disadvantages of Fibre Optic Transmission:

- **High Installation Costs:**Fibre optic cables are very expensive to install but last longer than copper cables. Though installation costs are dropping near about 60% per year, still installation ofFibre optic cabling is comparativelycostly.
- **Special Test Equipment'sareoftenrequired:** The test equipment's that used typically and traditionally for conventional networking are of no use in a Fibre optic network. Expensive and specialized optical test equipment'slike Optical Time-Domain Reflectometer**(OTDR)** is required, and optical probes are needed in order to provide proper testing of optical Fibre.
- **Susceptible to Physical Damage:**Since it is small and compact, it is highly susceptible to physical damage during installation or construction activities.
- **Price:**Though the raw material requires for manufacturing optical Fibres, sand, is ampleand cheap.Still optical fibres are verycostly than copper cables.
- **Brittle in nature:** Optical Fibre cables are more brittle than electrical wires.
- **Chemicals Impact:**Various chemicals like hydrogen gas have adverse impact.
- **Opaqueness:** Most Fibre become opaque when exposed to radiation.
- **Special Skills Required:** Optical Fibre cannot be connected together as easily as copper cable. It requires special training and accurateconnecting and measurement equipment.

1.11.2 **Unguided media:**Unbound transmission media are the ways of transmitting data without using any cables. It uses wireless links hence known as unbounded media, and also known as unguided or wireless media. Unlike bound media, it transmits data without using any physical connectors between two communicating devices. It uses microwave, infrared or radio signals to transmit information. These media are not bounded by physical geography.

Unguided Media transmits electromagnetic waves without using a solid conductor. Electromagnetic waves do not require any media to propagate and can travel even through vacuum.

This type of transmission is called as**Wireless communication.**Now a day's wireless communication is becoming popular. Wireless LANs are being installed in office and college campuses. This transmission uses Microwave, Radio wave, Infra-red are some of popular unbound transmission media.

1.11.2.1 **Types of Communication Band:**The characteristics and quality of a data transmission are determined both bythe characteristics of the medium and the characteristics of the signal. In guided media, the medium is very important in determining the limitations oftransmission.

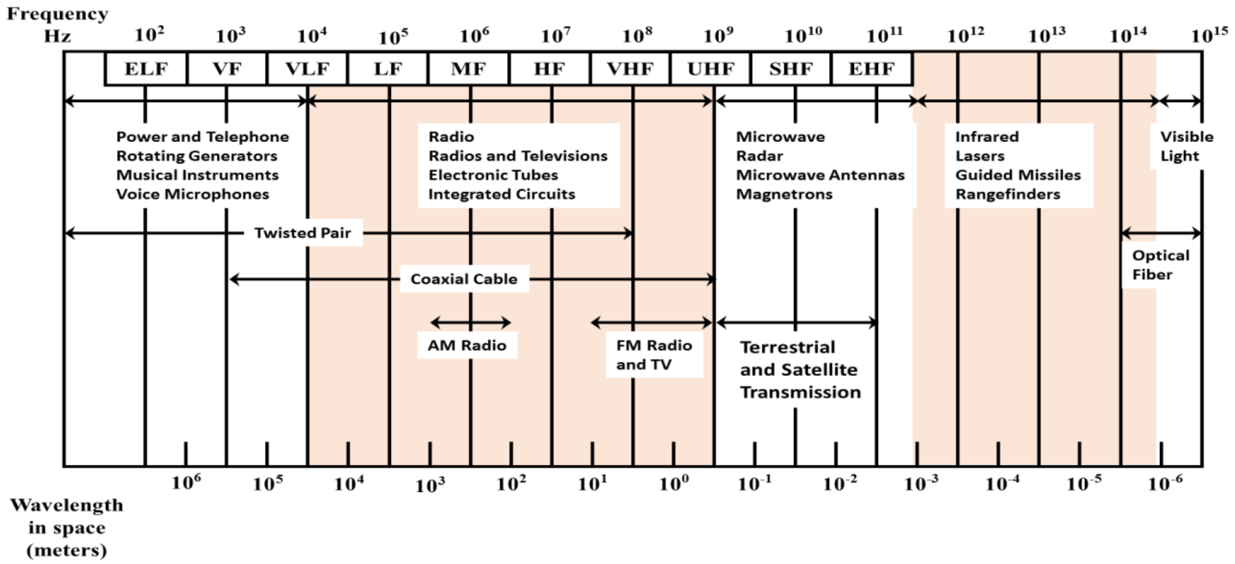
In unguided media, bandwidth of the signal produced by the transmittingantenna is more important than the medium in determining transmission characteristics.

Directionality is key property of signals transmitted by antenna. Normallylower signalfrequencies are omnidirectional, such signals propagates inall directions from the antenna. It is possible to focus higher frequencies signalinto a directional beam.

Key concernsin the design of data transmission systems are data transferrate and distance. Higher the data transfer rate, longer the distance.The designfactors that relates to the transmission medium and the signal determine the datarate and distance are:

- **Bandwidth:**Greater the bandwidthof a signal, higher the data rate that can be achieved.
- **TransmissionLosses:**Losses, such as attenuation, limit the distance.
- **Interference:** Interference from competing signals in overlapping frequency bands can distort or wipe out a signal.
- **Number of Receivers:** A guided medium can be used to construct a point-to point link or a shared link with multiple attachments. Each attachment beginssome attenuation and distortion on the line, which limits thedistance and/or data rate.

Electromagnetic spectrum is used for wireless communication. It is divided into various sub-bands.**Figure 3.9**shows the electromagnetic spectrum and indicates the frequenciesat which various guided media and unguided transmission techniques operate.



ELF = Extremely Low Frequency	MF = Medium Frequency	UHF = Ultrahigh Frequency
VF = Voice Frequency	HF = High Frequency	SHF = Super High Frequency
VLF = Very Low Frequency	VHF = Very High Frequency	EHF = Extremely High Frequency
LF = Low Frequency		

Figure 3.9: Electromagnetic Spectrum for Telecommunications

A signal radiated from an antenna propagates along one of three routes: ground wave,sky wave, or line of sight (LOS).Table 3.1 shows in which frequency range each predominates.

Band	Frequency Range	Free-Space Wavelength Range	Propagation Characteristics	Typical Use
ELF(extremely low frequency)	30 to 300 Hz	10,000 to 1000 km	GW	Power line frequencies: used by some home control systems
VF (voice frequency)	300 to 3000 Hz	1000 to 100 km	GW	Used by the telephone system for analog subscriber lines

VLF (very low frequency)	3 to 30 kHz	100 to 10 km	GW; low attenuation day and night; high atmospheric noise level	Long-range navigation; submarine communication
LF(low frequency)	30 to 300 kHz	10 to 1 km	GW; slightly less reliable than VLF;absorption in daytime	Long-range navigation; marine communication time radio beacons
MF (medium frequency)	300 to 3000 kHz	1000 to 100 m	GW and night SW; attenuation low atnight, high in day; atmospheric noise	Maritime radio; direction finding; AM broadcasting
HF (high frequency);	3 to 30 MHz	100 to 10 m	SW quality varies with time of day,season, and frequency	Amateur radio; international broadcasting,military communication; long-distance aircraft and ship communication
VHF (very highfrequency)	30 to 300 MHz	10 to 1 m	LOS; scattering because of temperatureinversion; cosmic noise	VHF television; FM broadcast and two-wayradio, AM aircraft communication; aircraft navigational aids
UHF (ultra-highfrequency)	300 to 3000 MHz	100 to 10 cm	LOS; cosmic noise	UHF television; cellular telephone; radar;microwave links; personal communications systems
SHF (super highfrequency)	3 to 30 GHz	10 to 1 cm	LOS; rainfall attenuation above 10 GHz; atmospheric attenuation due to oxygenand water vapour	Satellite communication; radar; terrestrial microwave links; wireless local loop
EHF (extremely frequency)	30 to 300 GHz	10 to 1 mm	atmospheric attenuation due to oxygen and water vapour	Experimental; high LOS; wireless local loop
Infrared	300 GHz to 400 THz	1 mm to 770 nm	LOS	Infrared LANs; consumer electronicapplications
Visible light	400 to 900 THz	770 to 330 nm	LOS	Optical communication

Table 4.1: Frequency Bands of Electromagnetic Spectrum

Wired Data communication frequencies:

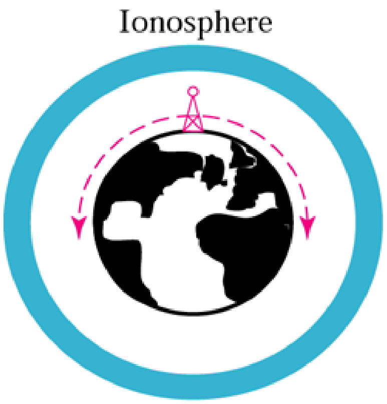
- Twisted Pair: 0 – 100MHz
- Coaxial Cable: 1 KHz – 1GHz
- Optical Fibre: 100 THz – 1PHz

Wireless Data Communication frequencies

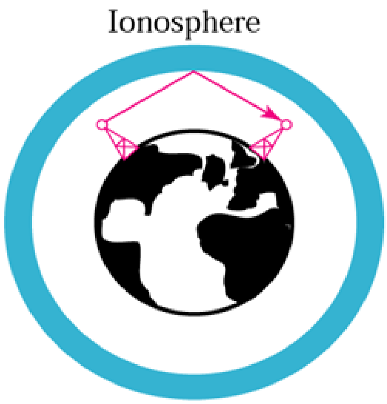
- AM Radio: 530 KHz – 1600KHz
- FM Radio: 88 MHz – 108Hz
- Terrestrial and Satellite / Microwave: 1 GHz – 1THz
- Infrared: 1 THz – 100THz

Signal Propagation Methods:

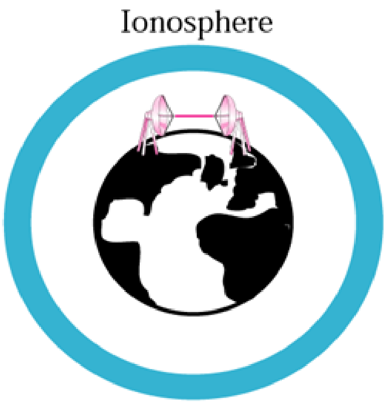
- **Ground Propagation**
- **Sky Propagation**
- **Line of Sight Propagation**



Ground propagation
(below 2 MHz)



Sky propagation
(2 - 30 MHz)



Line-of-sight propagation
(above 30 MHz)

- **Ground Propagation**: Radio waves travel through the lowest portion of the atmosphere following the curvature of the planet. Ground wave propagation more or less follows the contour of the earth and can propagate considerable distances, well over the visual horizon as shown in figure 3.10. This effect is found in frequencies up to about 2 MHz, Several factors account for the tendency of electromagnetic wave in this frequency band to follow the earth’s curvature. One factor is that the electromagnetic wave induces a current in the earth’s surface, the result of which is to slow the wave front near the earth, causing the wave front to tilt downward and hence follow the earth’s curvature. Another factor is diffraction, which is a phenomenon having to do with the behaviour of electromagnetic waves in the presence of obstacles.

Electromagnetic waves in this frequency range are scattered by the atmosphere in such a way that they do not penetrate the upper atmosphere.The best-known example of ground wave communication is AM radio.

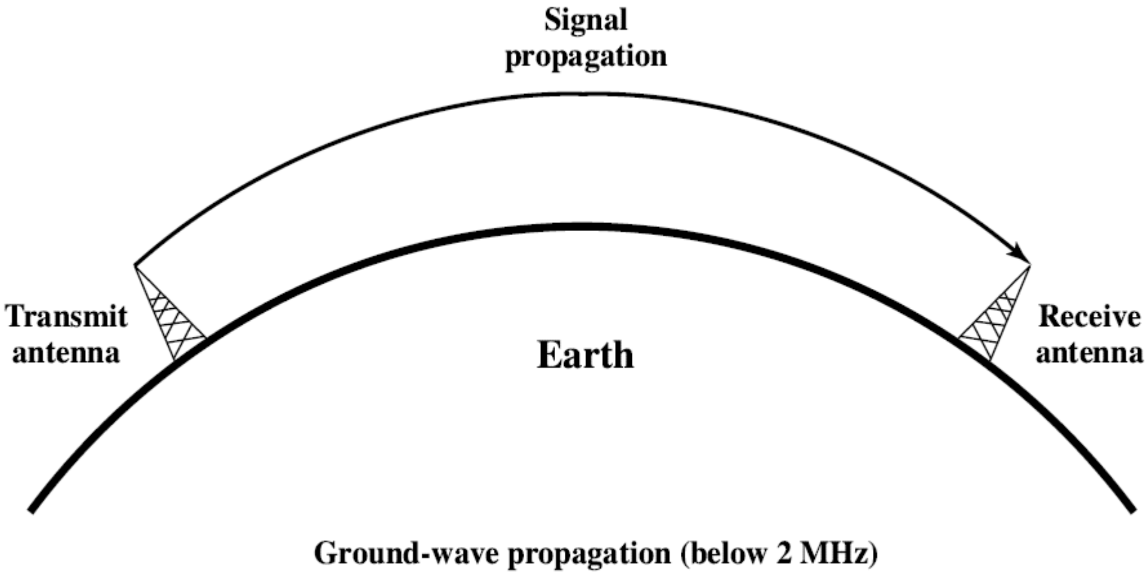


Figure 3.10: Ground Wave Propagation

- **Sky Propagation:** High frequency radio waves radiate upward into the ionosphere where they are reflected back to the earth. Sky wave propagation is used for amateur radio, CB radio, and international broadcasts such as BBC and Voice of America. With sky wave propagation, a signal from an earth-based antenna is reflected from the ionized layer of the upper atmosphere (ionosphere) back down to earth. Although it appears the wave is reflected from the ionosphere as if the ionosphere were a hard reflecting surface, the effect is in fact caused by refraction. Refraction is described subsequently.

  A sky wave signal can travel through a number of hops, bouncing back andforth between the ionosphere and the earth's surface as shown in figure 3.11.With this propagationmode, a signal can be picked up thousands of kilometres from the transmitter.

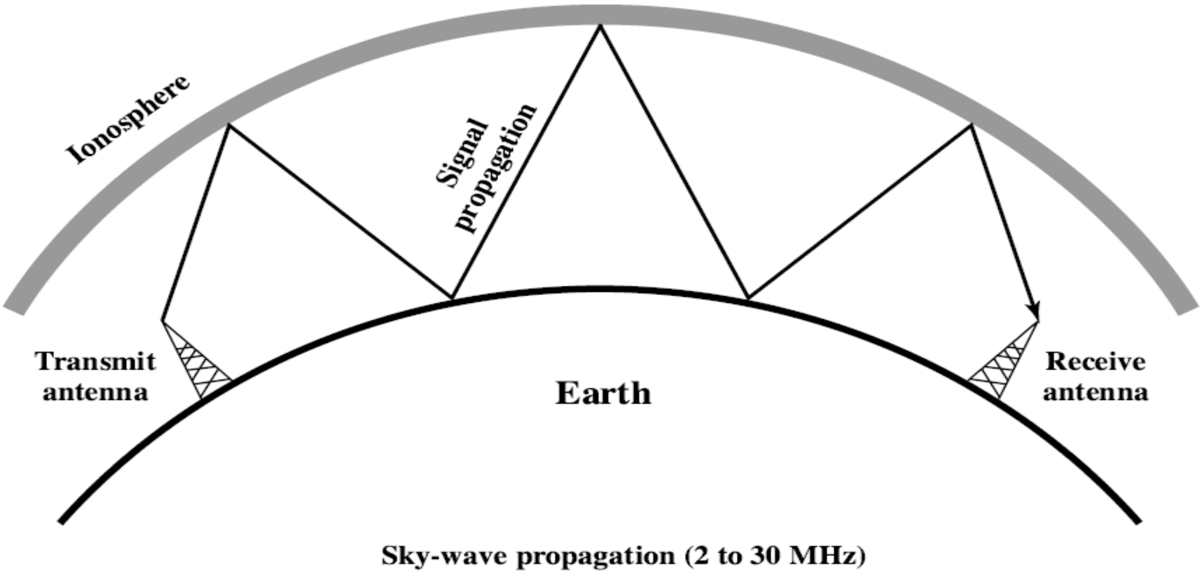


Figure 3.11: Sky Wave Propagation

- **Line-of-sight Propagation:**Very high frequency signals are transmitted in straight lines directly from antenna to antenna.Above 30 MHz, both ground wave and sky wave propagation modes do not operates, and communication must be by line of sight refer figure 3.12. For satellite communication, a signal above 30 MHz is not reflected by the ionosphere and therefore a signal can be transmitted between an earth station and a satellite overhead that is not beyond the horizon. For ground-based communication, the transmitting and receiving antennas must be within an effective line of sight of each other. The term effective is used because microwaves are bent or refracted by the atmosphere. The amount and even the direction of the bend depends on conditions, but generally microwaves are bent with the curvature of the earth and will therefore propagate farther than the optical line of sight.

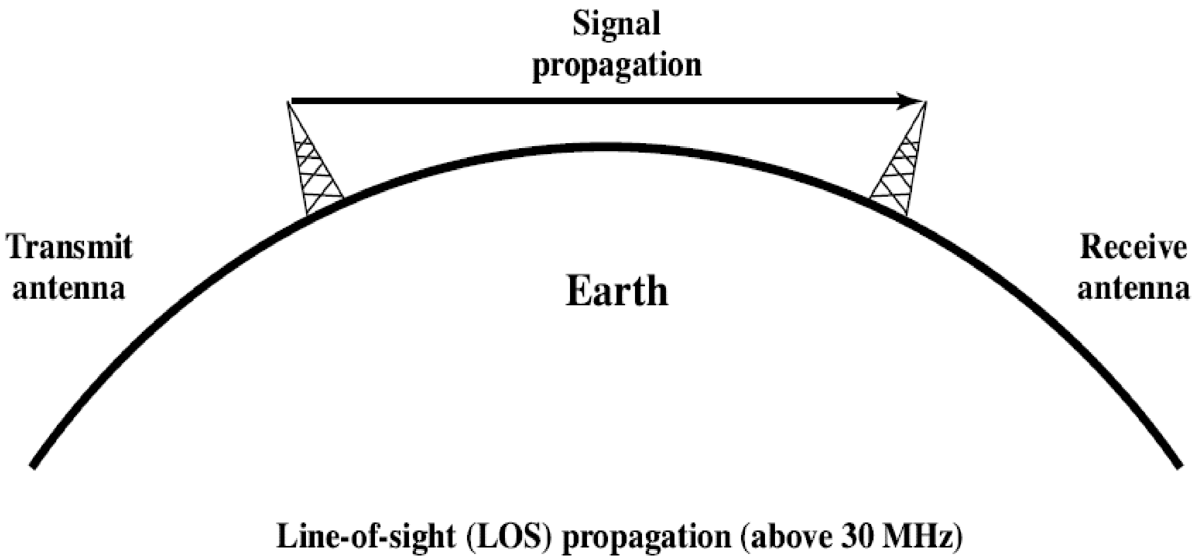


Figure 3.12: Line – of – Sight Propagation

Types of Wireless Communication:

- Microwave Communication
- Radio Wave Communication
  - Terrestrial Microwave
  - Satellite Microwave
- Infrared Communication

1.11.2.2 **Microwave Communication:**Microwave communication is method of wirelessly sending data.In microwave transmission information is transmitted by electromagnetic waves.A microwave is an electromagnetic wave with a very short wavelength, between .039 inches (1 millimetre) and 1 foot (30 centimetres). This part of the radio spectrum ranges across frequencies of roughly 1.0 gigahertz (GHz) to 300 GHz. These correspond to wavelengths from 30 centimetres down to 0.1 cm.

Within the electromagnetic spectrum, microwaves can be found between radio waves and shorter infrared waves. Their short wavelengths make microwaves ideal for use in radio and television broadcasting. They can transmit along a vast range of frequencies without causing signal interference or overlap.

Microwave is a powerful tool to transmit data at a long distance without using physical wires. Microwave communication is helpful in rural mountainous regions, where installing physical transmission lines is difficult and expensive. Microwave systems minimize installations and maintenance, as a signal microwave tower can transmit data across dozens of miles.

Microwave Transmission is divided into two types:

- **Terrestrial Microwave**
- **Satellite Microwave**

- **Terrestrial Microwave:** Terrestrial microwave communication employs Earth-based transmitters and receivers. The frequencies used are in the low-gigahertz range, which limits all communications to line-of-sight. Mostly used for long-distance telephone service. It uses radio frequency spectrum ranges from 2 to 40 GHz.

  The most common type of microwave antenna is the parabolic dish. A typical size is about 3 m in diameter. The antenna is fixed rigidly and focuses a narrow beam to achieve line-of-sight transmission to the receiving antenna. Microwave antennas are usually located at substantial heights above ground level to extend the range between antennas and to be able to transmit over intervening obstacles. To achieve long-distance transmission, a series of microwave relay towers is used, andpoint-to-point microwave links are strung together over the desired distance.

Application: Primarily terrestrial microwave systems are usedfor long distance telecommunicationservices, an alternative to coaxial cable and optical fibre. Microwave is mostly used in voice and television transmission.Microwave provides short point-to-point links between buildings. This can be used for closed-circuit TV or as a data link between local area networks.A business can establish a microwave link to a long-distancetelecommunications facility in the same city, bypassing the local telephone company.Another major use of microwave is in cellular systems

Power utilities use microwaves to remotely manage the power grid. Also used by public safety agencies like, police, fireman for remote monitoring and management. Many industries used microwave.

Band (GHz)	Bandwidth (MHz)	Data Rate (Mbps)
2	7	12
6	30	90
11	40	135
18	220	274

Typical Digital Microwave Performance

Advantages:

- The microwave spectrum has larger bandwidth and hence large amount of information can be transmitted using it.
- Microwave technology helps to manage crowded spectrum with the use of high selective receivers, modulation (SSB, PSK, QAM etc.) and spread spectrum techniques, data compression etc.
- Microwave spectrum is divided into different channels as per application.
- No cables needed
- Multiple channels available
- Wide bandwidth

Disadvantages:

- Standard circuit analysis can be applied only for the frequencies which are below 30MHz.
- Conventional transistors do not function properly at microwave frequency compare to lower frequency.
- Since microwave communication uses line of sight mode only,other modes of communication cannot be used.

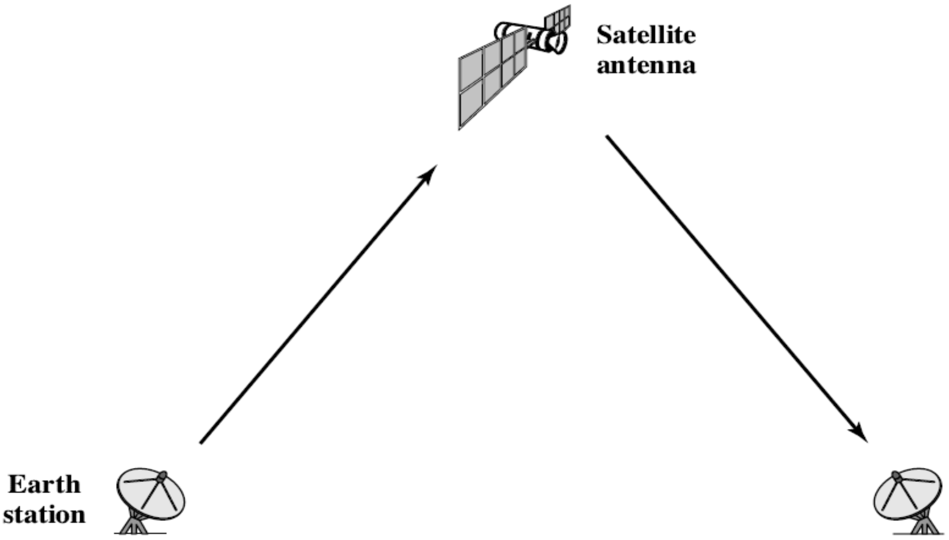
- Line-of-sight will be disrupted if any obstacle, such as new buildings, are in the way
- Signal absorption by the atmosphere. Microwaves suffer from attenuation due to atmospheric conditions.
- Towers are expensive to build

- **Satellite Microwave:**

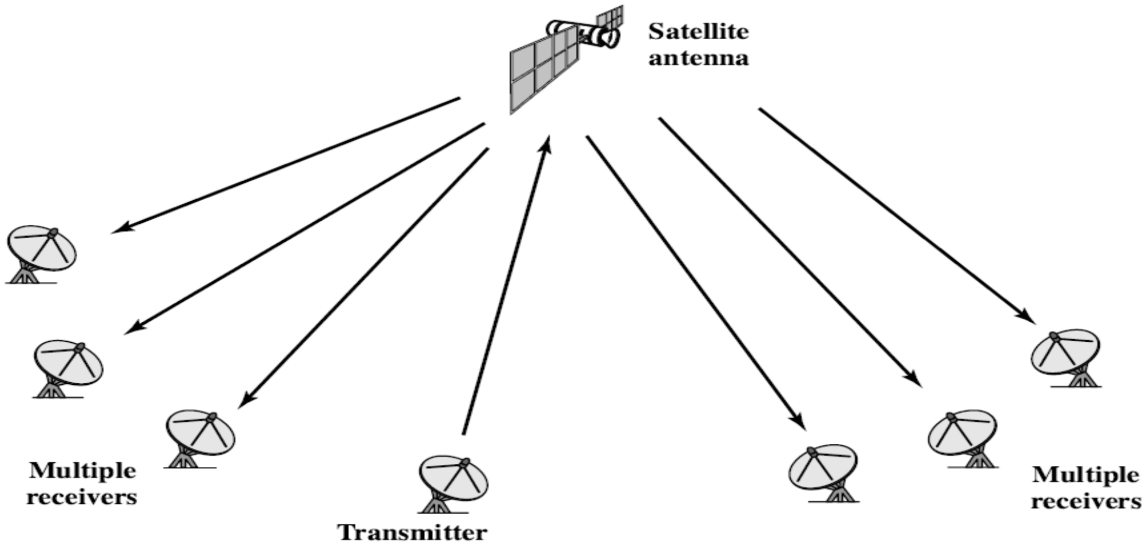
  A communication satellite is, in effect, a microwave relay station. It is used tolink two or more ground-based microwave transmitter/receivers, known as earthstations, or ground stations. The satellite receives transmissions on one frequencyband (uplink), amplifies or repeats the signal, and transmits it on another frequency(downlink). A single orbiting satellite will operate on a number of frequency bands,called transponder channels, or simply transponders.

  Figure 3.13shows a general way two common configurations for satellitecommunication. In the first, the satellite is being used to provide a point-to-pointlink between two distant ground-based antennas. In the second, the satellite providescommunications between one ground-based transmitter and a number ofground-based receivers.

  For a communication satellite to function effectively, it is generally requiredthat it remain stationary with respect to its position over the earth. Otherwise, itwould not be within the line of sight of its earth stations at all times.To remain stationary,the satellite must have a period of rotation equal to the earth's period of rotation.This match occurs at a height of 35,863 km at the equator.



(a) Point-to-point link



(b) Broadcast link

Figure 3.13: Satellite Communication Configurations

Two satellites using the same frequency band, if close enough together, will interferewith each other.To avoid this, current standards require a spacing (angulardisplacement as measured from the earth) in the 4/6-GHz band and a spacingat 12/14 GHz.Thus the number of possible satellites is quite limited.

Applications

The communication satellite is a technological revolution as important as fibreoptics. Among the most important applications for satellites are the following:

- Television Distribution
- Long-Distance Telephone Transmission
- Private Business Networks
- Satellite radio
- Satellite internet access

Types of Satellite by their purpose:

- Communication Satellite
- Weather satellite
- Remote- Sensing Satellite
- Scientific Satellite

Principal Satellite Transmission Bands

- **C band:**
  - 4(downlink) - 6(uplink) GHz
  - The first to be designated
- **Ku band:**
  - 12(downlink) -14(uplink) GHz
  - Rain interference is the major problem
- **Ka band:**

- 19(downlink) - 29(uplink) GHz
- Equipment needed to use the band is still very expensive

1.11.2.3 **Radio Wave Communication:** The principal difference between radio wave and microwave communication is that the radio wave is omnidirectional and the latter is microwave. Hence broadcast radio wave communication does not require dish-shaped antennas, and the antennas need not be rigidly mounted to a precise alignment. Electromagnetic waves ranging in frequency between 3 kHz and 1 GHz are normally called radio waves. A sending antenna sends waves that can be received by any receiving antenna. Radio waves, particularly of low and medium frequencies, can penetrate walls. It is an advantageous because, an AM radio can receive signals inside a building.It is disadvantageousas radio communication cannot be isolated to just inside or outside a building.

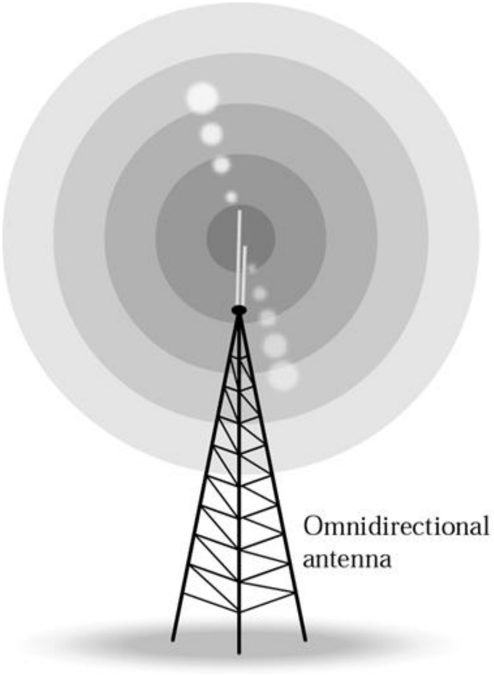


Figure 3.14 Radio Wave Communication

Applications

Radio is a general term used to encompass frequencies in the range of 3 kHz to

300 GHz.We are using the informal term broadcast radio to cover the VHF and partof the UHF band: 30 MHz to 1 GHz.This range covers FM radio and UHF and VHFtelevision.This range is also used for a number of data networking applications.

- AM and FM radio,
- Television,
- Maritime radio,

- Cordless phones and paging.

Self-Test (Multiple Choice Questions)

Self-test

1.11.2.4 **Infrared Communication:** Infrared communications is achieved using transmitters/receivers (transceivers) that modulate non-coherent infrared light. Transceivers must be within the line of sight of each other either directly or via reflection from a light-coloured surface suchas the ceiling of a room.

One important difference between infrared and microwave transmission isthat the former does not penetrate walls. Thus the security and interference problemsencountered in microwave systems are not present. Furthermore, there is nofrequency allocation issue with infrared, because no licensing is required.

Infrared signals, with frequencies from 300 GHz to 4 THz, can be used for short-range communication. Infrared signals, having high frequencies never pass through walls. This is advantageous when communication systems are separated by physical walls. However we cannot use infrared outside a building because the sun's rays contain infrared waves that interfere with the communication.

Applications

- TV Remote control
- Guidance in weapon system
- Wireless keyboards and mouse.

Advantages

- **Security:**Infrared communication has high directionality and can identify the person with whom you are communicating, which is different from wireless communication in which information diffuses, allowing for high confidentiality to be maintained.
- **Effect on the human body:** Infrared communication has no harmful effect on the human body.
- **Data communication speed:**Compared with the wireless communication with a maximum speed of about 100 Mbps, the infrared communication has a potential of 1 Gbps. It also has a much shorter wavelength than wireless communication, which is easily enough for broadband communication. It is optimal for when large-volume data such as video must be sent at a high speed.

Self-Test (Multiple Choice Questions)

Self-test

1.12 Latest Technologies in Wireless Network

1.12.1 Bluetooth Architecture: The Bluetooth technology was developed to provide a wireless interconnect between small mobile devices and their peripherals. The goals of the technology did not include developing another Wireless Local Area Network (WLAN) technology, for which there were already many in the market and many more being developed. Bluetooth technology was designed to connect mobile devices over apersonal and private connection

It uses radio frequency for communication and also maintains a high level of security. Robustness, low power and low cost are some of the key features of Bluetooth technology. A uniform structure is defined for a wide range of devices to connect and communicate with each other. Now Bluetooth is globally accepted that Bluetooth enabled devices, which is almost everywhere in the world can connect to other devices in proximity.

Bluetooth architecture defines two types of networks:

- Piconet
- Scatternet

Piconet: Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.Thus, piconet can have upto eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.There can be only one primary or master station in each piconet.The communication between the primary and the secondary can be one-to-one or one-to-many.All communication is between master and a slave. Salve-slave communication is not possible.In addition to seven active slave station, a piconet can have upto 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.

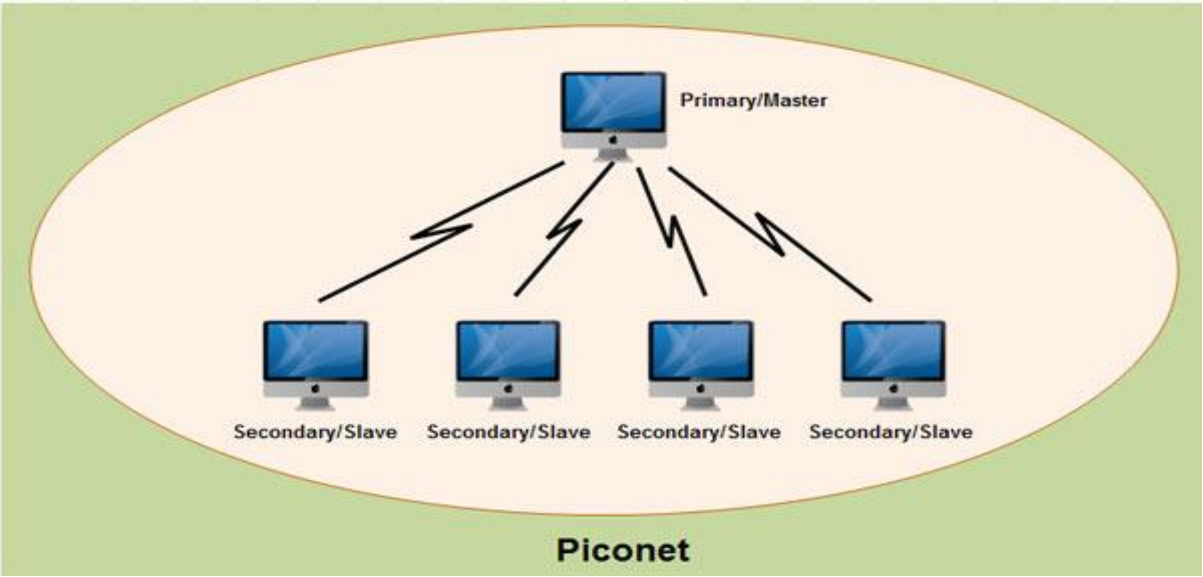


Figure 3.14: Piconet

Scatternet: Scattemet is formed by combining various piconets.A slave in one piconet can act as a master or primary in other piconet.Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.Thus a station can be a member of two piconets.A station cannot be a master in two piconets.

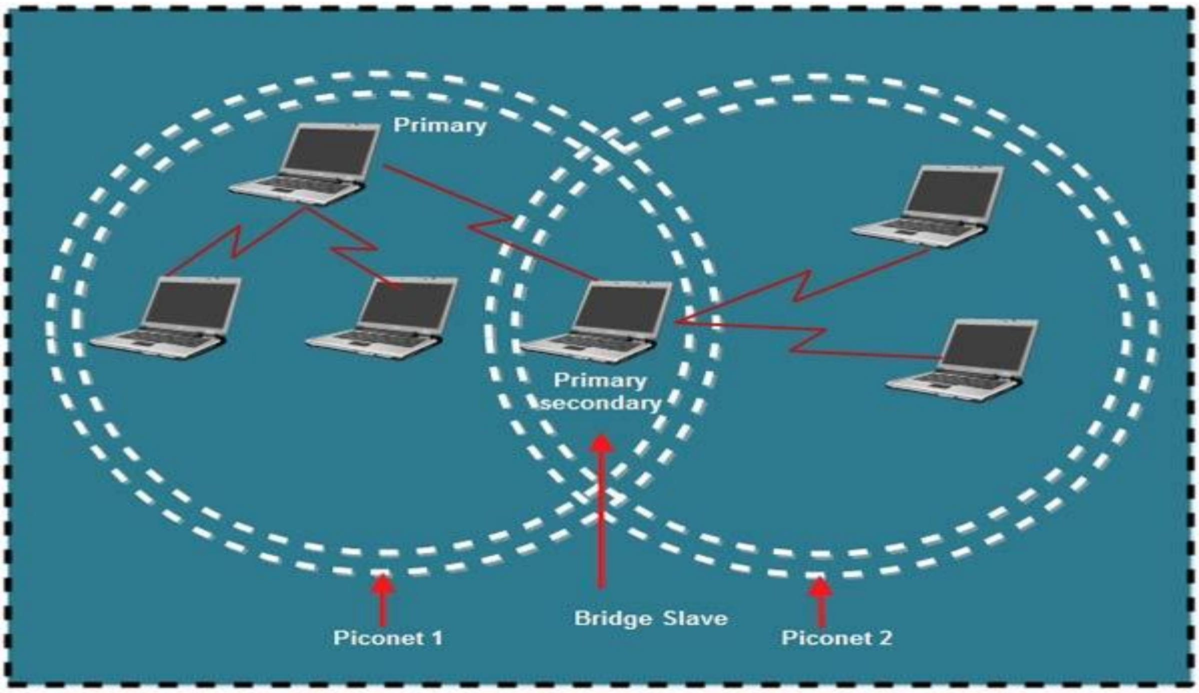


Figure 3.15: Scatternet

Bluetooth layers and Protocol Stack: Bluetooth standard has many protocols that are organized into different layers.The layer structure of Bluetooth does not follow OS1 model, TCP/IP model or any other known model.The different layers and Bluetooth protocol architecture.

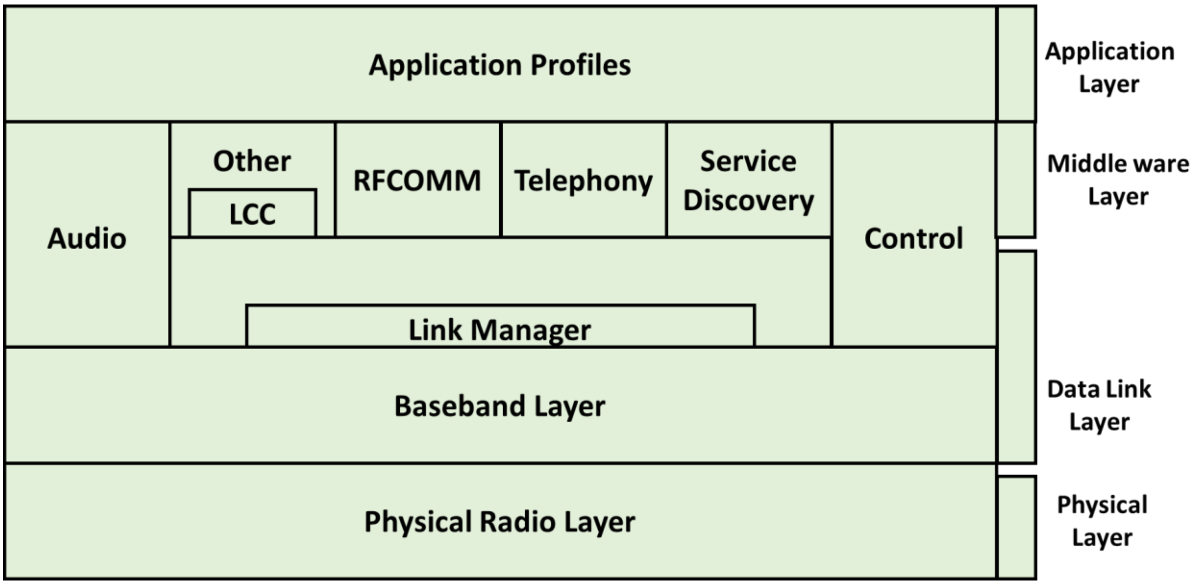


Figure 3.16: Bluetooth Layer and Protocol Architecture

Radio Layer: The Bluetooth radio layer corresponds to the physical layer of OSI model.It deals with ratio transmission and modulation.The radio layer moves data from master to slave or vice versa.It is a low power system that uses 2.4 GHz ISM band in a range of 10 meters.This band is divided into 79 channels of 1MHz each. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or networks.Bluetooth hops 1600 times per second, i.e. each device changes its modulation frequency 1600 times per second.In order to change bits into a signal, it uses a version of FSK called GFSK i.e. FSK with Gaussian bandwidth filtering.

Baseband Layer: Baseband layer is equivalent to the MAC sublayer in LANs.Bluetooth uses a form of TDMA called TDD-TDMA (time division duplex TDMA).Master and slave stations communicate with each other using time slots.The master in each piconet defines the time slot of 625 µsec.In TDD-TDMA, communication is half duplex in which receiver can send and receive data but not at the same time.If the piconet has only no slave; the master uses even numbered slots (0, 2, 4 ...) and the slave uses odd-numbered slots (1, 3, 5 ...). Both master and slave communicate in half duplex mode. In slot 0, master sends & secondary receives; in slot 1, secondary sends and primary receives.If piconet has more than one slave, the master uses even numbered slots. The slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.

In Baseband layer, two types of links can be created between a master and slave. These are:

1. **Asynchronous Connection-less (ACL):** It is used for packet switched data that is available at irregular intervals. ACL delivers traffic on a best effort basis. Frames can be lost & may have to be retransmitted. A slave can have only one ACL link to its master. Thus ACL link is used where correct delivery is preferred over fast delivery. The ACL can achieve a maximum data rate of 721 kbps by using one, three or more slots.
2. **Synchronous Connection Oriented (SCO):**SCO is used for real time data such as sound. It is used where fast delivery is preferred over accurate delivery.In an SCO link, a physical link is created between the master and slave by reserving specific slots at regular intervals.Damaged packet; are not retransmitted over SCO links.A slave can have three SCO links with the master and can send data at 64 Kbps.Logical Link, Control Adaptation Protocol Layer (L2CAP). The logical unit link control adaptation protocol is equivalent to logical link control sublayer of LAN.The ACL link uses L2CAP for data exchange but SCO channel does not use it.

The various functions of L2CAP are:

1. **Segmentation and reassembly:** L2CAP receives the packets of upto 64 KB from upper layers and divides them into frames for transmission.It adds extra

information to define the location of frame in the original packet. The L2CAP reassembles the frame into packets again at the destination.

2. **Multiplexing:**L2CAP performs multiplexing at sender side and demultiplexing at receiver side.At the sender site, it accepts data from one of the upper layer protocols frames them and deliver them to the Baseband layer. At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol1ayer.
3. **Quality of Service (QOS):**L2CAP handles quality of service requirements, both when links are established and during normal operation.It also enables the devices to negotiate the maximum payload size during connection establishment.

Bluetooth Frame Format

The various fields of blue tooth frame format are:

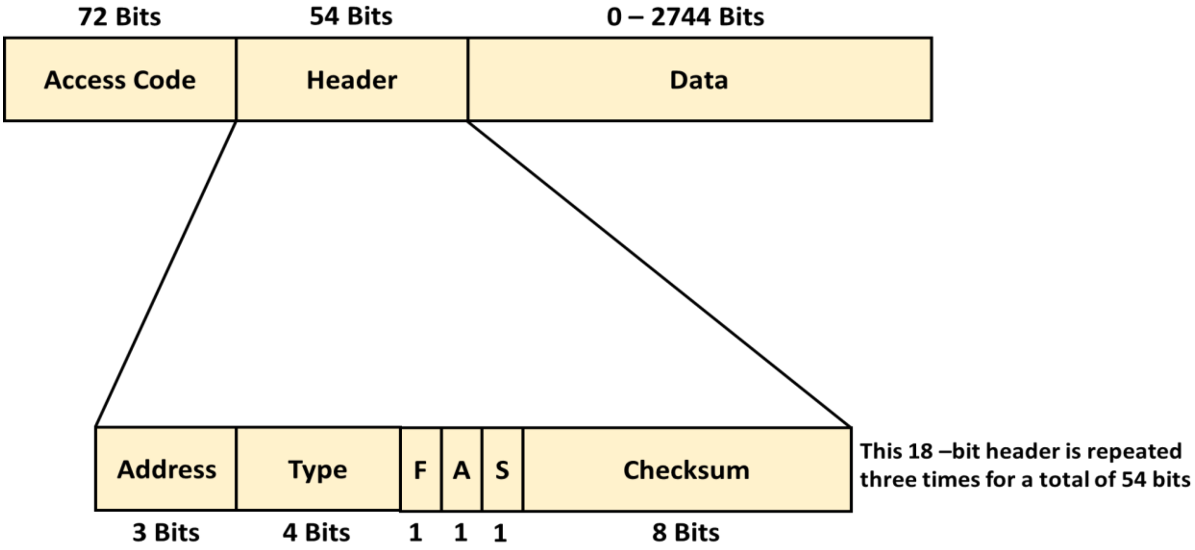


Figure 3.17: Bluetooth Frame format

1. **Access Code:** It is 72 bit field that contains synchronization bits. It identifies the master.
2. **Header:** This is 54-bit field. It contain 18 bit pattern that is repeated for 3 time.

The header field contains following subfields:

- **Address:** This 3 bit field can define up to seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondary's.
- **Type:** This 4 bit field identifies the type of data coming from upper layers.
- **F:** This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.
- **A:** This bit is used for acknowledgement.

- **S:** This bit contains a sequence number of the frame to detect retransmission. As stop and wait protocol is used, one bit is sufficient.
- **Checksum:** This 8 bit field contains checksum to detect errors in header.

3. **Data:** This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers

1.12.2 **Wi-Fi:**Wi-Fi is the name of a popular wireless networking technology which provide wireless high-speed Internet and network connections using radio waves. In Wi-Fi networks there is no physical connection between sender and receiver, they are connected by using radio frequency (RF).

The foundation of any wireless network is an access point (AP). The main job of an access point is to transmit a wireless signal that computers can detect and "tune" into. To connect to an access point and to join a wireless network, computers and devices must be equipped with wireless network adapters.

Wi-Fi is supported by many applications and devices including video game consoles, home networks, PDAs, mobile phones, major operating systems, and other types of consumer electronics.Wi-Fi or Wireless Fidelity has a range of about 100m and allows for faster data transfer rate between 10 - 54Mbps.

There are three different wireless standards under Wi-Fi, 802.11a, 802.11b and 802.11g.802.11 being the wireless standard set by The Institute of Electrical and Electronic Engineers (IEEE).Wi-Fi is used to create wireless Local Area Networks (WLAN).The most widely used standard is 802.11b and 802.11g is expected to grow rapidly.

These two standards are relatively inexpensive and can be found providing wireless connectivity in airports, railway stations, cafes, bars, restaurants and other public areas.The main difference between the two is the speed. 802.11b has data transfer rate of upto 11Mbps and 802.11g has a rate of upto 54Mbps.802.11g is a relatively new and has yet to be adopted widely. 802.11a is more expensive and as a result it not available for public access.

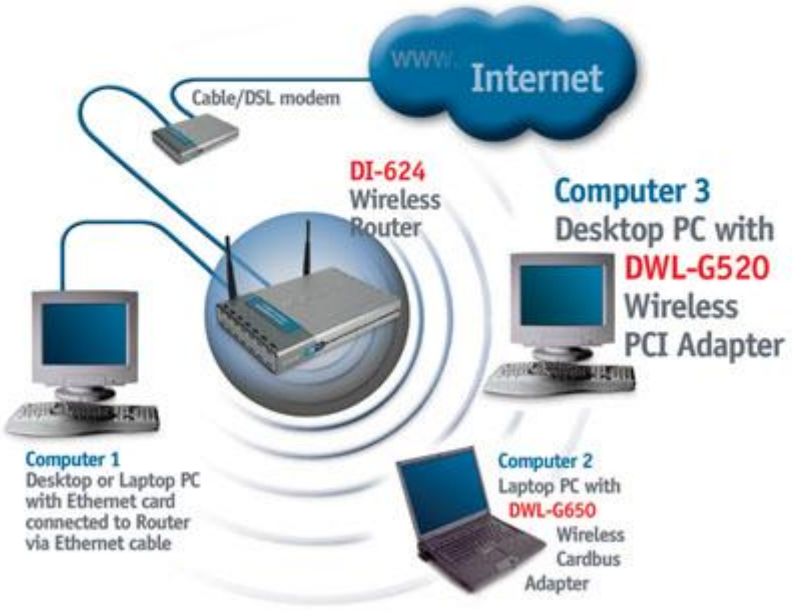


Figure 3.15: Wi-Fi network

1.12.3 **Wi- Max:**WiMAX is one of the hottest broadband wireless technologies around today.WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way.WiMAX is a type of wireless communication standards based on the IEEE 802.16 set of standards that provides multiple physical layer and Media Access Control options.

In fact Wi-MAX is:

- Abbreviation for Worldwide Interoperability for Microwave Access.
- Based on Wireless MAN technology.
- A wireless technology optimized for the delivery of IP centric services over a wide area.
- A scalable wireless platform for constructing alternative and complementary broadband networks.
- A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard.
- The IEEE 802.16 Working Group develops standards that address two types of usage models:
  - A fixed usage model (IEEE 802.16-2004)
  - A portable usage model (IEEE 802.16e)

WiMAX network design is based on the following major principles:

- **Spectrum:**Capablein deployed in both licensed and unlicensed spectra.
- **Topology:** supports different Radio Access Network (RAN) topologies.
- **Interworking:**Provides an independent RAN architecture to enable seamless integration and interworking with Wi-Fi, 3GPP and 3GPP2 networks and existing IP operator core network.
- **IP Connectivity:**It supports combination of IPv4 and IPv6 network to interconnect clients and application servers.
- **Mobility management:**It is possible to extend the fixed access to mobility and broadband multimedia services delivery.

WiMAX can provide two forms of wireless service −

- **Non-line-of-sight service:**It is a Wi-Fi sort of service. Here a small antenna on a computer connects to the WiMAX tower. In this mode, WiMAX uses a lower frequency range from 2 GHz to 11 GHz that is similar to Wi-Fi.
- **Line-of-sight service:** Where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. The line-of-sight connection is stronger and more stable, so it's able to send a lot of data with fewer errors. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz.

WiMAX operates on two frequency bands, 2 - 11GHz and 10 - 66GHz and has a range of about 50km with speeds of upto 80Mbps.This enables smaller wireless LANs to be interconnected by WiMAX creating a large wireless MAN.Networking between cities can be achieved without the need for expensive cabling.It is also able to provide high speed wireless broadband access to users.As it can operate in two frequency bands WiMAX can work by line-of-sight and non-line-of-sight.At the 2 - 11GHz frequency range it works by non-line-of-sight, where a computer inside a building communicates with a tower/antenna outside the building.

Short frequency transmissions are not easily disrupted by physical obstructions.Higher frequency transmissions are used for non-line-of-sight service.This enables to towers/antennae to communicate with each other over a greater distance.Due to infrastructure and costs involved it would be more suited to provide the backbone services for ISPs and large corporations providing wireless networking and internet access.

Comparison of Wireless Technologies:

Technology→	**Bluetooth**	**Wi-Fi (a)**	**Wi-Fi (b)**	**Wi-Fi (g)**	**WiMAX**
Standard	802.15	802.11a	802.11b	802.11g	802.16
Frequency (GHz)	2.45	5	2.4	2.4	2 - 66

Speed (Mbps)	0.72	54	11	54	80
Range	10m	50m	100m	100m	50km
Advantages	Low Cost	Speed	Low Cost	Speed	Speed, Range
Disadvantages	Range	Cost	Speed	Cost, Range	Cost

Solved Problems

Solved problem

Self-Test (Multiple Choice Questions)

Self-test

1.13 **Cellular (Mobile) Telephone:**Cellular communication is designed to provide communications between two moving units, or between one mobile unit and one stationary phone or land unit (PSTN). The entire network coverage area is divided into cells based on the principle of frequency reuse. A Cell -basic geographical unit of a cellular network; is the area around an antenna where a specific frequency range is used. Cell is represented graphically as a hexagonal shape, but in reality it is irregular in shape. A cluster is a group of adjacent cells, usually 7 cells; no frequency reuse is done within a cluster. In heavy traffic zones cells are smaller, while in isolated zones cells are larger.

1.13.1 **Band in Cellular Telephony:**Analog transmission is used for cellular telephony. Frequency modulation is used for communication between the mobile phone and cell office. Two frequency bands are allocated for this purpose. One band of them is for the communication that is initiated by mobile phone & the other band for the land phone. Each channel requires a full-duplex dialog.

For preventing interference, adjacent channels are rarely allocated; some of them are also required for control purposes. This reduces the number of channels available for each cell.

- GSM uses FDMA and TDMA to transmit voice and data
- The uplink channel - between the cell phone and the BTS uses FDMA
- The downlink channel- between the BTS and the cell phone uses a TDMA technique.
- Uplink and downlink channels have a bandwidth of 25 MHz
- Each uplink and downlink frequency bands is further split up as Control Channel (used to set up and manage calls) and Traffic Channel (used to carry voice).

GSM Frequency band	**Uplink/BTS Transmit**	**Downlink/BTS Receive**
900 MHz	935-960 MHz	890-915 MHz
1800 MHz	1805-1880 MHz	1710-1785 MHz
1900 MHz	1930-1990 MHz	1850-1910 MHz

The same frequency band can be used for multiple non-adjacent cells as shown in figure 3.16.

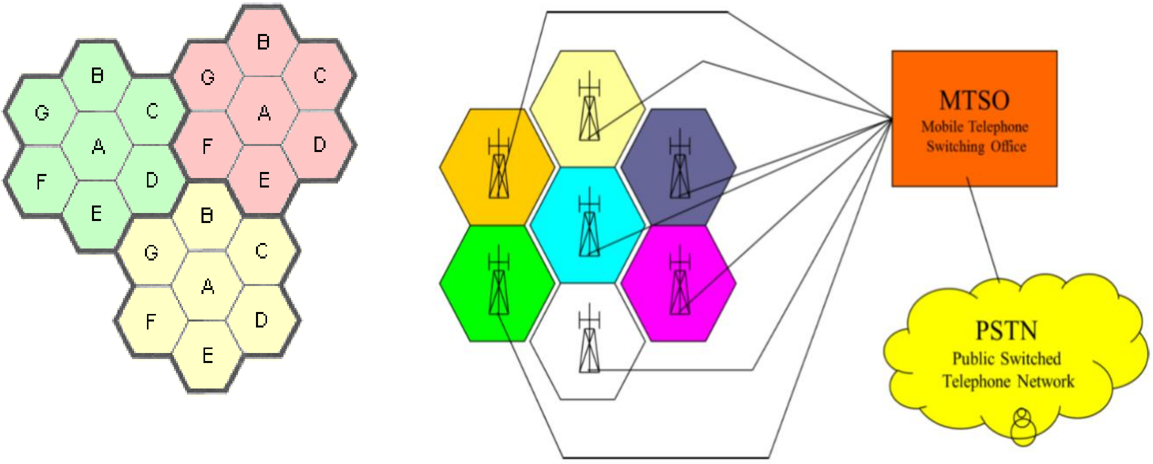


Figure 3.16: Frequency band for multiple non-adjacent cells

1.13.2 Calls using Mobile Phones:

- Call is made from the mobile phone by entering 10-digit phone number. The mobile phone itself scans the band & seeks a channel for setting up the call.
- After seeking, it sends this number to the closest cell office, which in turn, sends it to the CTO.
- If the called party is available, CTO lets MTSO (mobile telephone switching office) know.
- At this point, MTSO allocates an empty voice channel to the cell to establish the connection.
- The mobile phone adjust its tuning to the new channel & the dialog begins.
- Transmitting receiving / Handoff operations.

Call from Land Phone to a mobile phone,

- The telephone central office sends the number to the MTSO.
- The MTSO performs a lookup to see where the mobile phone is currently placed by sending appropriate query signal to all the cells.
- This process is known paging.
- The cell where the mobile phone is currently located responds to the MTSO. Incoming calls work differently.
- To start with idle phone is continuously listen to paging channel to detect messages at directed at them.
- The MTSO then transmit the incoming call signal to that mobile phone & when the mobile phone is answered

Transmitting/Receiving/Handoff Operation

Define the process of hand-over

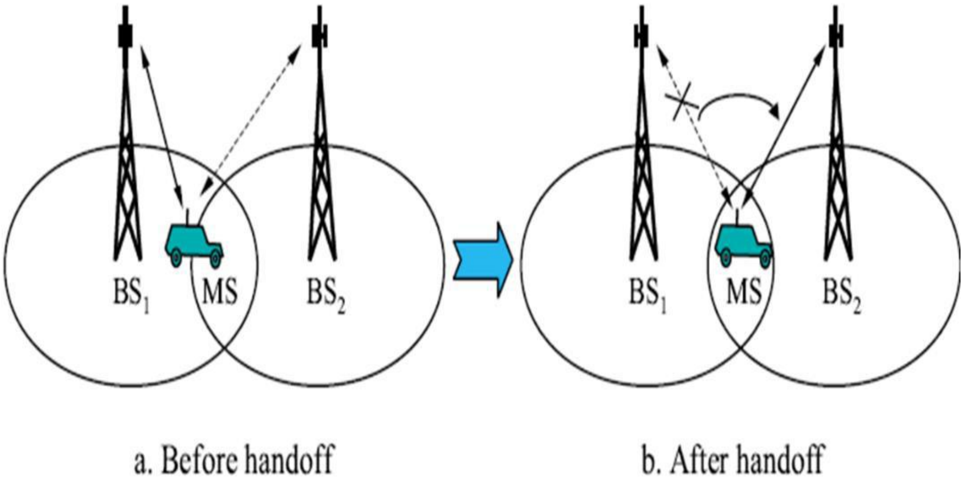
- When a mobile moves into a different cell while a conversation is in progress, the MSC automatically transfers the call to a new channel belonging to the new base station.
- This handoff operation not only involves identifying a new base station, but also requires that the voice and control signals be allocated to channels associated with the new base station.
- Processing handoffs is an important task in any cellular radio system.

Handoff

- When a mobile user is engaged in conversation, the MS is connected to a BS via a radio link.
- If the mobile user moves to the coverage area of another BS, the radio link to the old BS is eventually disconnected, and a radio link to the new BS should be established to continue the conversation.
- This process is referred to as automatic link transfer, handover, or handoff.

1. **Hard Hand Off**

- In Hard Hand Off a mobile station only communicates with one base station.
- When the (mobile handset) MS moves from one cell to another, communication must first be broken with the previous base station before communication can be re-established with the new one.
- This may create a rough transition.
- Hard hand off was used in earlier systems.



2. **Soft Hand Off**

- In this case, a mobile station can communicate with two base stations at the same time this means that, during Hand off a mobile station may continue with the new base station before breaking off from the old one.
- This is used in new systems.
- This provides seamless connectivity while roaming from one cell to another.
- Roaming

- Roaming refers to a wireless network service extension in an area that differs from the registered home network location.
- Roaming enables a mobile device to access the Internet and other mobile services when out of its normal coverage area.
- It also gives a mobile device the ability to move from one access point to another.

Solved Problems

Solved problem

Self-Test (Multiple Choice Questions)

Self-test

1.14 Summary
1.15 Exercise (short answer questions)
1.16 References
1.16.1 Books
1.16.2 Wikipedia
1.16.3 MOOCs
1.16.4 YouTube Videos
1.16.5 OER

Unit4: Network Architecture and Protocols

1.17 Learning Objectives: After successful completion of this unit, you will be able to:

- Understand concept of Layered Architecture
- State the requirement for layered approach
- Explain the basic concept of layering in the network model
- Understand concept of Peer-to- Peer Processes
- Understand concept ofProtocols
- Define entities protocols in networking context
- Understand concept ofEncapsulation

1.18 **Layered Architecture:**A technique used in designing computer software, hardware, and communications in which system or network components are isolated in layers so that changes can be made in one layer without affecting the others.

Networking engineering is a complicated task, which involves software, firmware, chip level engineering, hardware, and electric pulses. To ease network engineering, the whole networking concept is divided into multiple layers. Each layer is involved in some particular task and is independent of all other layers. But as a whole, almost all networking tasks depend on all of these layers. Layers share data between them and they depend on each other only to take input and send output.

To reduce the design complications, most of the networks are organized as a series of layers or levels, each one build upon one below it. The basic idea of a layered architecture is to divide the design into small pieces. Each layer adds to the services provided by the lower layers in such a manner that the highest layer is provided a full set of services to manage communications and run the applications. The benefits of the layered models are modularity and clear interfaces, i.e. open architecture and comparability between the different providers' components.

A basic principle is to ensure independence of layers by defining services provided byeach layer to the next higher layer without defining how the services are to be performed.This permits changes in a layer without affecting other layers. Prior to the use of layeredprotocol architectures, simple changes such as adding one terminal type to the list ofthose supported by an architecture often required changes to essentially allcommunications software at a site. The number of layers, functions and contents of eachlayer differ from network to network. However in all networks, the purpose of each layeris to offer certain services to higher layers, shielding those layers from the details of howthe services are actually implemented.

The basic elements of a layered model are services, protocols and interfaces. A service isa set of actions that a layer offers to another (higher) layer. Protocol is a set of rules that alayer uses to exchange information with a peer entity. These rules concern both thecontents and the order of the messages used. Between the layers service interfaces aredefined. The messages from one layer to another are sent through those interfaces.

1.18.1 Layered Tasks:

In layered architecture of Network Model, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work.

In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by the-top most layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and passes on to lower layer. If the task is initiated by lower most layer, then the reverse path is taken.

Every layer clubs together all procedures, protocols, and methods which it requires to execute its piece of task. All layers identify their counterparts by means of encapsulation header and tail.

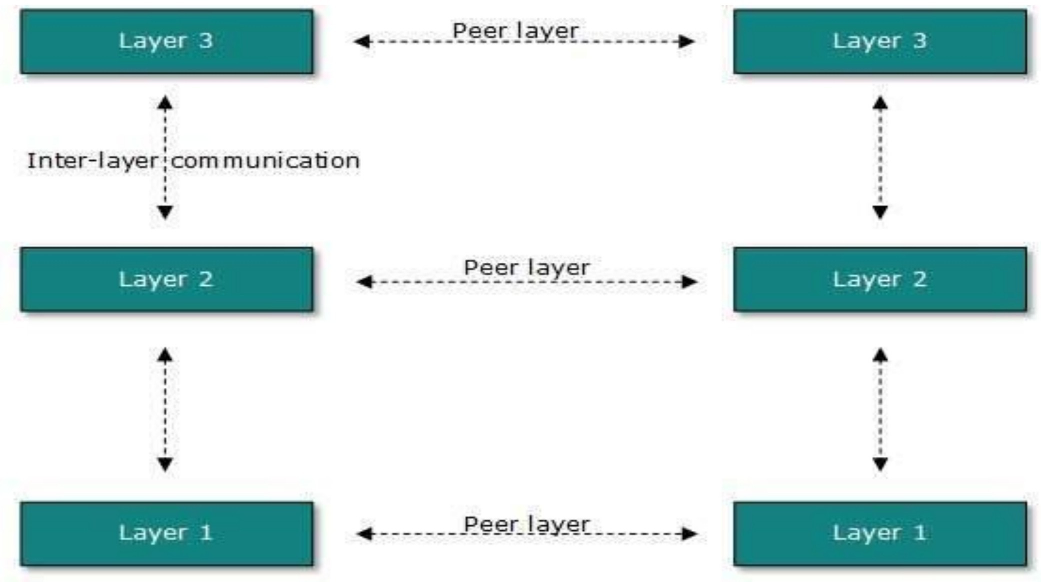


Figure 4.1 Layered Architecture

1.18.2 Benefits of Layered Architecture:

- It increases flexibility, maintainability, and scalabilityto modify and develop network services.
- It enables teams to work on different parts of the application parallel with minimal dependencies on other teams.
- It also helps you to test the components independently of each other.
- Different components of the application can be independently deployed, maintained, and updated, on different time schedules.
- It also allows us to accommodate too network users within the limitation of 4-byte address space with the help of Subnetting and CIDR and similar concepts.
- It enables us to maintain security along with privacy in an easier way.
- It simplifies the design process as the functions of each layers and their interactions are well defined.
- The number of layers, name of layers and the tasks assigned to them may change from network to network. But for all the networks, always the lower layer offers certain services to its upper layer.
- The concept of layered architecture redefines the way of convincing networks. This leads to a considerable cost savings and managerial benefits.

- Addition of new services and management of network infrastructure become easy.
- Due to segmentation, it is possible to break complex problems into smaller and more manageable pieces.
- Logical segmentation helps development taking place by different terms.

a. Why layered architecture is used in OSI reference model? Discuss

b. Give benefits of Layered Architecture

1.19 **Peer-to- Peer Processes:**The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.At the physical layer, communication is direct: In **Figure 4.2**, device A sends a stream of bits to device B (through intermediate nodes). At the higher layers, however, communication must move down through the layers on device A, over to device B, and thenback up through the layers. Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.

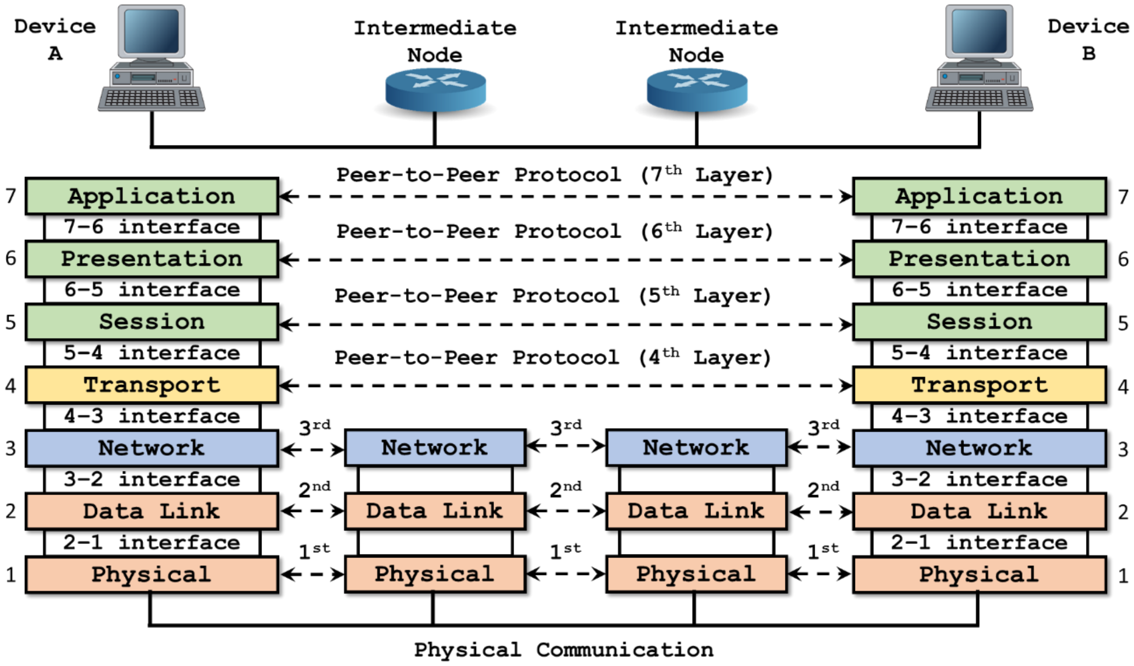


Figure 4.2: The interaction between layers in the OSI model

At layer 1 the entire package is converted to a form that can be transmitted to the receiving device. At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.

Functions of each of the layer are described below:

1. **Physical Layer:** It is responsible for movements of individual bits from one hop (node) to the next.

Functions:

i. To activate, maintain and deactivate the physical connection
ii. To define voltages and data rates needed for transmission
iii. To convert digital bits into electrical signal
iv. To decide whether the transmission is simplex, half-duplex or full-duplex.
v. A physical layer is concerned with the connection of devices to the media (Line configuration).
vi. It also defines the physical topology.
vii. It also helps in synchronization of bits.

2. **Data Link layer:** It transforms the physical layer, a raw transmission facility to a reliable link. It is responsible for moving frames from one hop (node) to the next i.e. Hop-to-Hop delivery.

Functions:

i. Framing: The layer divides the stream of bits received from the network layer into manageable data units called frames.
ii. Physical addressing: It adds a header to the frame to define the physical address of the sender and/or receiver of the frame.
iii. Flow Control: It provides a flow control mechanism to avoid a fast transmitter from over-running a slow receiver by buffering the extra bits.
iv. Error control: It is achieved by adding a trailer at the end of the frame. It also uses a mechanism to prevent duplication of frames.
v. Access Control: The layer determines which device has control over the link at any given time, when two or more devices are connected to the same link.

3. **Network Layer:** The network layer is responsible for the delivery of individual packets from the source host to the destination host i.e End to End delivery or source to destination delivery.

Functions:

i. It translates logical network address into physical machine address i.e. the numbers used as destination IDs in the physical network cards.
ii. It determines the quality of service by deciding the priority of message and then route a message will take if there are several ways a message can get to its destination.
iii. It breaks the larger packets into smaller packets if the packet is larger than the largest data frame the data link will accept
iv. Routers and gateways operate in the network layer.

4. Transport layer: It is responsible for process-to-process delivery of the entire message i.e. source to destination delivery of the entire message. It ensures that the whole message arrives intact and in order, ensuring both error control and flow control at source destination level.

Functions:

i. Segmentation and re-assembly: It divides each message into packets at the source and reassembles than at the destination.
ii. Service point addressing: The transport layer header H4 includes service point to deliver a specific process from source to a specific process at the destination.
iii. Connector Control: The layer can be either connectionless or connection oriented.
iv. Flow Control: It provides end-to-end flow control rather than across a single link.
v. Error Control: It ensures that the entire message arrives at the receiving transport layer without error.

5. Session Layer: It is responsible for dialog control and synchronization i.e it is network dialog controller. It establishes maintains and synchronizes the interaction among communicating systems.

6. Presentation Layer: It is responsible for translation, compression and encryption. It is concerned with the syntax and semantics of the information exchanged between two systems.

7. Application Layer: It is responsible for providing services to the user. It provides services that directly support user application such as database access, e-mail, file transfer.

Functions:

i. Network virtual terminal: The layer creates a software emulation of a terminal at the remote host. The user’s computer tasks to the software terminal, then the software terminal talks to the host and vice versa. The remote host feels that it is communicating with one of its own terminal and allows you to log on.
ii. Directory services: It provides distributed database sources and access to the worldwide information about various objects and services.

1.19.1 **Interfaces between Layer:**The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers. Each interface defines the information and services a layer must provide for the layer above it. Well-defined interfaces and layer functions provide modularity to a network. As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

1.19.2 **Organization of the Layers:**The seven layers can be thought of as belonging to three subgroups. Layers 1, 2, and 3-physical, data link, and network-are the network support layers; they deal withthe physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability). Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability among unrelated software systems. Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

c

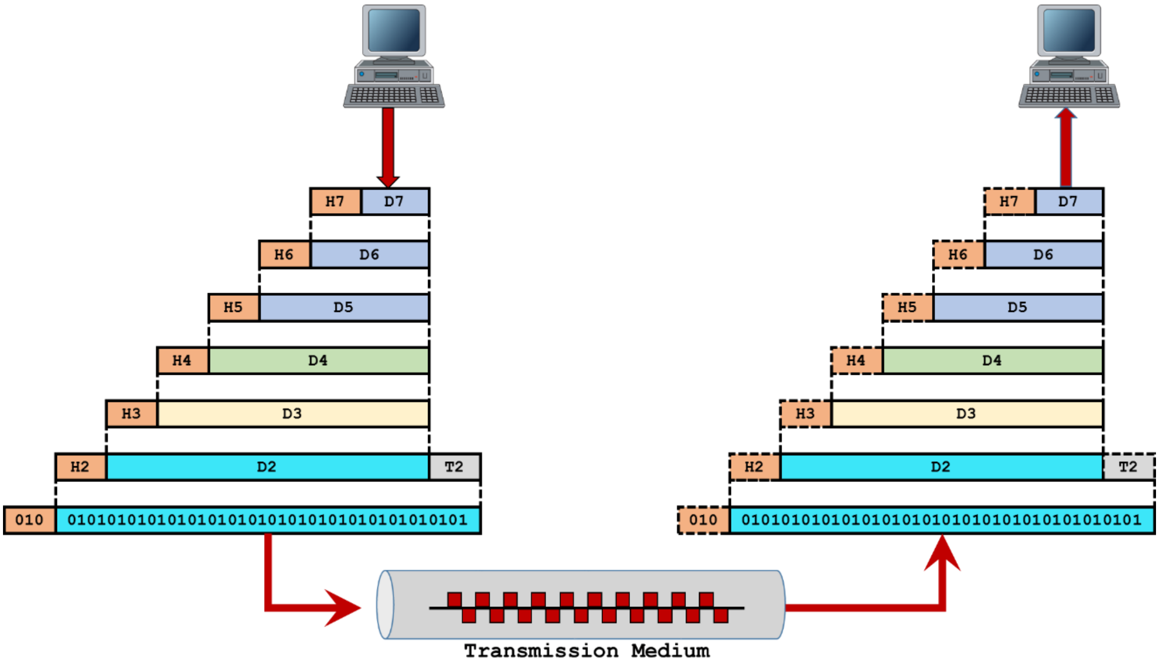


Figure 4.3: An exchange using the OSI model

Figure 4.3 gives an overall view of the OSI layers, D7 means the data unit at layer 7, D6 means the data unit at layer 6, and so on. The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order. At each layer, a header, or possibly a trailer, can be added to the data unit. Commonly, the trailer is added only at layer 2. When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported along a physical link.

Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken.

By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

Section text

Solved Problems

Solved problem

Self-Test (Multiple Choice Questions)

Self-test question

1.20 **Protocols:**Protocols are what describe the rules that control horizontal communication, that is, conversations between processes that run at corresponding layers within the OSI Reference Model. At every layer (except layer one) these communications ultimately take the form of some sort of message that is sent between corresponding software elements on two or more devices. Since these messages are the mechanism for communicating information between protocols, they are most generally called protocol data units (PDUs). Each PDU has a specific format that implements the features and requirements of the protocol.

Protocols at different layers are shown below:

OSI Model	Protocols
Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	TCP, UDP
Network Layer	ICMP, IGMP, IPSec, IPv4, IPv6, IPX, RIP
Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11, Wi-Fi

a. Write short note on protocols.

1.21 **Encapsulation: Figure 4.2** reveals another aspect of data communications in the OSI model: encapsulation. A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on.

In other words, the data portion of a packet at level N - 1 carries the whole packet (data and header and maybe trailer) from level N. The concept is called encapsulation; level N - 1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level N - 1, the whole packet coming from level N is treated as one integral unit.

The outgoing information will travel down through the layers to the lowest layer.

Each layer in the layered architecture provides service to the layers which are directly above and below it. The outgoing information will travel down through the layers to the lowest layer. While moving down on the source machine, it acquires all the control information which is required to reach the destination machine. The control information is in the form ofheaders and footers which surrounds the data received from the layer above. This process of adding headersand footers to the data is called as data encapsulation. The headers and footers contain control information in the individual fields. it is used to make message packet reach the destination. The headers and footers form the envelope which carries the message to the desired destination.

- While moving down on the source machine, it acquires all the control information which is required to reach the destination machine.
- The control information is in the form of Headers and Trailer which surrounds the data received from the layer above.
- This process of adding headers and trailers to the data is called as data encapsulation.
- The information added by each layer is in the form of headers or trailers.
- At layer 1 the entire package is converted to a form that can be transferred to the receiving machine.
- At the receiving machine, the message is unwrapped layer by layer, with eachprocess receiving and removing the data meant for it.
- For example, layer 2 removes the data meant for it, then passes the rest to layer 3.
- Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.
- The headers and trailers contain control information. The headers and trailers formthe envelope which carries the message to the desired destination.
- D7 means the data unit at layer 7, D6 means the data unit at layer 6, and so on.
- The process starts at layer 7 (the application layer), then moves from layer to layerin descending, sequential order.
- At each layer, a header, or possibly a trailer, can be added to the data unit.
- Commonly, the trailer is added only at layer 2.
- When the formatted data unit passes through the physical layer (layer 1), it ischanged into an electromagnetic signal and transported along a physical link.
- The fifth layer of sending machine wants to send a message M to the fifth layer of destination machine.
- The message M is produced by layer 5 of machine 1 and given to layer 4 for transmission. Layer 4 adds header H4 in front of the message and pass it to layer 3.
- Layer 3 breaks up the incoming message into small units as M1 and M2 and pass these packets to layer 2.

- Layer 2 adds the header as well as footer to each packet obtained from layer 3 and pass it to layer 1 for physical transmission.

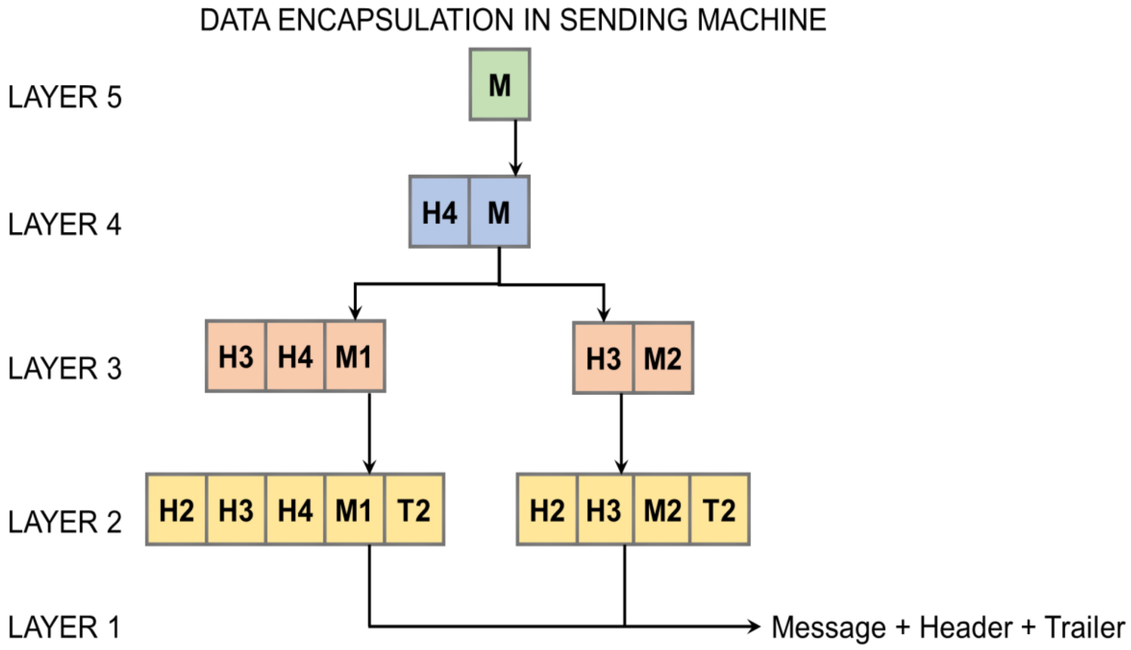


Figure 4.4: Five-layer stack for data encapsulation

a. Explain encapsulation with example.

1.22 Summary
1.23 Exercise (short answer questions)
1.24 References
1.24.1 Books
1.24.2 Wikipedia
1.24.3 MOOCs
1.24.4 YouTube Videos
1.24.5 OER

Unit5: OSI Reference Model

1.25 Learning Objectives: After successful completion of this unit, you will be able to:

- Understand concept of Reference Model.
- Understand OSI Reference Model Concept and be able to apply its terminology toreal networks.
- Understand layers of OSI Reference Model
- Enumerate the layers of the OSI model and TCP/IP.

- Explain the function(s) of eachlayer.

1.26 **Layers of the OSI Reference Model:**OSI Reference Model was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. The OSI model was intended to be the basis for the creation of the protocols in the OSI stack.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separatebut related layers, each of which defines a part of the process of moving information across a network as shown in figure 5.1.

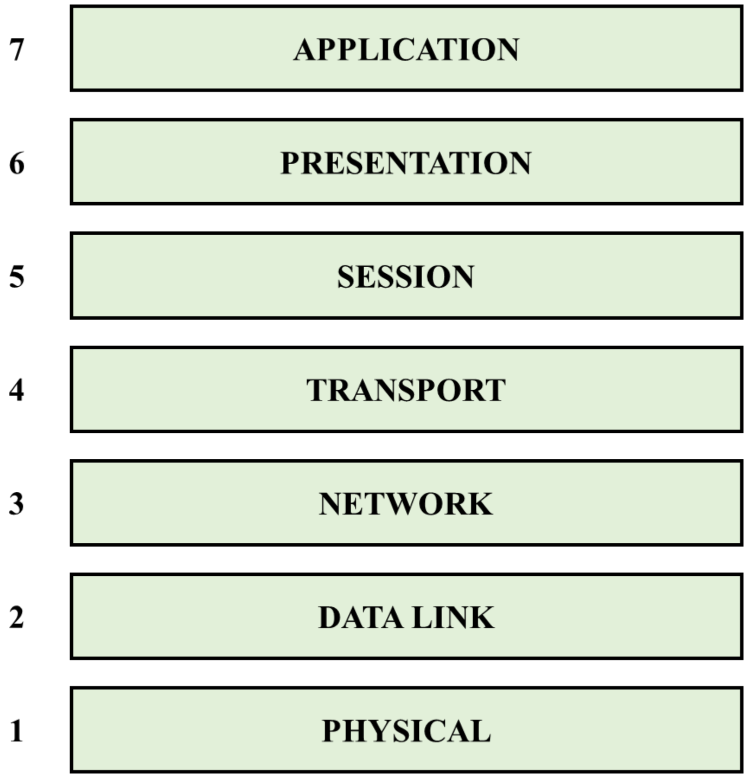


Figure 5.1: Seven layers of the OSI network model

Open System Interconnection (OSI) reference model defines a networking framework to implement protocols in seven layers. OSI reference model doesn’t perform any functions in the networking process. It is a conceptual framework used to understand complex interactions. International Standards Organization (ISO) developed the Open Systems Interconnection (OSI) model. It divides network communication into seven layers. Layers 1-4 are considered the lower layers, and mostly concern themselves with moving data around. Layers 5-7, the upper layers, contain application-level data. Networks operate on one basic principle: “pass it on”. Each layer takes care of a very specific job, and then passes the data onto the next layer. In the OSI model, control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. The OSI model takes the task of inter-networking and divides that up into what is referred to as a vertical stack that consists of the 7layers as shown in figure 5.1.

5.26.1 **Physical Layer:**Provides electrical, functional, and procedural characteristics to activate, maintain, and deactivate physical links that transparently send the bit stream. It only recognizes individual bits, not characters or multi-character frames.

The Physical Layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur. Figure 5.2 shows the position of thephysical layer with respect to the transmission medium and the data link layer.

The physical layer is also concerned with the following:

Physical characteristics of interfaces and medium: The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

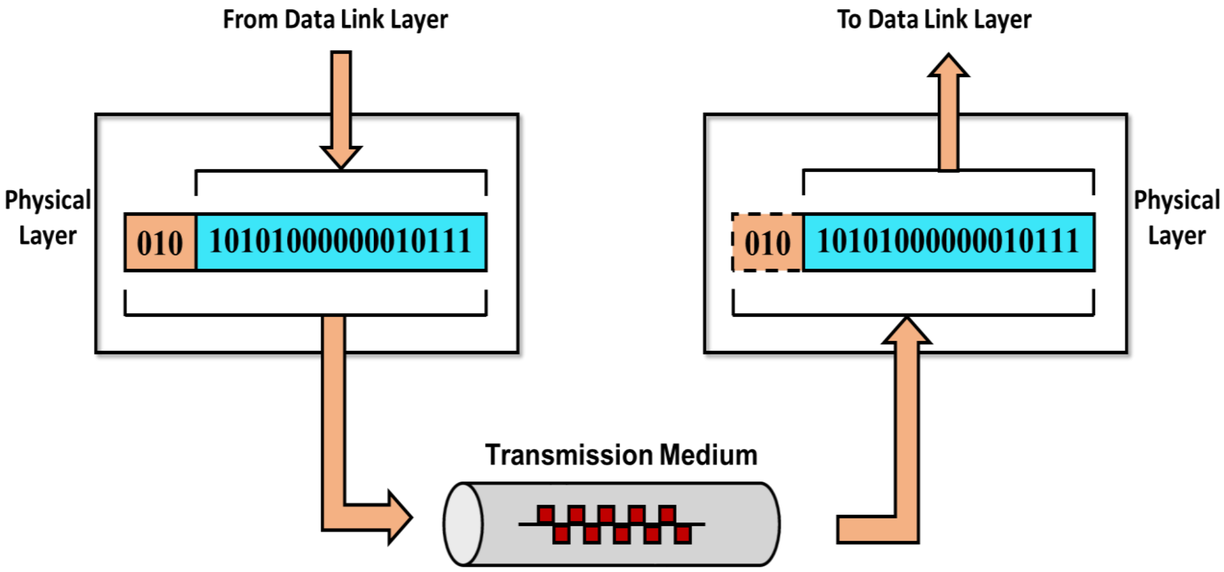


Figure 5.2:Physical Layer

Physical Layer is the lowest layer of the OSI model. It is related with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It Provides

- **Representation of bits** (**Data Encoding)**: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
  - What signal state represents a binary 1
  - How the receiving station knows when a "bit-time" starts
  - How the receiving station delimits a frame

  The physical layer data consists of a stream of bits (sequence of 0sor 1s) with no interpretation. To be transmitted, bits must be encoded into signals, either electricalor optical. The physical layer defines the type of encoding (how 0s and 1s are changed tosignals).
- **Data rate:** The transmission rate-the number of bits sent each second-is also defined by thephysical layer. In other words, the physical layer defines the duration of a bit, which is howlong it lasts.
- **Synchronization of bits:** The sender and receiver not only must use the same bit rate butalso must be synchronized at the bit level. In other words, the sender and the receiver clocksmust be synchronized.
- **Line configuration:** The physical layer is concerned with the connection of devices to themedia. In a point-to-point configuration, two devices are connected through a dedicated link.In a multipoint configuration, a link is shared among several devices.
- **Physical topology:** The physical topology defines how devices are connected to make anetwork. Devices can be connected by using a mesh topology, a star, a ring topology, a bustopology, or a hybrid topology.
- **Transmission Technique /Mode:**determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signalling.The physical layer also defines the direction of transmission betweentwo devices: simplex, half-duplex, or full-duplex.
- **Physical medium attachment, accommodating various possibilities in the medium:**
  - Will an external transceiver (MAU) be used to connect to the medium?
  - How many pins do the connectors have and what is each pin used for?
- **Physical Medium Transmission:** transmits bits as electrical or optical signals appropriate for the physical medium, and determines:
  - What physical medium options can be used
  - How many volts/db. should be used to represent a given signal state, using a given physical medium

5.26.2 **Data Link Layer:**Provides functional and procedural means to transfer data between network entities and (possibly) correct transmission errors; provides for activation, maintenance, and deactivation of data link connections, grouping of bits into characters and message frames, character and frame synchronisation, error control, media access control, and flow control.

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). Figure 5.3 shows the relationship of the data link layer to the network and physical layers.

Data Link Layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.

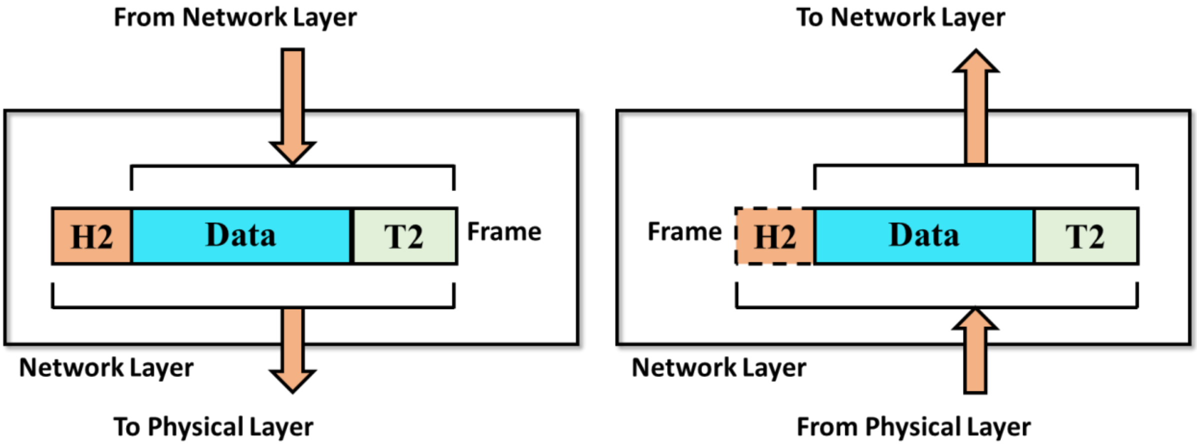


Figure 5.2: Data link Layer

Other responsibilities of the data link layer include the following:

- **Link Establishment and Termination:** establishes and terminates the logical link between two nodes.
- **Framing:**transmits/receives frames sequentially.The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Frame Acknowledgment:** provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- **Frame Delimiting:** creates and recognizes frame boundaries.
- **Physical Addressing:**If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the

sender's network, the receiver address is the address of the device that connects the network to the next one.

- **Flow Control:**If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.Frame traffic control tells the transmitting node to "back-off" when no frame buffers are available.
- **Error Control:**Frame error checking checks received frames for integrity.The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
- **Access Control:**When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.Media access management determines when the node "has the right" to use the physical medium.

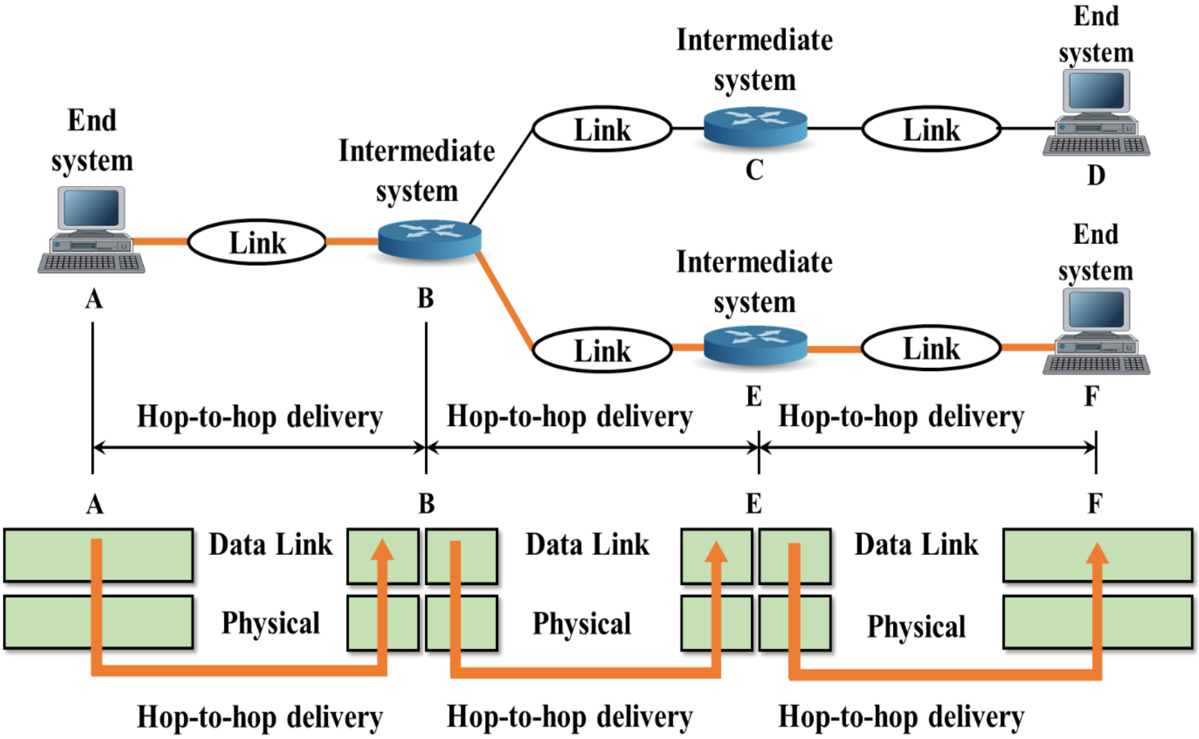


Figure 5.3Hop-to-hop delivery

Figure 5.3 illustrates hop-to-hop (node-to-node) delivery by the data link layer. As shown in the figure, communication at the data link layer occurs between two adjacent nodes. To send datafrom A to F, partially three deliveries are made. First, the data link layer at A sends a frame to thedata link layer at B (a router). Second, the data link layer at B sends a new frame to the data linklayer at E. Finally, the data link layer at E sends a new frame to the data link layer at F. The frames that are exchanged between the three nodes have different values in the headers. Theframe from A to B has B as the destination address and A as the source address.The frame fromB to E has E as the destination address and B as the source address. The frame from E to F has Fas the destination address and E as the source address. The values of the trailers can also bedifferent if error checking includes the header of the frame.

5.26.3 **Network Layer:**The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layerensures that each packet gets from its point of origin to its final destination.

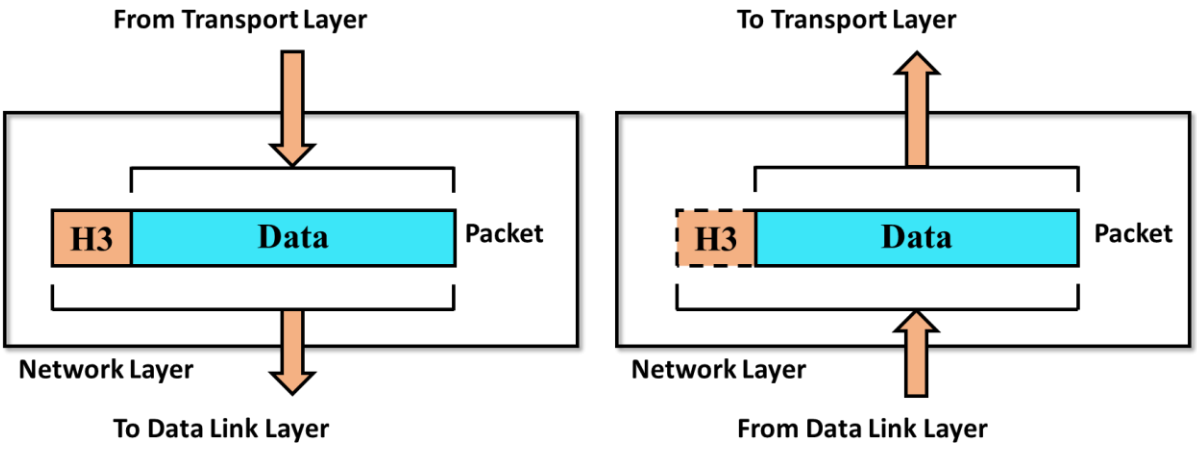


Figure 5.4: Network Layer

If two systems are connected to the same link, there is usually no need for a network layer.However, if the two systems are attached to different networks (links) with connecting devicesbetween the networks (links), there is often a need for the network layer to accomplish source-todestinationdelivery. Figure 5.4 shows the relationship of the network layer to the data link andtransport layers.

Other responsibilities of the network layer include the following:

- **Logical Addressing:** The physical addressing implemented by the data link layer handles theaddressing problem locally. If a packet passes the network boundary, we need anotheraddressing system to help distinguish the source and destination systems. The network layeradds a header to the packet coming from the upper layer that, among other things, includesthe logical addresses of the sender and receiver. We discuss logical addresses later in thischapter.

- **Routing:** When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.One of the functions of the network layer is to provide this mechanism.

Figure 5.5shows end-to-end delivery by the network layer. The figure shows, a source-to-destination delivery. The network layer at A sends the packet to the networklayer at B. When the packet arrives at router B, the router makes a decision based on the finaldestination (F) of the packet. Router B uses its routing table to find that the next hop is router E.The network layer at B, therefore, sends the packet to the network layer at E. The network layerat E, in turn, sends the packet to the network layer at F.

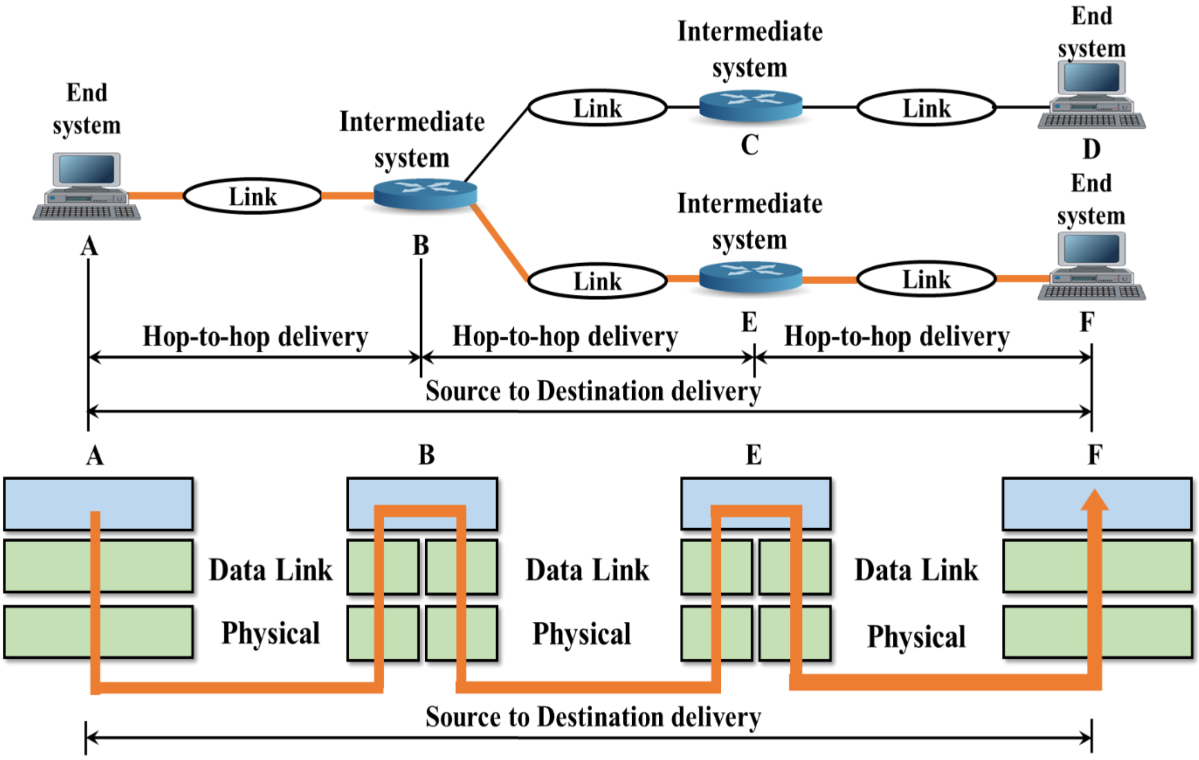


Figure 5.5:Source to Destination delivery

5.26.4 **Transport Layer:** The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. Figure 5.6 shows the relationship of the transportlayer to the network and session layers.

Other responsibilities of the transport layer include the following:

- **Service-point addressing:** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

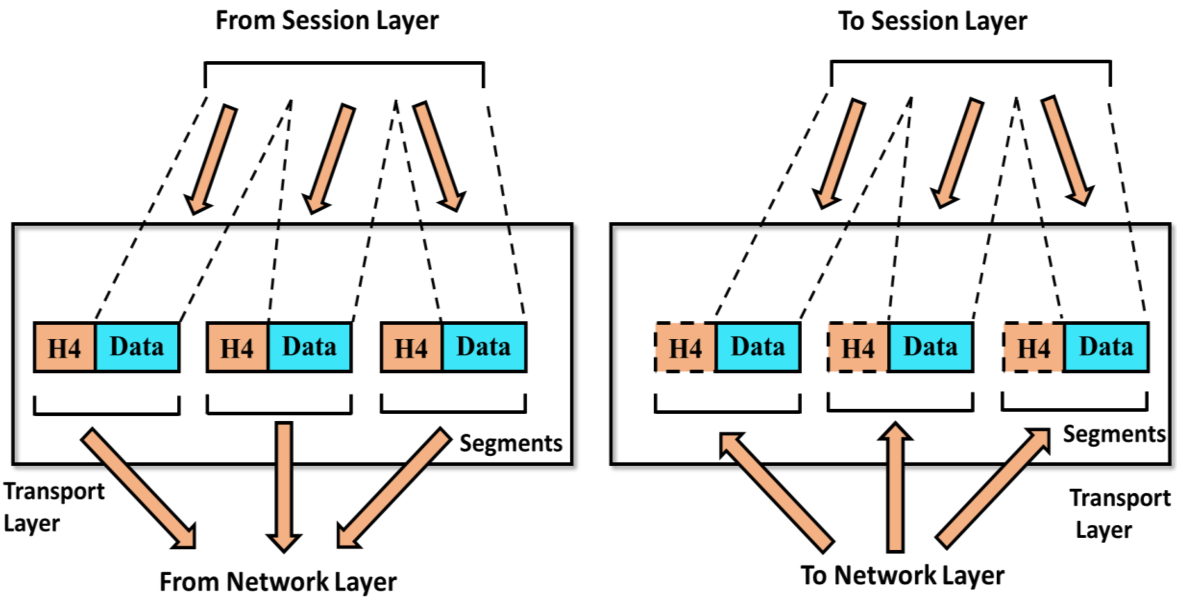


Figure 5.6: Transport Layer

- **Segmentation and reassembly:** A message is divided into transmittable segments, with eachsegment containing a sequence number. These numbers enable the transport layer to reassemblethe message correctly upon arriving at the destination and to identify and replace packets thatwere lost in transmission.
- **Connection control:** The transport layer can be either connectionless or connection oriented.A connectionless transport layer treats each segment as an independent packet and delivers it tothe transport layer at the destination machine. A connection oriented transport layer makes aconnection with the transport layer at the destination machine first before delivering the packets.After all the data are transferred, the connection is terminated.

- **Flow control:** Like the data link layer, the transport layer is responsible for flow control.However, flow control at this layer is performed end to end rather than across a single link.
- **Error control:** Like the data link layer, the transport layer is responsible for error control.However, error control at this layer is performed process-to-process rather than across a singlelink. The sending transport layer makes sure that the entire message arrives at the receivingtransport layer without error (damage, loss, or duplication). Error correction is usually achievedthrough retransmission.

5.26.5 **Session Layer:**The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

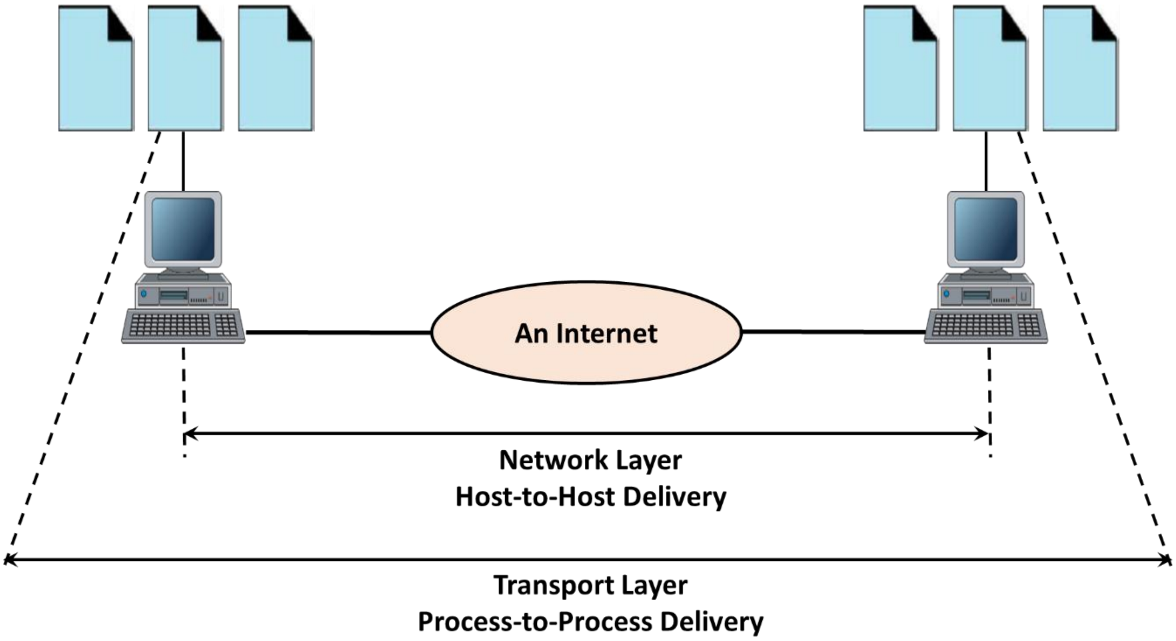


Figure 5.7: Reliable process-to-process delivery of a message

Specific responsibilities of the session layer include the following:

- **Dialog control:** The session layer allows two systems to enter into a dialog. It allows thecommunication between two processes to take place in either half duplex or full-duplex mode.
- **Synchronization:** The session layer allows a process to add checkpoints, or synchronizationpoints, to a stream of data. For example, if a system is sending a file of 2000 pages, it isadvisable to insert checkpoints after every 100 pages to ensure that each 100-page unit isreceived and acknowledged independently. In this case, if a crash happens during thetransmission of page 523, the only pages that need to be resent after system recovery are pages501 to 523. Pages

previous to 501 need not be resent. Figure 5.8 illustrates the relationship ofthe session layer to the transport and presentation layers.

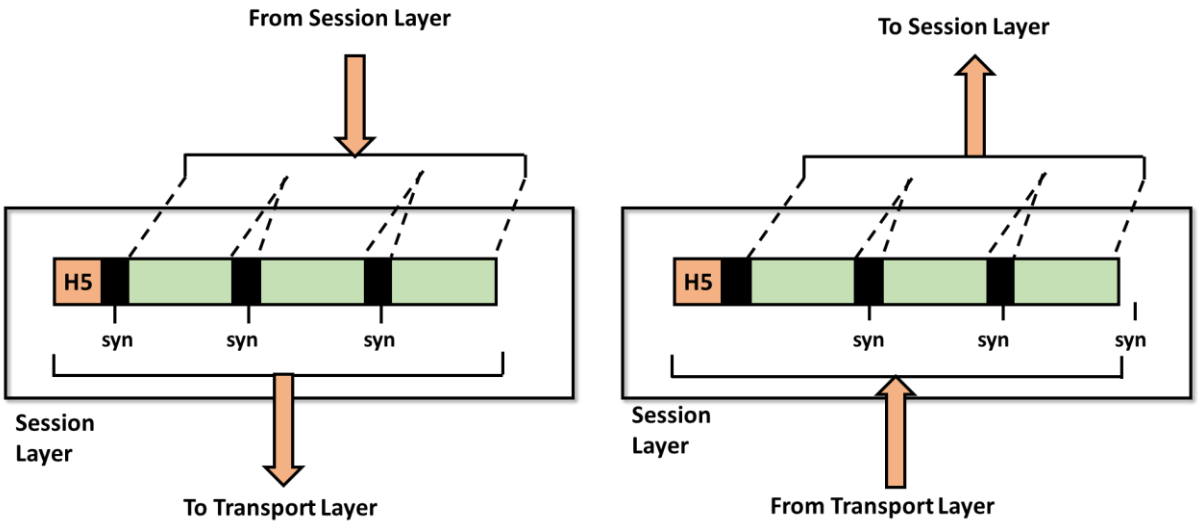


Figure 5.8: Session Layer

5.26.6 **Presentation Layer:** The presentation layer is concerned with the syntax and semantics of theinformation exchanged between two systems. Figure 5.9 shows the relationship between thepresentation layer and the application and session layers.

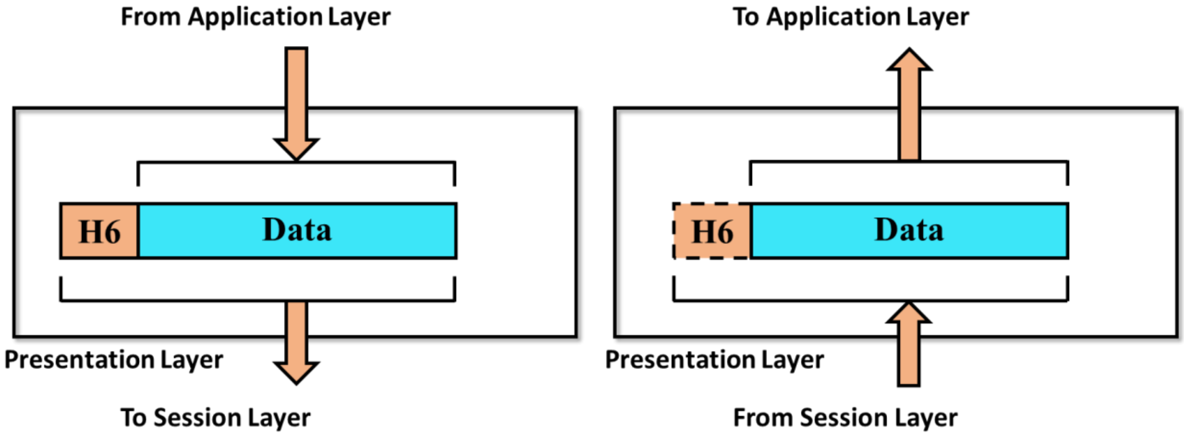


Figure 5.9 Presentation Layer

Specific responsibilities of the presentation layer include the following:

- **Translation:** The processes (running programs) in two systems are usually exchanginginformation in the form of character strings, numbers, and so on. The information must bechanged to bit streams before being transmitted. Because different computers use differentencoding systems, the presentation layer is responsible for interoperability between thesedifferent encoding methods. The presentation layer at the sender changes the information fromits sender-dependent format into a common format. The presentation layer at the receivingmachine changes the common format into its receiver-dependent format.

- **Encryption:** To carry sensitive information, a system must be able to ensure privacy. Encryptionmeans that the sender transforms the original information to another form and sends the resultingmessage out over the network. Decryption reverses the original process to transform the messageback to its original form.
- **Compression:** Data compression reduces the number of bits contained in the information. Datacompression becomes particularly important in the transmission of multimedia such as text,audio, and video.

5.26.7 **Application Layer:**The application layer enables the user, whether human or software, toaccess the network. It provides user interfaces and support for services such as electronic mail,remote file access and transfer, shared database management, and other types of distributedinformation services.

Figure 5.10 shows the relationship of the application layer to the user and the presentation layer.

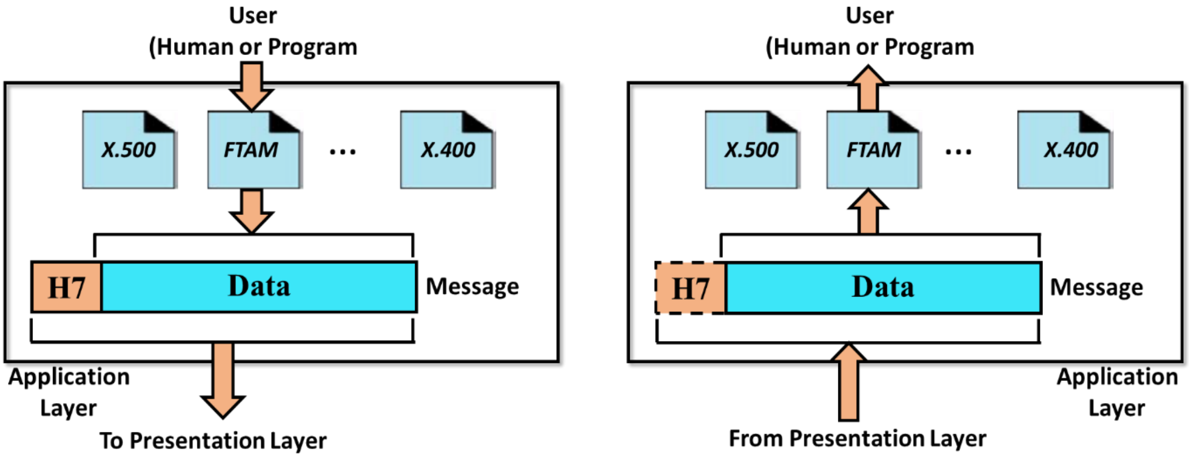


Figure 5.10: Application Layer

Of the many application services available, the figure shows only three:

- XAOO (messagehandlingservices),
- X.500 (directory services), and
- File Transfer, Access, and Management(FTAM).

The user in this example employs XAOO to send an e-mail message.

Specific services provided by the application layer include the following:

- **Network virtual terminal:** A network virtual terminal is a software version of a physicalterminal, and it allows a user to log on to a remote host. To do so, the application creates asoftware emulation of a terminal at the remote host. The user's computer talks to the softwareterminal which, in turn, talks to the host, and vice versa. The remote host believes it iscommunicating with one of its own terminals and allows the user to log on.

- **File transfer, access, and management:** This application allows a user to access files in aremote host (to make changes or read data), to retrieve files from a remote computer for use inthe local computer, and to manage or control files in a remote computer locally.
- **Mail services:** This application provides the basis for e-mail forwarding and storage.
- **Directory services:** This application provides distributed database sources and access for globalinformation about various objects and services.

1.27 Summaryof Layers:

- Application: Allows access to network resources
- Presentation: Translates, Encrypts and Compresses data
- Session: Establishes, Manages and Terminates the sessions.
- Transport:Provides reliable process – to – process message delivery and error recovery
- Network: Moves packets from source to destination and provides internetworking
- Data Link: Organizes bits into frames and provides hop – to – hop delivery
- Physical: Transmits bits over a medium and provides electrical and mechanical specifications

OSI Reference Model Layer Summary

Group	#	Layer Name	Key Responsibilities	Data Type Handled	Scope	Common Protocols and Technologies
Lower Layers	1	Physical	Encoding and Signaling; Physical Data Transmission; Hardware Specifications; Topology and Design	Bits	Electrical or light signals sent between local devices	(Physical layers of most of the technologies listed for the data link layer)
	2	Data Link	Logical Link Control; Media Access Control; Data Framing; Addressing; Error Detection and Handling; Defining Requirements of Physical Layer	Frames	Low-level data messages between local devices	IEEE 802.2 LLC, Ethernet Family; Token Ring; FDDI and CDDI; IEEE 802.11 (WLAN, Wi-Fi); HomePNA; HomeRF; ATM; SLIP and PPP
	3	Network	Logical Addressing; Routing; Datagram Encapsulation; Fragmentation and	Datagrams / Packets	Messages between local or remote devices	IP; IPv6; IP NAT; IPsec; Mobile IP; ICMP; IPX; DLC; PLP;

			Reassembly; Error Handling and Diagnostics			Routing protocols such as RIP and BGP
	4	Transport	Process-Level Addressing; Multiplexing/Demultiplexing; Connections; Segmentation and Reassembly; Acknowledgments and Retransmissions; Flow Control	Datagrams / Segments	Communication between software processes	TCP and UDP; SPX; NetBEUI/NBF
Upper Layers	5	Session	Session Establishment, Management and Termination	Sessions	Sessions between local or remote devices	NetBIOS, Sockets, Named Pipes, RPC
	6	Presentation	Data Translation; Compression and Encryption	Encoded User Data	Application data representations	SSL; Shells and Redirectors; MIME
	7	Application	User Application Services	User Data	Application data	DNS; NFS; BOOTP; DHCP; SNMP; RMON; FTP; TFTP; SMTP; POP3; IMAP; NNTP; HTTP; Telnet

1.28

1.29 Exercise (short answer questions)

1.30 References

- 1.30.1 Books
- 1.30.2 Wikipedia
- 1.30.3 MOOCs
- 1.30.4 YouTube Videos
- 1.30.5 OER

Unit6: TCP/IP SUITE

1.1 Learning Objectives

After successful completion of this unit, you will be able to:

- Understand and implement addressing mechanism in the internet.
- Understand the concept of TCP/ IP Model
- Understand functioning of different Layers of TCP / IP suite

1.2 The TCP/IP Suite

TCP/IP means Transmission Control Protocol and Internet Protocol. Current internet architecture uses TCP/IP network model. Protocols are set of rules used tocontrolall theprobable communication onthe network. The movement of data between the source and destination over the internet is described by these protocols. These protocols provide simple naming and addressing schemes.

TCP/IP reference model was developed to:

- Support a flexible architecture byeasily adding more computersin a network.
- To keep network robust.
- To keep connections intact until the source and destination machines are functioning.

1.3 Addressing mechanism in the Internet

Introduction: Over a half million networks are connected to the Internet. An Internet Protocol address (IP address) is a numerical tagallocated to each device (e.g., computer, printer) connected in a computer network andthat uses Internet Protocol for communication. IP address provides two mainfunctions: host/ network interface identification and location addressing. It functions as follows:

1. **Name:** it indicates what we seek.
2. **Address:**tells where it is.
3. **Route:**shows how to get there.

IP address is an address used to identify a device uniquely over an internet. IP address is made-up of 32 binary bits, it is divided into two parts

a. Networkportion
b. Host portion

, with the help of a subnet mask.

These 32 bits are broken into four octets (1 octet = 8 bits). Each octet isconverted to decimal and separated by a period (dot). Hence IP address is expressed in dotted decimal format (for example, 192.178.10.20).The range of value in each octet is from 0 to 255 decimal, or 00000000 – 11111111binary. To avoid duplication**I**nternet **A**ssigned **N**umbers **A**uthority (**IANA**) manages the IP address space allocations globally and delegate’s five regional Internet registries (RIRs) to allocate IP address blocks to localInternet service providers and other individuals.

Solved Problems

Solved problem

Self Test (Multiple Choice Questions)

Self test question

1.4 IP Addressing - IPv4

A network IP address is divided into Netid and Hostid, also known as Prefix and Suffix.IP addresses are unique addresses. Each address defines one, and only one,connection to the Internet. No device at a same time over the internet can have same IP address.

Address Space:

IPv4 uses 32-bit addresses, which means that the address space is 232 or4,294,967,296 (more than 4 billion), i.e. if there were no restrictions, more than 4 billiondevices can be connected to the Internet.

Notations:

There are two prevalent notations to show an IPv4 address: Binary notation and Dotteddecimal notation.

1.4.1 Binary Notation:

- In binary notation, the IPv4 address is displayed as 32 bits.
- Each octet is often referred to as a byte.
- So it is common to hear an IPv4 address referred to as a 32-bit address or a4-byte address.
- The following is an example of an IPv4 address in binary notation:
- **1100000010110010 0000101000010100**

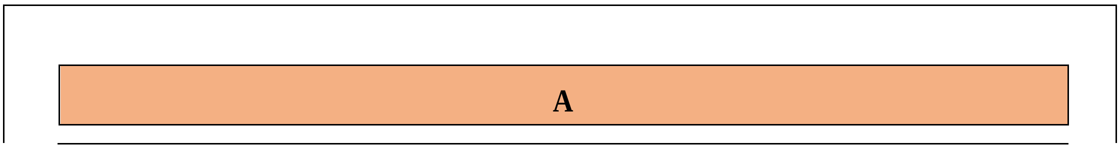
1.4.2 Dotted-Decimal Notation:

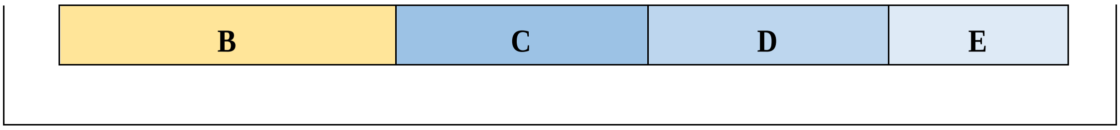
- To make the IPv4 address more compact and easier to read, Internetaddresses are usually written in decimal form with a decimal point (dot)separating the bytes.
- Each byte is identified by a decimal number in the range [0 – 255].
- The following is the dotted decimal notation of the above address:**192.178.10.20**
- **Explained:**

11000000	**10110010**	**00001010**	**00010100**
1st Byte	**2nd Byte**	**3rd Byte**	**4th Byte**
= 192	**= 178**	**= 10**	**= 20**

IP Address classes:

In IPv4 addressingconcept of classes is used, also known as classful addressing. In this the address space is divided into five classes: **A**, **B**, **C**, **D**, and **E**. Each class occupies some part of the address space.





Finding the class in binary notation:

	1st Byte	2nd Byte	3rd Byte	4th Byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

Fig: Finding the class in binary notation.

If the address is given in decimal-dotted notation, the first byte defines theclass.

	1st Byte	2nd Byte	3rd Byte	4th Byte
Class A	0 – 127			
Class B	128 – 191			
Class C	192 – 223			
Class D	224 – 239			
Class E	240 – 255			

Fig: Finding the class in decimal notation

Finding the address class:

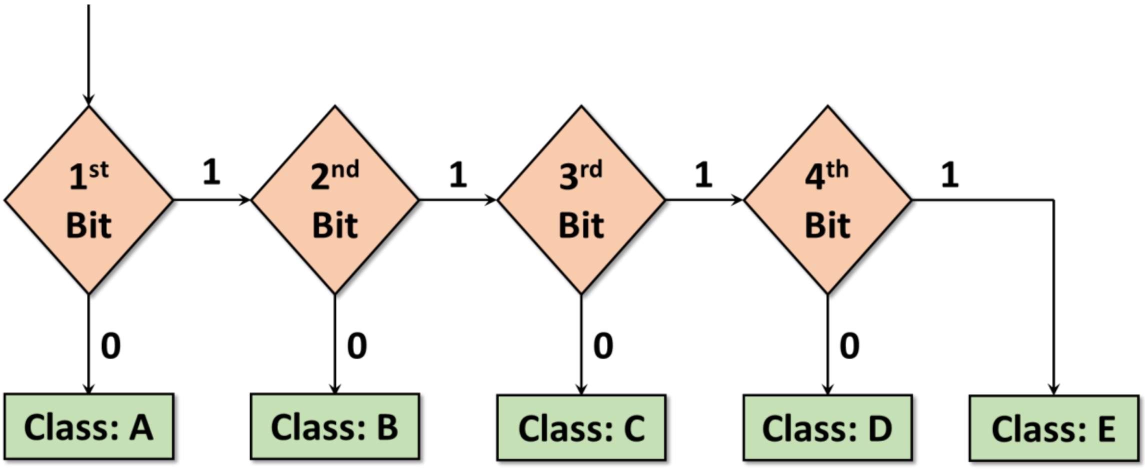


Fig: Finding Address Class

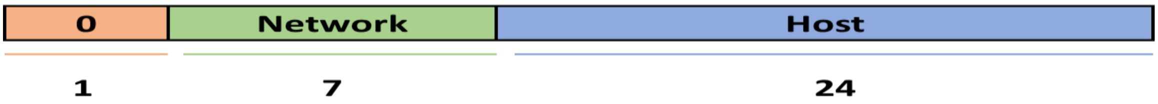
Classes and Blocks:

Class	Subnet Mask Decimal	No. of Hosts per Network	No of Networks	Start – End Address
A	255.0.0.0	16 Million	127	1.0.0.0 – 126.255.255.255
B	255.255.0.0	6500	1600	128.0.0.0 – 191.255.255.255
C	255.255.255.0	254	2 Million	192.0.0.0 – 223.255.255.255
D	Reserved for multicast groups			224.0.0.0 – 239.255.255.255
E	Reserved for future use, or Research and Development Purposes			240.0.0.0 – 254.255.255.255

Fig: Number of blocks and block size in classful IPv4 addressing.

Class A:

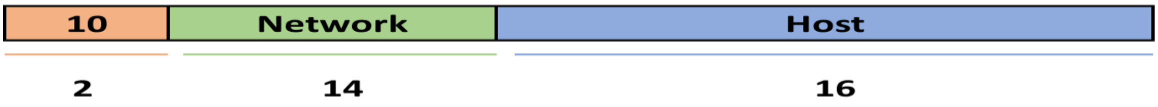
- The high-order (First) bit in a class – Aaddress is always set to zero.
- The next seven bits complete the network ID.
- The remaining 24 bits represent the host ID.
- This allows for 128 networks and 16,777,214 hosts per network.
- In this 7 bits are used for network field and 24 bits for host field.
- Class A IP address range includes 1.0.0.0 to 127.255.255.255



Note: Millions of class A addresses are wasted.

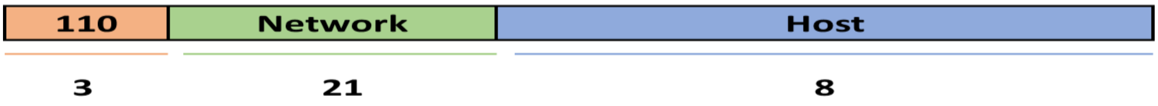
Class B:

- Class B addresses are assigned to medium-sized to large-sized networks.
- The two high-order bits in a class B address are always set to binary 1 0.
- The next 14 bits complete the network ID.
- The remaining 16 bits represent the host ID.
- This allows for 16,384 networks and 65,534 hosts per network.
- Class B IP address range includes 128.0.0.0 to 191.255.255.255



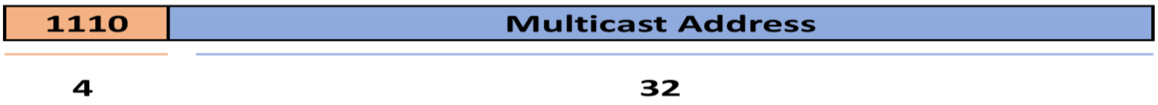
Class C:

- Class C addresses are used for small organizations with a small number of attached hosts or routers.
- The three high-order bits in a class C address are always set to binary 1 1 0.
- The next 21 bits complete the network ID.
- The remaining 8 bits (last octet) represent the host ID.
- This allows for 2097152 networks and 256 hosts per network.
- Class C IP address range includes 192.0.0.0 to 223.255.255.255.



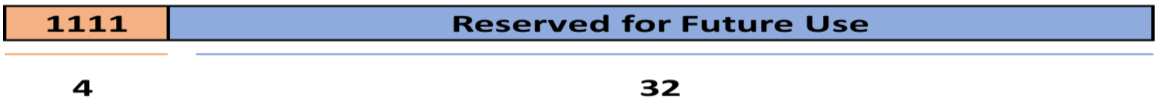
Class D:

- Class D addresses are reserved for IP multicast addresses.
- The four high-order bits in a class D address are always set to binary 1 1 1 0.
- The remaining bits recognize hosts.
- Class D IP address range includes 224.0.0.0 to 239.255.255.255



Class E:

- Class E is an experimental address that is reserved for future use.
- The high-order bits in a class E address are set to binary 1111.
- Class E IP address range includes 240.0.0.0 to 255.255.255.255



Netid and Hostid

- In classful addressing, an IP address in class A, B, or C is divided into Netid and Hostid.
- These parts are of varying lengths, depending on the class of the address.

Network Prefix
Host Number

Note that the concept does not apply to classes D and E.

- In class A, one byte defines the Netid and three bytes define the Hostid.
- In class B, two bytes define the Netid and two bytes define the Hostid.
- In class C, three bytes define the Netid and one byte defines the Hostid.

Mask

- Although the length of the Netid and Hostid (in bits) is predetermined in classful addressing, we can also use a mask (also called the default mask/natural masks), a 32-bit number made of contiguous 1’s followed by contiguous 0’s.
- The masks for classes A, B, and C are shown in Table.
- The concept does not apply to classes D and E.

Class	Subnet Mask Binary	Subnet Mask Decimal
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

- The mask can help us to find the Netidand the Hostid.
- For example, the mask for a class-A address has eight 1s, which means the first 8 bits of any address in class A define the Netid; the next 24 bits define the Hostid.

Subnetting

- If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors.
- Subnetting increases the number of 1’s in the mask.
- To create multiple logical networks that exist within a single Class A, B, or C network.
- If subnet masking is not done, only one network from Class A, B, or C network can be used, which is unrealistic.
- The subnet mask follows two rules:
  - If a binary bit is set to a 1 (or on) in a subnet mask, the corresponding bit in the address identifies the network.

- If a binary bit is set to a 0 (or off) in a subnet mask, the corresponding bit in the address identifies the host.

Supernetting

- The most of the class A and class B addresses were exhausted; however, there was still a huge demand for midsize blocks.
- The size of a class C block with a maximum number of 256 addresses did not satisfy the needs of most organizations.
- One solution was supernetting.
- In supernetting, an organization can combine several class C blocks to create a larger range of addresses.
- In other words, several networks are combined to create a supernetwork or a supernet.
- An organization can apply for a set of class C blocks instead of just one.
- For example, an organization that needs 1000 addresses can be granted four contiguous class C blocks.
- The organization can then use these addresses to create one supernetwork.
- Supernetting decreases the number of 1's in the mask.
- For example,
  - If an organization is given four class C addresses, the mask changes from 24 to 22.

Address Depletion

- The flaws in classful addressing scheme combined with the fast growth of the Internet lead to the near depletion of the available addresses.
- Yet the number of devices on the Internet is much less than the 232 address space.
- We have run out of class A and B addresses, and a class C block is too small for most midsize organizations.
- One solution that has alleviated the problem is the idea of classless addressing.

Classless Addressing

- To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented.
- In this scheme, there are no classes, but the addresses are still granted in blocks.

Address Blocks

- In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses.

- The size of the block (the number of addresses) varies based on the nature and size of the entity.
- For example, a household may be given only two addresses; a large organization may be given thousands of addresses.
- An ISP, as the Internet service provider, may be given thousands of addresses based on the number of customers it may serve.

Restriction: To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1. The addresses in a block must be contiguous, one after another.
2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8 ...).
3. The first address must be evenly divisible by the number of addresses.

Solved Problems:

1. **Example: Change the following IPv4 addresses from binary notation to dotted decimal notation.**

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution:

We replace each group of 8 bits with its equivalent decimal number and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

2. **Find the class of the address in binary notation:**

Ex:
a.00000001000010110000101111101111

Solution: The first bit is 0. This is a class: **A** address.
b. 11000001100000110001101111111111

Solution: The first 2 bits are 1; the third bit is 0.This is a class:**C** address.

3. **Find the class of the address in decimal notation:**

Ex:
a. 229.10.24.57

Solution: The first byte is 227 (between 224 and 239), the class is **D**.

b. 221.10.24.57

Solution: The first byte is 193 (between 192 and 223), the class is **C**.

4. **Finding the Subnet Address: Use binary notation for both the address and the mask and then apply the AND operation to find the subnet address.**

Example:

What is the subnetwork address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0?

Solution:

Step 1: Convert given IP and Subnet mask to Binary

Step 2: Perform AND Operation on these two.

11001000 00101101 00100010 00111000 **Binary 200.45.34.56**

11111111 11111111 1111000000000000 **Subnet Mask 255.255.255.0**

11001000 00101101 0010**0000 00000000**

The subnetwork address is **200.45.32.0**.

Step 3: Convert the result of AND operation to Dotted Decimal format which is Subnet mask.

Example 2:

A company is granted the site address 201.70.64.0 (class C). The company needs six subnets. Design the subnets.

Solution:

- The number of 1s in the default mask is 24 (class C).
- The company needs six subnets.
- This number 6 is not a power of 2.
- The next number that is a power of 2 is 8 (23).
- We need 3 more 1’s in the subnet mask.
- The total number of 1’s in the subnet mask is 27 (24 + 3).
- The total number of 0’s is 5 (32 - 27).
- The mask is

11111111 11111111 11111111 11100000

Or

255.255.255.224

- The number of subnets is 8.
- The number of addresses in each subnet is 25 (5 is the number of 0s) or 32.
- Subnet 1: The bit combination is 001.

  Taking last octet in binary: 0 0 1 0 0 0 0 0 = 32 (10)

  Hence the subnet address is, 201.70.64. 32
- Subnet 2: The bit combination is 01 0.

  Taking last octet in binary: 0 0 1 0 0 0 0 0 = 64(10)

Hence the subnet address is, 201.70.64. 64

- Subnet 3: The bit combination is 011.

  Taking last octet in binary: 0 1 1 0 0 0 0 0 = 96(10)

  Hence the subnet address is, 201.70.64. 96
- Subnet 4: The bit combination is 100.

  Taking last octet in binary: 1 0 0 0 0 0 0 0 = 128(10)

  Hence the subnet address is, 201.70.64. 128
- Subnet 5: The bit combination is 101.

  Taking last octet in binary: 1 0 1 0 0 0 0 0 = 160(10)

  Hence the subnet address is, 201.70.64. 160
- Subnet 6: The bit combination is 110.

  Taking last octet in binary: 1 1 0 0 0 0 0 0 = 192 (10)

  Hence the subnet address is, 201.70.64. 192

Example 3:

A company is granted the site address 181.56.0.0 (class B). The company needs 1000 subnets. Design the subnets.

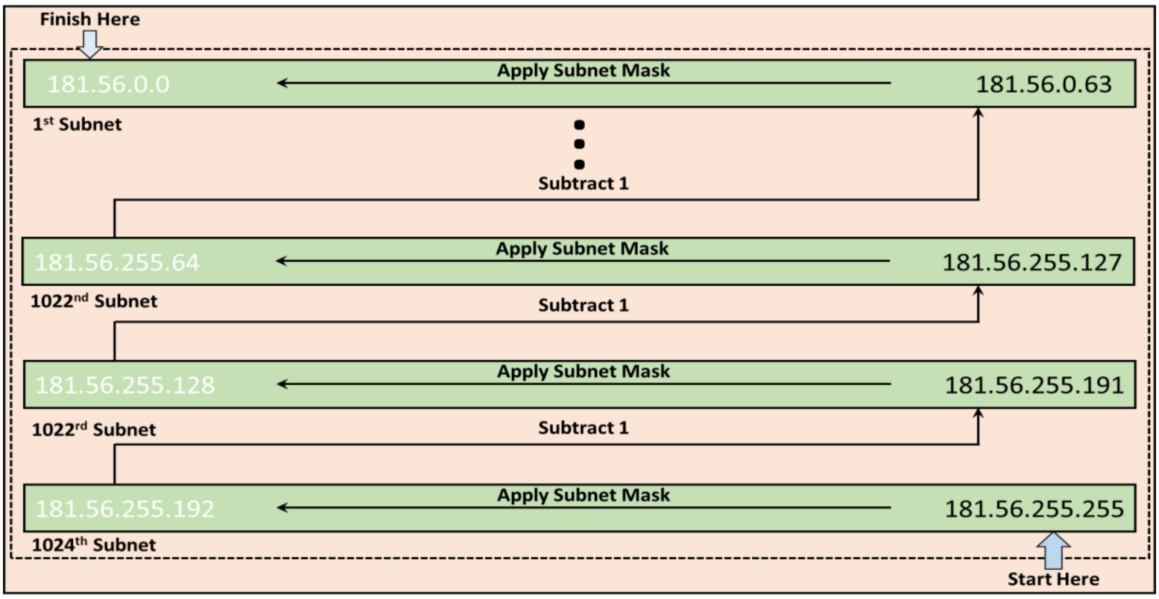
Solution:

- The number of 1s in the default mask is 16 (class B).
- The company needs 1000 subnets.
- This number is not a power of 2.
- The next number that is a power of 2 is 1024 (210).
- We need 10 more 1's in the subnet mask.
- The total number of 1's in the subnet mask is 26 (16 + 10).
- The total number of 0's is 6 (32 - 26).
- The mask is

  11111111 11111111 11111111 11000000

  or

  255.255.255.192
- The number of subnets is 1024.
- The number of addresses in each subnet is 26 (6 is the number of 0s) or 64.



5. Supernetting Example:

We need to make a supernetwork out of 16 class C blocks. What is the supernet mask?

Solution:

- We need 16 blocks.
- For 16 blocks we need to change four 1s to 0s in the default mask. So the mask is

11111111 11111111 11110000 00000000

Or

255.255.240.0

6. Example:

A company needs 600 addresses. Which of the following set of class C blocks can be used to form a supernet for this company?

1. 198.47.32.0 198.47.33.0 198.47.34.0
2. 198.47.32.0 198.47.42.0 198.47.52.0 198.47.62.0
3. 198.47.31.0 198.47.32.0 198.47.33.0 198.47.52.0
4. 198.47.32.0 198.47.33.0 198.47.34.0 198.47.35.0

Solution:

- 1: No, there are only three blocks.
- 2: No, the blocks are not contiguous.
- 3: No, 31 in the first block is not divisible by 4.
- 4: Yes, all three requirements are fulfilled.

Self-Test (Multiple Choice Questions)

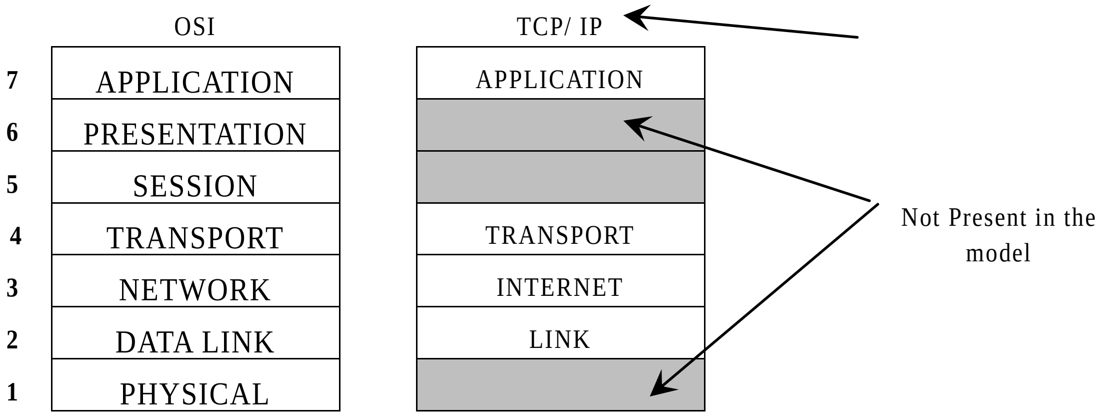
2 Self test question

3 Self-test question

6.5 Layered Structure of the TCP / IP Model

Transport, Application Layer:

- The TCP/IP protocol suite was developed before the OSI model.
- So layers in TCP/IP protocol suite do not exactly match with layers in the OSI model.
- Original TCP/IP protocol suite was designed as having four layers:
  - **Host-To-Network**
  - **Internet**
  - **Transport**
  - **Application**



- When TCP/IP is compared with OSI,
- Host-To-Network layer is equivalent to Physical and Data Link layers.
- Internet layer is equivalent to Network layer, and Application layer performing the work of the Session, Presentation, and Application layers.

Network Access Layer

- Also known as Host-to-Network Layer.
- Performs all functions of physical Layer and Data Link Layer.
- Exchange of data between end system and network.
- Address of host and destination
- Prioritization of transmission.
- This deals with hardware level, connections as in other network model.
- TCP/IP Protocol Suite includes Host-to-Network Layer protocols such as-
- Serial Line Internet Protocol (SLIP) and Point to Point Protocol (PPP).

TCP/IP Internet Layer

- An Internet is an interconnection of two or more networks.
- Internet layer handles tasks similar to network access layer, but between networks rather than between nodes on a network.
- Uses IP for addressing and routing across networks.
- Implemented in workstations and routers.
- This layer is concerned with the format of datagrams as defined in the internet protocol (IP).
- The protocols in this layer include Address Resolution Protocol (ARP),
- Reverse Address Resolution Protocol (RARP) and
- Internet Control Message Protocol (ICMP).

TCP/IP Transport Layer

- Also known as host-to-host layer.
- This layer is concerned with the transmission of the data.
- The two main protocols that operate at this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- TCP is reliable transmission protocol and it guarantees that the proper data transfer will take place.
- UDP is not designed to be reliable or guarantee data delivery.

Functions of Transport Layer

1. Service point addressing: - Delivery is from specific process on computer to specific process on another computer. For this transport layer uses port addresses.
2. Segmentation and reassemble: -Each segment of a message contains a sequence number which is used to reassemble the message correctly.
3. Connection control:-Logical connection is created between source and destination for the duration of complete message transfer.
4. Flow control:-Flow control is performed end to end.
5. Error control:-Error control is performed process to process. It ensures that entire message arrives at receivers transport layer without error (damage or loss or duplication). Error correction is done by retransmission.

TCP/IP Application Layer

- The application layer is concerned with providing network services to applications.
- There are many application network processes and protocols that work at this layer, including
- Hyper Text Transfer Protocol (HTTP), Simple Mail Transport Protocol (SMTP) and File Transfer Protocol (FTP).

Solved Problems

Self Test (Multiple Choice Questions)

6.6 TCP / IP Protocol Suite:

1. Host-to-Network: **SLIP and PPP,**
2. Internet Layer-**ARP, RARP and IP**

   Introduction, IPv4, IPv6 (Header Format), Difference between IPv4 & IPv6.
3. Transport Layer: **TCP and UDP (Frame Format, port addresses),**
4. Application Layer: **FTP, SMTP, DNS.**

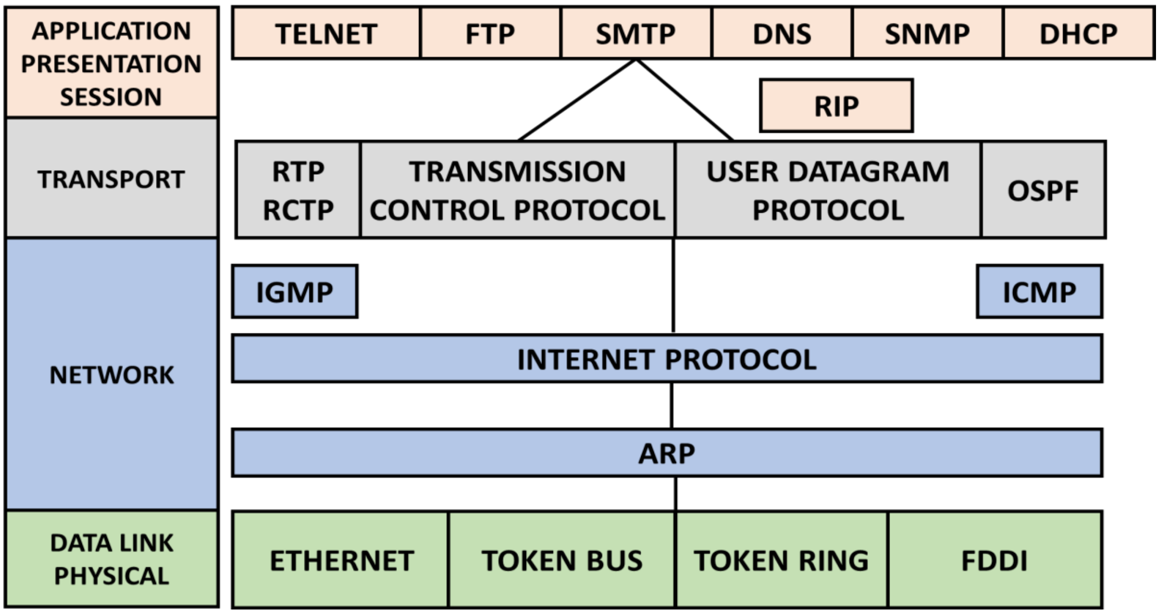


Fig: TCP/ IP Protocol Suite

1. Host-to-Network Layer Protocol

Host to network Layer Defines two protocols

- SLIP
- PPP

SLIP and PPP Protocols allow a user to dial into an ISP over Telephone Line.

SLIP (Serial Line Internet Protocol):

- It designed to work over serial ports and modem connections.
- Defines a sequence of bytes that frame IP packets on a serial line.
- Commonly used for point-to-point serial connections running TCP/IP.
- It is designed to transmit signals over a serial connection and has very low overhead.
- Data transmission with SLIP is very simple.
- This protocol sends a frame composed only of data to be sent followed by an end of transmission character (the END character, the ASCII code 192).
- A SLIP frame looks like:

Data to be transmitted	END

Problems with SLIP:

- SLIP does not perform error detection and correction.
- SLIP does not provide any authentication.
- SLIP is not approved internet standard.
- SLIP supports static IP address assignment.

PPP (Point to Point Protocol):

- It is a much more developed protocol than SLIP (which is why it is replacing it).

- It transfers additional data, better suited to data transmission over the Internet.
- PPP is More Complex than SLIP.
- PPP Protocol supports a set of Authentication Protocol.

Line Control Protocol (LCP):

- Responsible for establishing, maintaining, and terminating connection.

Password Authentication Protocol (PAP):

- The second is of authentication.
- Password Authentication is used.

Network Control Protocol (NCP):

- After authentication is done, PPP sends NCP packet.
- This packet tells ISP server what kind of traffic is to be passed over PPP link.

IP Control Protocol (IPCP):

- Finally the IP packets are exchanged.
- IPCP Establishes and terminates the Network layer connection.

PPP solves the problems of SLIP:

- PPP is point to point protocol.
- PPP perform error detection.
- PPP provides authentication and security.
- PPP is approved internet standard.
- PPP supports IP and other protocols.
- PPP supports Dynamic IP address assignment

PPP Frame Format:

Flag	1 Byte
Address	1 Byte
Control	1 Byte
Protocol	1 or 2 Byte

Data and Padding	Variable
Frame check Sequence	2 or 4 Byte
Flag	1 Byte

Difference between SLIP and PPP:

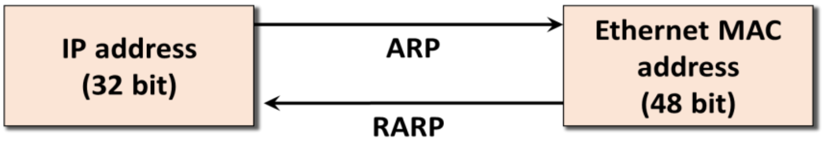
SLIP	PPP
Serial Line Internet Protocol does not establish or maintain connection between the client and ISP server.	In PPP, LCP (Line Control Protocol) is responsible for establishing, maintaining and termination connection between two end points.
Communication starts once the connection between two modems are established.	Communication begins only after authentication and the types of traffic is sent by the client.
Type of traffic cannot be selected in SLIP.	Type of traffic can be selected by NCP(Network Control Protocol)
No protocol for termination.	IPCP(IP Control Protocol) terminates a network layer connection between the user and ISP.
No addressing mechanism provided.	Additional services for addressing mechanism is provided
Doesn’t allow error control	Allows error control
No provision for data compression	Provides Data compression

2. Internet Layer Protocols

- The Four Network Layer protocols are:
  - **ARP**
  - **RARP**
  - **IP**
  - **ICMP**

1. **ARP-Address Resolution Protocol**

- ARP takes the IP address of a host as input & gives its corresponding physicaladdress as the output.
  - The Internet is based on IP addresses
  - Data link protocols (Ethernet, FDDI, ATM) may have different (MAC)addresses
- The ARP and RARP protocols perform the translation between IP addresses andMAC layer addresses.

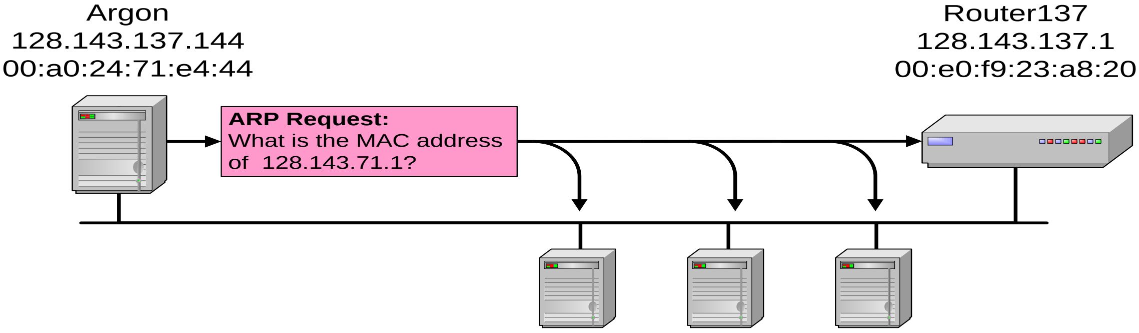


- ARP sends the IP broadcast message to all the computer on the network.
- The computer whose IP address matches the broadcast IP address sends a reply and along with, it's physical address to the broadcasting computer.
- All other computers ignore the broadcast message.

Address Translation with ARP

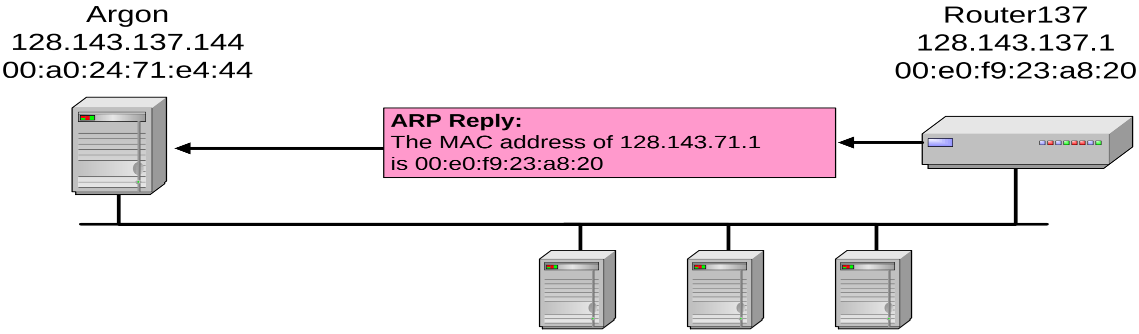
Example:

ARP request: Argon broadcasts an ARP request to all stations on the network: "What isthe hardware address of Router137?"

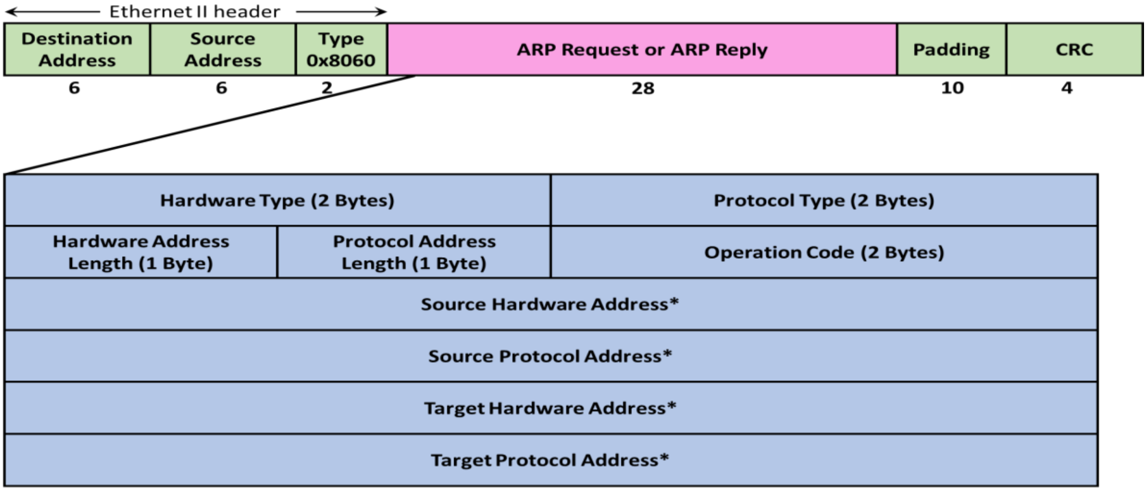


ARP Reply:

Router 137 responds with an ARP Reply which contains the hardware address



ARP Packet Format:



* Note: The length of the address fields is determined by the corresponding address length fields

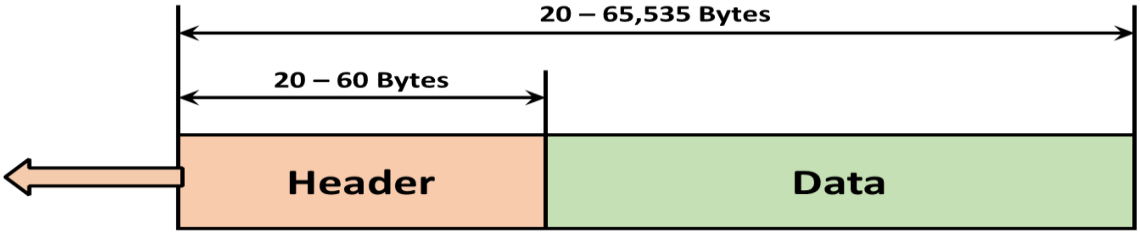
2. RARP (Reverse Address Resolution Protocol)

- If we have to obtain the IP address corresponding to the given Ethernet address.
- RARP works in very similar way of ARP, but in exactly opposite direction.
- The RARP server looks at this request.
- Then it looks up the Ethernet address in its configuration files and sends back thecorresponding IP address.

ARP	RARP
ARP converts IP address to its MAC address	RARP converts Ethernet MAC address to IP address
ARP broadcast IP address to discover its equivalent MAC address	RARP broadcasts systems MAC address
ARP table is maintained by local host	RARP table is maintained by RARP server
RFC 826 describes ARP	RFC 903 describes RARP

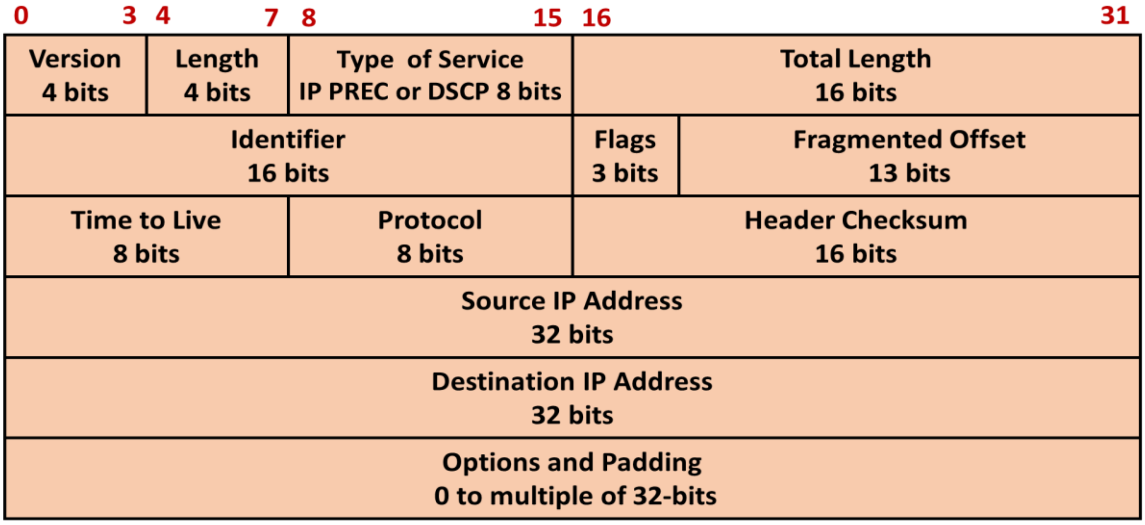
3. Internet Protocol (IP)

- IP is internet Protocol.
- It is unreliable protocol because it does not provide any error control and flow control.
- Packets in IP are called “Datagram”.
- Datagram is variable length packet with two parts –header and data



a. IP Datagram

IP Header Format



0 3	4 7	8 15	16	31
Version 4 bits	Length 4 bits	Type of Service IP PREC or DSCP 8 bits	Total Length 16 bits	
Identifier 16 bits			Flags 3 bits	Fragmented Offset 13 bits
Time to Live 8 bits		Protocol 8 bits	Header Checksum 16 bits	
Source IP Address 32 bits				
Destination IP Address 32 bits				
Options and Padding 0 to multiple of 32-bits				

b. Header Format

Fields in the IP header:

Version: is a 4-bit field that identifies the IP version being used. The current version is 4, and referred as IPv4.

Length: is a 4-bit field containing the length of IP header in 32-bit increments. Minimum length of an IP header is 20 bytes, or five 32-bit increments. Maximum length of an IP header is 24 bytes, or six 32-bit increments, i.e. in multiples of 4 bytes.

Type of Service (ToS): is the 8-bit ToS uses 3 bits for IP Precedence, 4 bits for ToS with the last bit not being used. The 4-bit ToS field, although defined, has never been used.

- **DS/ECN field:**previously known as Type-of-Service (TOS) field
  - **Differentiated Service (DS) (6 bits):** Used to specify service level (currently not supported in the Internet)
  - **Explicit Congestion Notification (ECN) (2 bits):**New feedback mechanism used by TCP.

Total Length: Specifies the length of the IP packet that includes the IP header and the user data. The length field is 2 bytes, so the maximum size of an IP packet is 216 – 1 or 65,535 bytes.

Identifier: Unique identification of a datagram from a host. Incremented whenever a datagram is transmitted.

Flags: 3-bits

- First bit always set to 0
- DF bit (Do not fragment)
- MF bit (More fragments)

Fragment Offset: Offset of the payload of the currentfragment in the original datagram.

This field contains the offset (in terms of 8 bytes units) from the start of IP datagram. So again, this field is used in reassembly of fragmented IP datagrams.

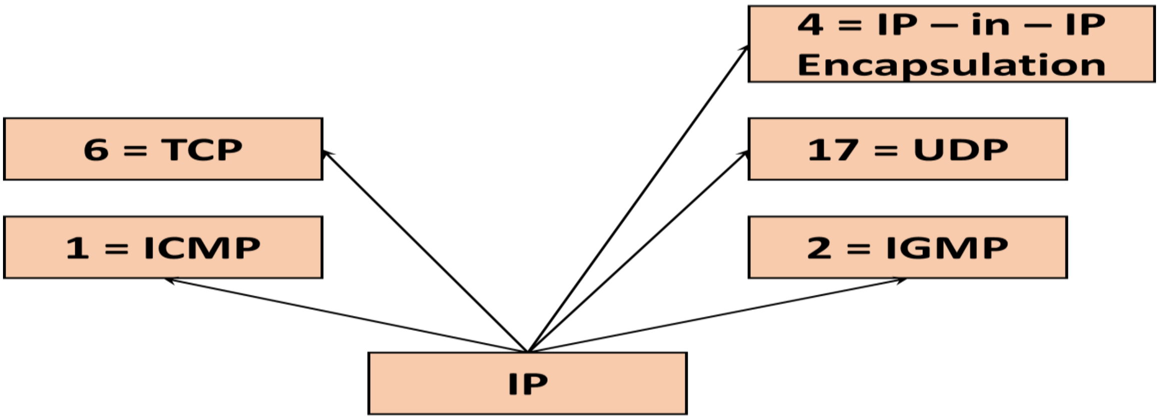
Time to Live (TTL): Specifies longest paths before datagram is dropped.

Role of TTL field: Ensure that packet is eventually dropped when a routing loop occurs.

Used as follows:

- Sender sets the value (e.g., 64)
- Each router decrements the value by 1
- When the value reaches 0, the datagram is dropped

Protocol: Specifies the higher-layer protocol.Used for demultiplexing to higher layers.



Header Checksum: A simple 2-Byte long checksum which is computed for the header of the datagram. The receiving host will discard the packet if it fails the checksum calculation.

Source IP Address: is a 32-bit IP address of the sender.

Destination IP Address: is a 32-bit IP address of the intended recipient.

Options: Security restrictions

- **Record Route:** each router that processes the packet adds its IP address to the header.
- **Timestamp:** each router that processes the packet adds its IP address and time to the header.
- **Source Routing:** specifies a list of routers that must be traversed.

Padding: Padding bytes are added to ensure that header ends on a 4-byte boundary.

Functions of the IP

1. **Addressing:**
   - In order to perform the job of delivering datagrams, IP must know where to deliver them to. For this reason, IP includes a mechanism for host addressing.
2. **Data Encapsulation and Formatting/ Packaging:**
   - IP accepts data from the transport layer protocols UDP and TCP.
   - It then encapsulates this data into an IP datagram using a special format prior to transmission.
3. **Fragmentation and Reassembly:**
   - IP fragment IP datagrams into pieces.

- The receiving device uses the reassembly function to recreate the whole IP datagram again.

4. **Routing / Indirect Delivery:**
    - When an IP datagram must be sent to a destination on the same local network, this is done using direct delivery.
    - However, if the final destination is on a distant network not directly attached to the source datagram must be delivered indirectly.

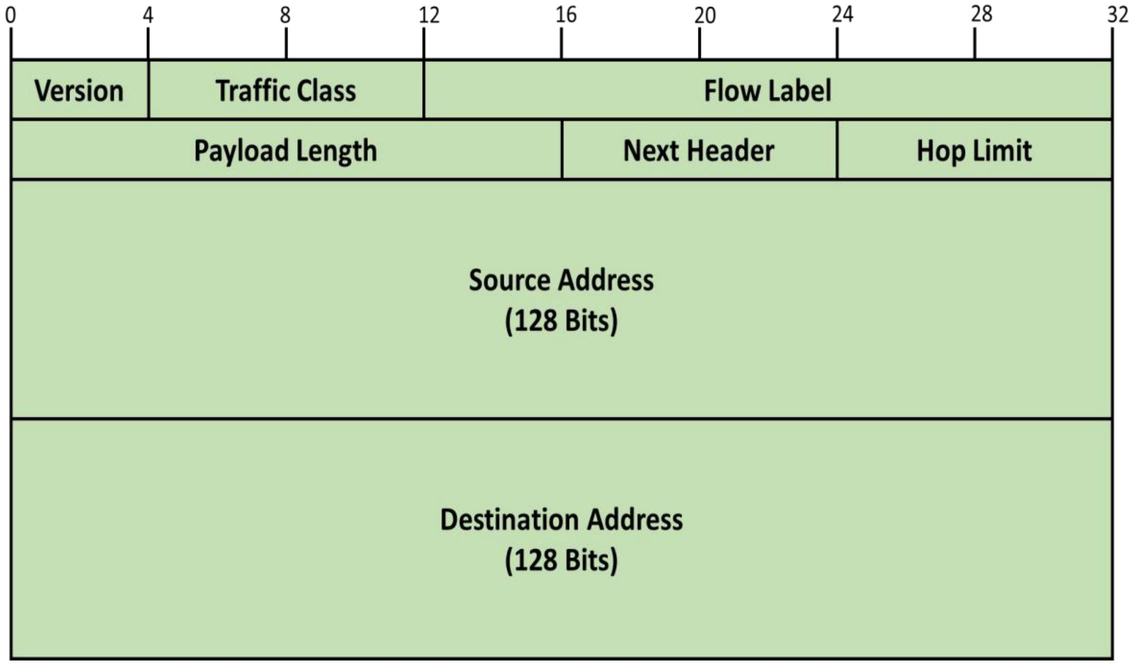
IPV6

- IP version 6 (IPv6) is an advanced version of IPv4.
- It takes all good features of IPv4 and adds new ones.
- Larger address space: IPv6 uses 128 bit(16 Bytes) Address.
- Better header format: This simplifies and speeds up the routing process.
- New options. IPv6 has new options to allow for additional functionalities.
- Allowance for extension: IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

IPv6 major goals:

1. Support billions of hosts.
2. Reduce the size of the routing tables.
3. Simplify the protocol.
4. Provide better security (authentication and privacy).
5. More attention to the type of service
6. Aid multicasting by allowing scopes to be specified.
7. Make it possible for a host to roam without changing its address.
8. Allow the protocol to evolve in the future.
9. Permit the old and new protocols to coexist for years.

IPv6 Header Format



Header Fields:

- **Version (4-bit):** Defines the version number of the IP. For IPv6, the value is 6.
- **Priority (4-bit):** Defines the priority of the packet with respect to traffic congestion.
- **Flow label (3-byte /24-bit):** It is designed to provide special handling flow of data.
- **Payload length (2-byte):** Defines the length of the IP datagram excluding the baseheader.
- **Hop limit (8-bit):** Serves the same purpose as the TTL field in IPv4.
- **Next header (8-bit):**
  - Defines the header that follows the base header in the datagram.
  - The next header is either one of the optional extension headers used by IP or the header of an encapsulated packet such as UDP or TCP.
  - Note that this field in version 4 is called the protocol.
- **Source address:**
  - The source address field is a 16-byte (128-bit)
  - Internet address that identifies the original source of the datagram.
- **Destination address:**
  - The destination address field is a 16-byte (128-bit)
  - Internet address that usually identifies the final destination of the datagram.
  - However, if source routing is used, this field contains the address of the next router.

Sr. No	**IPv4**	**IPv6**

Sr. No	**IPv4**	**IPv6**
1.	Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits(16 bytes)in length.
2.	Uses broadcast addresses to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, multicast scoped addresses are used.
3.	Fragmentation is supported at Originating hosts and intermediate routers.	Fragmentation is not supported at routers. It is only supported at theoriginating host.
4.	IP header include a checksum.	IP header does not include a checksum.
5.	IP header includes options.	All optional data is moved toIPv6 extension headers.
6.	IPsec support is optional	IPsec support is required in a full IPv6 implementation.
7.	No identification of payload for QoS Handling by routers is present within the IPv4 header.	Payload identification for QoS handling By routers is included in theIPv6 header using the Flow Label field.
8.	Address must be configured either manually or through DHCP.	Addresses can be automatically assigned using stateless address auto configuration, assigned using DHCPv6, or manually configured.
9.	IP address represented in decimal number system	IP address is represented in hexadecimal number system
10.	"." used as separator	':' used as separator.
11.	Uses host address (A) resource records in the domain name system to map host names to IPv4 addresses.	Uses host address (AAAA) resource records in the domain name system to map host names to IPv6 addresses.
12.	ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	Uses ICMPv6 Router Solicitation and Router Advertisement to determine the IPv6 address of the best default gateway and is a required function
13.	Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer	Uses multicast Neighbor Solicitation messages for address resolution.

Sr. No	IPv4	IPv6
	address.	
14.	Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	Uses Multicast Listener Discovery (MLD) messages to manage local subnet group membership.
15.	Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA or IP6.INT DNS domain to map IPv6 addresses to host names.
16.	For QoS, IPv4 supports both differentiated and integrated services.	Differentiated and integrated services are both supported. In addition, IPv6 provides a flow label that can be used for more granular treatment of packets.

4. ICMP

- It is internet control message protocol.
- It reports error and sends control messages.
- Error reporting messages include – destination unreachable, source quench, time exceed, parameter problem, redirection etc.
- Query message includes –echo request and reply, time stamp request and reply, router solicitation and advertisement, etc.

Transport Layer Protocols

- Transport Layer Works on top of Internet Layer.
- It is concerned with transport of packets from the source to destination.
- In TCP/IP the transport layer is represented by two Protocols:
  - TCP
  - UDP

1. Transmission Control Protocol (TCP)

- TCP is transmission control protocol.
- It Provides:
  - Connection oriented service
  - Reliable service
  - Stream delivery service
  - Sending and receiving buffers

- Bytes and segments
- Full duplex service

❖ TCP is a connection oriented protocol.

- Connection oriented means that a virtual connection is established before any user data is transferred.
- If the connection cannot be established, the user program is notified.
- If the connection is ever interrupted, the user program finds out there is a problem.

❖ TCP is Reliable-

- Reliable means that every transmission of data is acknowledged by the receiver.
- Reliable does not mean that things don't go wrong, it means that we find out when things go wrong.
- If the sender does not receive acknowledgement within a specified amount of time, the sender retransmits the data.

❖ Stream delivery service:

- TCP is a stream oriented protocol.
- It allows the sending and receiving process to obtain as a stream of bytes.
- TCP creates a working environment in such a way that the sending and receiving processes seem to be connected by an imaginary “tube” This is called as stream delivery service.

❖ TCP : Flow Control

- Sending and receiving buffers:
- The sending and receiving process may not produce and receive data at the same speed.
- Hence TCP needs buffers for storage.
- There are two types of buffers used in each direction:

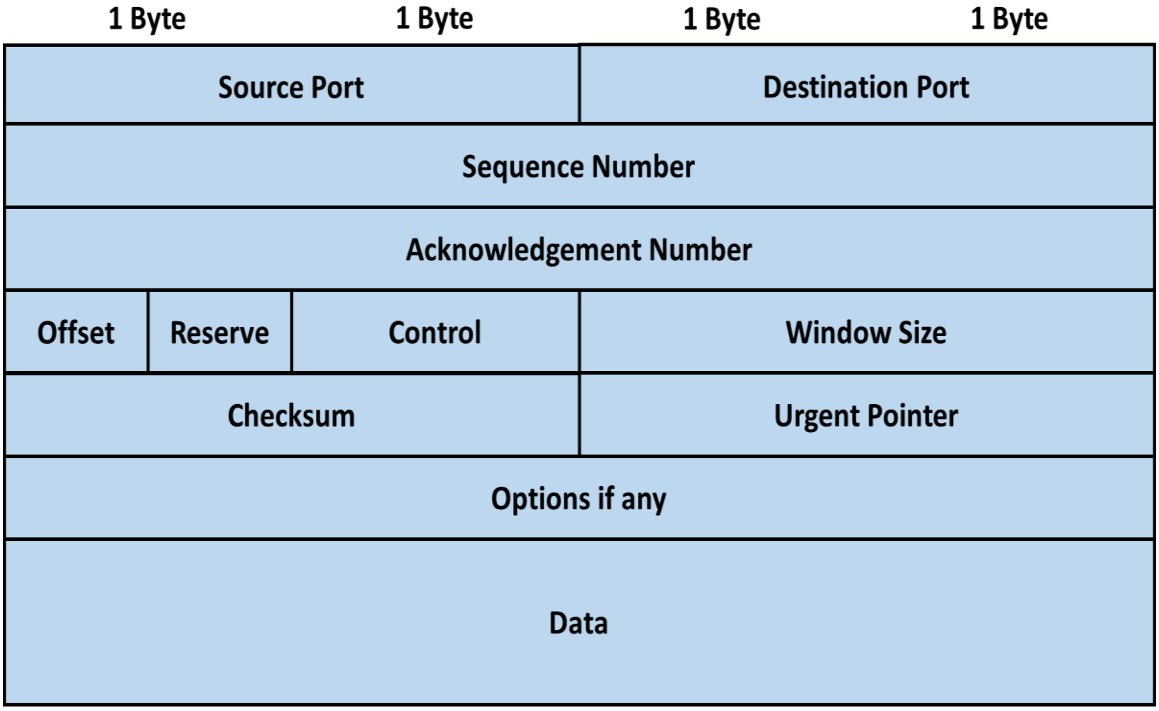
1) Sending buffer
2) Receiving buffer

❖ Full duplex service:

- TCP offers full duplex service where the data can flow in both the direction simultaneously.
- The TCP segments are sent both the directions.

- Process to process communication:
- The TCP uses port numbers as transport layer addresses.
- Also called as Port to Port communication.

TCP Header

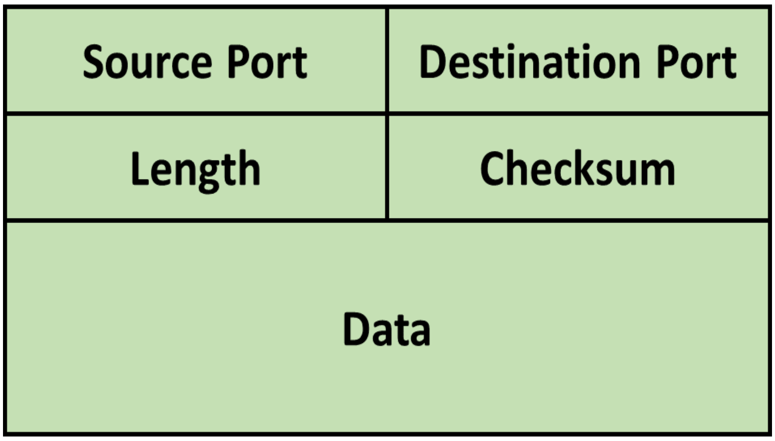


<table>
<tr><th colspan="2">1 Byte</th><th colspan="2">1 Byte</th><th colspan="2">1 Byte</th><th colspan="2">1 Byte</th></tr>
<tr><td colspan="4">Source Port</td><td colspan="4">Destination Port</td></tr>
<tr><td colspan="8">Sequence Number</td></tr>
<tr><td colspan="8">Acknowledgement Number</td></tr>
<tr><td>Offset</td><td>Reserve</td><td colspan="2">Control</td><td colspan="4">Window Size</td></tr>
<tr><td colspan="4">Checksum</td><td colspan="4">Urgent Pointer</td></tr>
<tr><td colspan="8">Options if any</td></tr>
<tr><td colspan="8">Data</td></tr>
</table>

2. User Datagram Protocol (UDP)

- It is connectionless protocol because data is sent without establishing a connectionbetween sender and receiver before sending the data.
- UDP is unreliable because data is delivered without acknowledgement.
- UDP does not perform Auto retransmission.
- UDP does not use flow control.
- UDP has high transmission speed.

UDP Datagram Format:



Source Port	Destination Port
Length	Checksum
Data	

UDP Vs TCP

	UDP	TCP
Complexity	UDP is less complex	TCP is more complex
Connection	UDP is connection less protocol	TCP is connection oriented protocol
Reliability	It provides guarantee of delivery of messages	It is unreliable
Ordering	Doesn't provide any ordering or sequencing guarantee	Guarantees order of message
Data Boundary	UDP does	Does not preserve data boundary
Speed	UDP is fast	TCP is slow
Header size	8 bytes	20 bytes
Weight of protocol	Light Weight Protocol	Heavy Weight Protocol
Congestion or Flow control	Handles reliability and congestion control, no option for flow control	Does Flow Control
Function	It is a protocol used in message transport or transfer. It is connectionless,i.e. one program can send a load of packets to another and that would be the end of the relationship.	As a message makes its way across the internet from one computer to another. This is connection based
Layer	Transport layer	Transport layer
Flow controlling	UDP has no flow control	TCP has flow control

Overhead	Overhead is very low	Overhead is low
Powerful	UDP is less powerful	TCP is more powerful
Acknowledgement	No Acknowledgement	Acknowledgement Segments

Application Layer Protocols

- SMTP
- FTP
- DNS
- Telnet

SMTP

- SMTP is simple mail transfer protocol.
- It is connection oriented text based protocol.
- Sender communicates with receiver using a command and supplying data over reliable TCP connection.
- SMTP is standard application layer protocol for delivery of email over TCP/IP network.
- SMTP establish a TCP connection between sender and port number 25 of receiver.
- Electronic Mail
- Three major components:
  - user agents
  - mail servers
  - simple mail transfer protocol: SMTP

User Agent

- Known as “mail reader”
- Composing, editing, reading mail messages e.g., Eudora, Outlook, Mozilla Thunderbird
- Outgoing, incoming messages stored on server.

Mail Servers

- Mailboxcontains incoming messages for user
- Messagequeue of outgoing (to be sent) mail messages

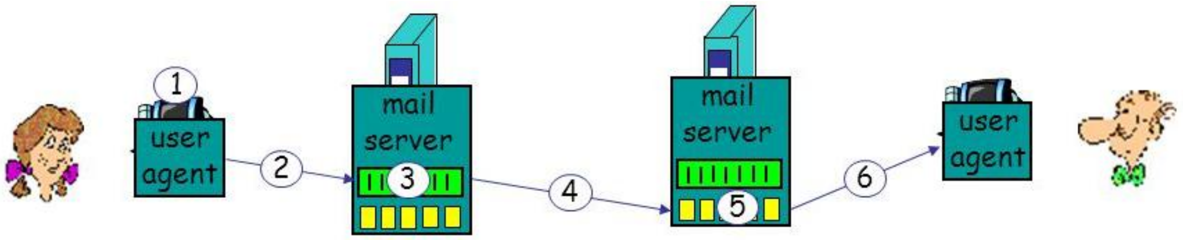
SMTP

- Protocol between mail servers to send email messages

- Client: sending mail server
- Server: receiving mail server

Scenario: Alice sends message to Bob

1) Alice uses UA to compose message and “to” bob@yahoo.com
2) Alice’s UA sends message to her mail server; message placed in message queue
3) Client side of SMTP opens TCP connection with Bob’s mail server
4) SMTP client sends Alice’s message over the TCP connection
5) Bob’s mail server places the message in Bob’s mailbox
6) Bob invokes his user agent to read message



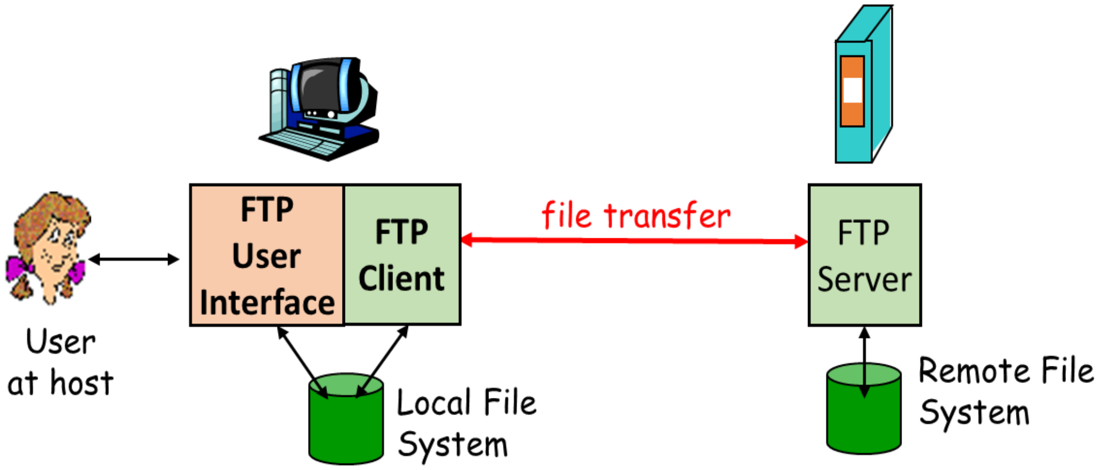
Sample SMTP Interaction

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250 Hello crepes.fr, pleased to meet you

C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok

C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok

C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
```

```
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

FTP

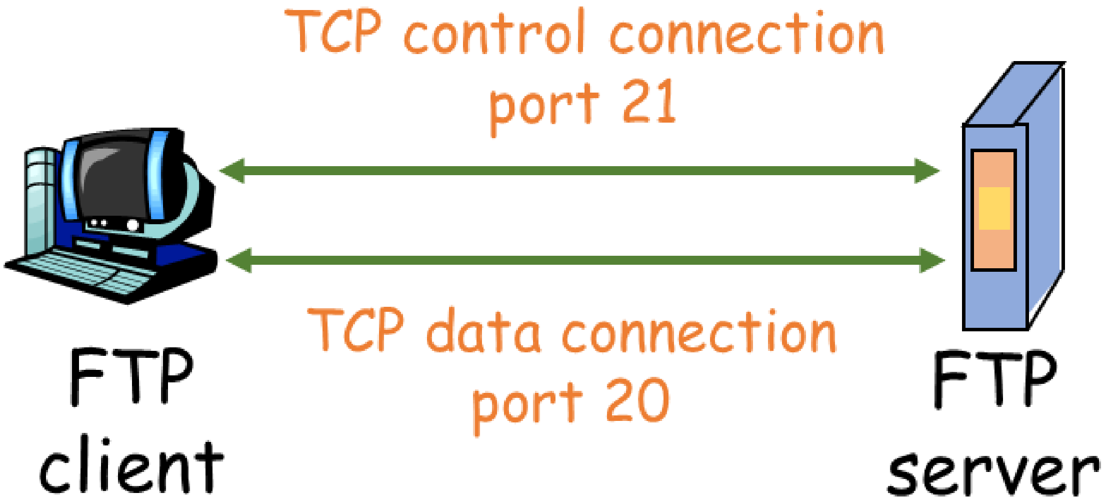
- FTP is used for copying a file from one host to the other.
- Some of the problem in transferring files:
    - Two systems may use different file name conventions.
    - Two systems may represent text data in different types.
- The directory structure of the two systems may be different.
- FTP provides a simple solution to all these problems.
- FTP established two connections between the client and server.
- One is for data transfer and the other is for the control information.



FTP: separate control, data connections

- FTP client contacts FTP server at port 21
- Client authorized over control connection.
- Client browses remote directory by sending commands over control connection.
- When server receives file transfer command, server opens 2nd TCP connection (for file) to client after transferring one file, server closes data connection.

- Server opens another TCP data connection to transfer another file.
- FTP server maintains “state”: current directory, earlier authentication.



- Control connection:
  - Control connection remains alive during the entire process.
  - The IP uses minimize delay type services because this is an interactive connection between a user and server.
- Data Connection:
  - Data connection uses the port 20 at the site.
  - This connection is opened when data to be transferred is ready and it is closed when transfer of data is over.
  - The service types used by IP is maximize throughput.

TELNET

- TELNET is abbreviation for Terminal Network.
- It is standard TCP/IP protocol for virtual terminal services proposed by ISO.
- TELNET enables establishment of connection to a remote system in such a way that a local terminal appears to be terminal at remote system.
- TELNET is general purpose client server application program.

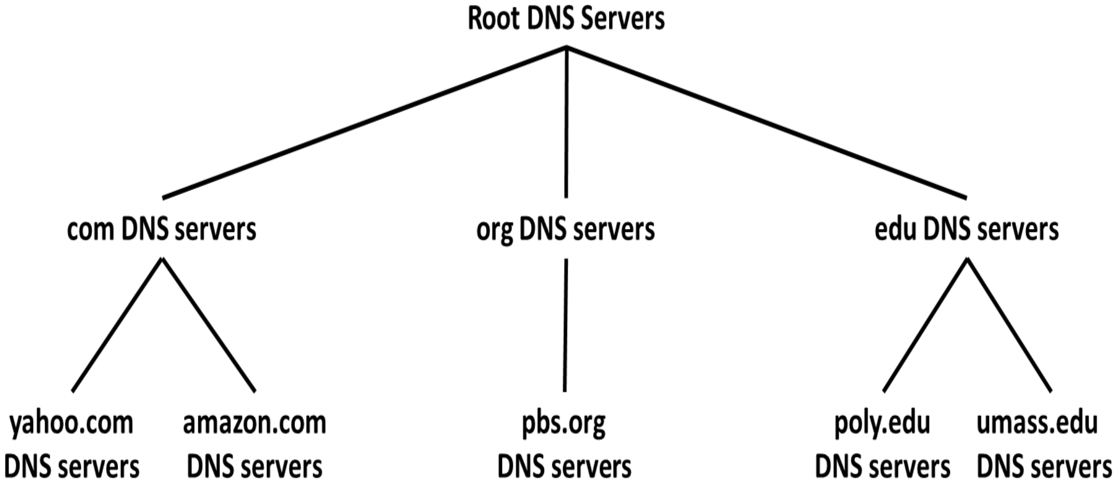
Remote login

- When user wants to access the application or utility located at the remote machine, he or she performs remote login.
- Here the telnet client and server program come into use.
- The user sends the keystrokes to local operating system. Local operating system accept it, but do not interpret them.
- The characters are send to TELNET client.

- TELNET client transform the character to a universal character set called Network Virtual Terminal Character and deliver them to the local TCP/IP stack.

DNS-Domain Name System

- Domain name is human readable name assigned to computer on the internet.
- Domain refers to group of computers called by common name.
- DNS is TCP/IP Application that maps Human Readable computer names to IP Addresses.
- DNS translates internet domain and host names to IP Addresses.



Example: Client wants IP for www.amazon.com:

- client queries a root server to find com DNS server
- client queries com DNS server to get amazon.com DNS server
- client queries amazon.com DNS server to get IP address for www.amazon.com

Solved Problems

Self Test (Multiple Choice Questions)

6.7 Comparison between OSI Reference and TCP / IP Network Model

Sr. No.	OSI Reference Model	TCP/IP Network Model
1.	OSI is a conceptual model	TCP/IP is a client-server model
2.	Not a protocol but a reference model used for understanding and designing the system architecture	Standard protocol used for every network including the Internet
3.	Seven layered model	Four layered model

4.	Supports Horizontal approach	Follows Vertical approach
5.	OSI is not	TCP/IP is Tangible
6.	Followsbottom-up approach	Followstop to bottom approach
7.	Transport layer guarantees delivery of packets	Transport layer does not guarantees delivery of packets
8.	Separate Presentation Layer	No Presentation Layer, characteristics are provided by Application Layer
9.	Separate Session Layer	No Session Layer, characteristics are provided by Transport Layer
10.	Network layer provides both connectionless and connection oriented services	Network layer provides only connection less services
11.	The protocol are hidden and couldbe easily replaced as the technology changes	Protocols cannot be easily replaced
12.	Defines the services, interfaces and protocols very clearly and clearly distinguishes them	Doesnot clearly distinguishes between service interface and protocols
13.	OSI Model is not reliable	TCP/IP Model is reliable
14.	OSI model has a problem of fitting the protocols into the model	TCP/IP model does not fit any protocol
15.	It is protocol independent	It is protocol dependent

6.8 Summary:

- The TCP/IP protocol suite maps to the four layers of the DARPA model: Application, Transport, Internet, and Network Interface.
- The protocols of the IPv4 Internet layer consist of ARP, IP (IPv4), ICMP, and IGMP.
- The protocols of the IPv6 Internet layer consist of IPv6, ICMPv6, ND, and MLD.
- The protocols of the Transport layer include TCP and UDP. TCP is a reliable, connection-oriented delivery service. UDP provides a connectionless datagram service that offers unreliable, best-effort delivery of data transmitted in messages.
- IP packets are multiplexed and demultiplexed between applications based on fields in the IPv4, IPv6, TCP, and UDP headers.
- TCP/IP components in Windows support two main APIs for networking applications: Windows Sockets and NetBIOS. Windows Sockets is a modern API that allows applications to manage stream sockets, datagram sockets, and raw sockets. NetBIOS

is an older API that allows applications to manage NetBIOS names, datagrams, and sessions.

- TCP/IP components in Windows support two naming schemes for networking applications: host names (used by Windows Sockets applications) and NetBIOS names (used by NetBIOS applications).

TCP/IP Protocols:

- **Connectionless protocols:**
  - IP
  - ICMP
  - UDP
- **Connection oriented protocol:**
  - TCP
  - SLIP
  - PPP
  - SMTP

6.9 Exercise (short answer questions)

6.10 References

Books

Wikipedia

MOOCs

YouTube Videos

OER

Unit7: Computer Security

1.31 **Learning Objectives:**After successful completion of this unit, you will be able to:

- Describe and analyze the hardware, software, components of a network and the interrelations.
- Information and Risk: Models including confidentiality, integrity and availability (CIA);concepts such as probability,consequence, harm, risk identification, assessment and mitigation; and the relationship between information andsystem risk
- Threats and attacks: Threats, how they materialise, typical attacks and how those attacks exploit vulnerabilities
- Computer SecurityArchitecture and Operations: Physical and process controls that can be implemented across anorganisation to reduce information and systems risk, identify and mitigate vulnerability, and ensure organisationalcompliance
- Secure Systems and Products: The concepts of design, defensive programming and testing and their applicationto build robust, resilient systems that are fit for purpose

This course teaches the security mind-set and introduces the principles and practices of computer security as applied to software, host systems, and networks. It covers the foundations of building, using, and managing secure systems.

1.32 **Introduction:**Today most of the shopping is done online. Many people work online, play online and live online. Since today human lives is increasingly depending on digital services, it is needed to protect the information from being maliciously disrupted or misused is really important. A breach in security can cause tremendous potentially harmful problems to the business and/or its customers. Setting up a security plan and an emergency action plan, the information storedon the computers and networks becomes safe and secure.

Computer security, also known as cybersecurity or IT security, is the process of preventing and detecting unauthorized use of your computer.Computer Security is usedto give protection to computing systems and the data that they store or access. Security means permitting legitimate user to do things what they want to do, while restricting unwanted things from happening. Computer Security consists of authentication and validation, encryption and physical security. Computer security can be treated as a basic management task. It is an expansion of the duty to defendthe organization's assets against misuse or loss. Also, the information stored and processed by computers is the most significant asset of most organizations.

The protection supported to a computerized information system to secure the applicable target of protecting the integrity, availability, and confidentiality of information system resources (which includes hardware, software, firmware, information or data, and telecommunications).

1.33 **Need for Security:**Prevention of data theft such as bank account numbers, credit card information, passwords, work related documents or sheets, etc. is essential in today’s communications since many of the day to day actions depend on the security of the data paths.Data present in a computer can also be misused by unauthorized intrusions. An intruder can modify and change the program source codes and can also use user’s pictures or email accounts to create derogatory content such as pornographic images, fake misleading and offensive social accounts. It is quite obvious that we would never like that any other person should have an illegal approach to our emails and our messages and our accounts and send spam emails to other people. And so computer security is very important not just on the personal level, but on the national level as well. To protect our electronic data from disclosure, change, or destruction of unauthorized individuals' we need security.

Computer Security is needed:

- For prevention of data theft such as bank account numbers, credit card information,passwords, work related documents or sheets, etc.
- To make data remain safe and confidential.
- To provide confidentiality which ensures that only those individuals should ever be ableto view data they are not entitled to.
- To provide integrity which ensures that only authorized individuals should ever be ablechange or modify information.
- To provide availability which ensure that the data or system itself is available for usewhen authorized user wants it.
- To provide authentication which deals with the desire to ensure that an authorizedindividual.
- To provide non-repudiation which deals with the ability to verify that message has beensent and received by an authorized user.

Self-test question

1. State the need of Computer Security.
2. Describe the need for Computer Security.

1.34 **Security Basics:**According to the definition of Computer Security there are three key objectives (principles) of computer security:

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

These three principles are often denoted as the CIA triad (Figure 7.1). The three concepts represent the fundamental security objectives for both data and for information and computing services.

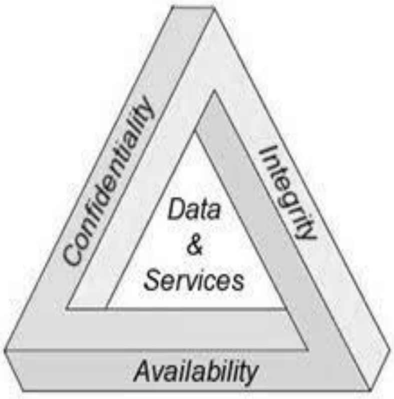


Figure 7.1:Security Requirement Triad (CIA)

Along with these two key objectives three other objectives are:

- Authentication
- Accountability
- Non-Repudiation

Confidentiality: Confidentiality refers to preventing the disclosure of information to unauthorized individuals or organizations. Confidentiality is essential for maintaining the privacy of the people whose personal information is held in the system.

This term covers two associated concepts:

- **Data Confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- **Information Privacy:** Assures that individuals control or impact what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

For example, user on internet needed to enter his login id and password for opening his/her online account (email, banking, etc….). The system attempts to enforce confidentiality by encrypting login id and password during transmission, by limiting the places where it might appear and by restricting access to the places where it is stored. If an unauthorized individual obtains the card number in any way, a breach of confidentiality will occur.

Integrity: Data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle and no modification is done without user's knowledge.

This term covers two associated concepts:

- **Data integrity:** Assures that information and programs are changed only with legitimate user's permission and in a specified and authorized manner.
- **System integrity:** Assures that a system performs its intended function in an unaffected manner, free from intentional or unintentional unauthorized access of the system.

Integrity is disrupted when a message is actively modified in transmission.

Availability: Ensures that systems work punctually and service is not denied to legitimate users. The information, resources and services must be available when it is needed. The goal of high availability systems is to remain available to legitimate at all times, besides the service disruptions like power outages, hardware failures, and system upgrades. Ensuring availability also includes preventing the systems from denial-of-service attacks, such as a flood of incoming messages to the target system mainly forcing it to shut down.

Authentication: Authentication is the process of identifying an individual's identity (for example person or computer) usually based on a username and password. In computer security, authentication is different from authorization. Authentication is the process of giving individuals access to system objects based on their identity. Authentication simply ensures that the individual is one who he or she claims to be.

Accountability: Accountability involves the processes, policies, and controls necessary to trace the actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.

Non-Repudiation: Nonrepudiation is the assurance that someone cannot deny something. Ensuring that a message transferred has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to assure that neither the sender of a message can later deny having sent the message and nor the recipient can deny having received the message.

Self-test question

1. What is CIA of security? Describe in brief.
2. Describe the basic principles of computer security.

1.35 **Threats to Security:**There are many different threats that face computer and network administrators as they attempt to protect their computer systems and networks. There are several forms of natural disasters that organizations have faced for years. There are a number of ways that we can break down the various threats. First way is to classify them is to separate threats those come from outside of the organization from those that are internal. Second way is to look at the different levels of sophistication of the attacks, from those by “script kiddies (Unskilled Individuals)” to those by “elite hackers (Highly Professionals).” And third way is to examine the various levels of organization of the various threats, from unstructured threats to highly structured threats. All of these are valid methods, and they in fact related to each other.

Viruses: Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs. A virus can do anything that any other programs can do.

A virus attaches itself to another program and executes secretly when the host program is running. Once a virus is executing, it can perform any function, such as erasing files and programs.

Phases of Computer Virus Life Cycle: A typical virus goes through the following four phases:

- Dormant phase
- Propagation phase
- Triggering phase
- Execution phase

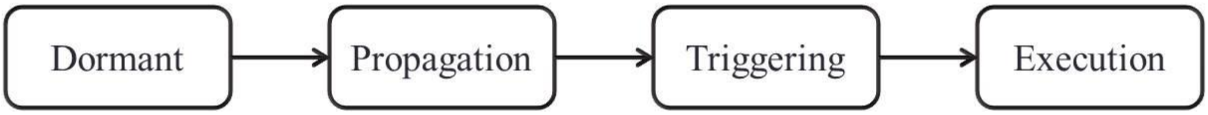


Figure 7.2: Phases of Computer Virus Life Cycle

Dormant phase: In this phase the virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.

Propagation phase: In this phase the virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

Triggering phase: The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

Execution phase: The function is performed, which may be harmless, e.g. a message on the screen, or damaging, e.g. the destruction of programs and data files

Types of Viruses:

- Boot Sector Virus
- Program Virus
- Multipartite Virus

- Stealth Virus
- Polymorphic Virus
- Macro Virus
- Memory Resident Viruses
- Non- Resident Viruses
- Overwriting Viruses
- Stealth Virus
- Companion Viruses
- Email Viruses
- Metamorphic Viruses
- Parasitic Viruses

Boot Sector Virus: Infects the boot or MBR of diskettes and hard drives through the sharing of infected disks and pirated software applications Once your hard drive is infected all diskettes that you use in your computer will be infected

Program Virus: Becomes active when the program file (usually with extensions .BIN, .COM, .EXE, .OVL, .DRV) carrying the virus is opened. It then makes copies of itself and will infect other programs on the computer.

Multipartite Virus: Hybrid of a Boot Sector and Program viruses. It infects program files and when the infected program is active it will affect the boot record.

Stealth Virus: Disguises itself to prevent from being detected by antivirus software. It alters its file size or conceals itself in memory

Polymorphic Virus: Act like a chameleon, changing its virus signature (binary pattern) every time it multiples and infects a new file

Macro Virus: Programmed as a macro embedded in a document, usually found in Microsoft Word and Excel. Once it gets in to your computer, every document you produce will become infected. A new type of virus may slip by your antivirus software if you don't have the most recent version installed

Memory Resident Viruses: This type of virus lives in the memory after its execution. Its inserts themselves as a part of operating system or application and can manipulate any file that executed. Copied or moved

Non-resident Virus: This type of virus executes itself and terminated or destroyed after specific time.

Overwriting Virus: Overwriting viruses deletes the original code and replaces it by new, malicious code. When the replaced file is executed the virus can try to replicate again. Since the original file is deleted by overwriting either in whole or in part, it is not possible to disinfect them. The original file is to be restored from a backup.

Stealth Virus: It's a virus that hides the modification it has made in the file or boot record

Companion Virus: This is the virus which, creates a new program instead of modifying an existing file

Email Viruses: Virus gets executed when E-mail attachment is open by recipient. Virus stands itself to everyone on the mailing list of sender

Metamorphic Viruses: This type of virus keeps rewriting itself every time. It may change their behaviour as well as appearance code

Parasitic Viruses: It attaches itself to executable code and replicates itself. When the infected code is executed, it will find other executable code or program infect.

Worms: Computer Worms are reproducing programs that run independently and travel across network connections. A worm is a computer program that copy itself from machine to machine in a network. The main difference between viruses and worms is the method in which they reproduce and spread. A worm usually exploits some sort of security hole in a piece of software or the operating system.Worms normally move around and infect other machines through computer networks. Using a network, a worm can expand from a single copy veryrapidly.

Computer worms are malicious software applications that designed to spread via computer networks. Computer worms are one form of malware along with viruses and Trojans. A person typically installs worms by inadvertently opening an email attachment or message that contains executable scripts.

Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Many worms that have been created are designed only to spread, and do not attempt to change the systems they pass through.

Virus V/S Worms:

	Virus	**Worm**
How does it infect a computer system?	It inserts itself into a file or executable program.	It exploits a weakness in an application or operating system by replicating itself.
How can it spread?	It has to rely on users transferring infected files/programs to other computer systems.	It can use a network to replicate itself to other computer systems without user intervention.
Does it infect files?	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	Usually not. Worms usually only monopolize the CPU and memory.
Whose speed is more?	Slower than worm.	Faster than virus.
Definition	The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.

Intruders: The act of intentionally accessing computer systems and networks without authorization or without permission is generally referred to ashacking. The individuals those who perform this activity are commonly ashackers.

An Intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system. In summary, this person attempts to violate Security by interfering with system Availability, data Integrity or data Confidentiality.

Intruders have to be extremely patient, since the process to gain access to a system takes persistence and strong-willed determination. The attacker has to conduct many pre-attack activities in order to obtain the information needed to perform the successful attack. Before launching the attack, intruder has to be very confident about the gathered information. An attack performed by an individual or even a small group of attackers comes under theunstructured threatcategory.

Insiders: Insiders may have accounts giving them legitimate access to computer systems, with this access originally having been given to them to serve in the performance of their duties; these permissions could be abused to harm the organization.

An Insider Threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems.

Insiders are more dangerous in many aspects than the intruders. Since insiders are having direct access and the necessary knowledge to cause instant damage to the organization. In most organizations security is designed to protect against intruders. Insiders may actually already have all the access they need to commit criminal activity such as fraud. In addition to direct access, insiders also normally have the details of the security systems in organization and so they can easily avoid detection. Attacks by insiders are often the result of employees who have become irritated, dissatisfied, and unhappy with their organization and are looking for ways to disturb work.

Criminal Organizations: Criminal activity on the Internet is more similar to the criminal activity in the real world. Fraud, extortion, theft, embezzlement, and forgery all take place in the electronic environment.

There is a difference between criminal groups and the “average” hacker if the level of organization that criminal elements are employed in their attack.

Attacks by criminal organizations can fall into the structured threat category, which is characterized by:

- Planning.
- Long period of time to conduct the activity.
- More financial backing.
- Corruption of or collusion with insiders.

Terrorists and Information Warfare: Every one across the worldhas been dependent on the Computer Systems, Networks (Specially the world wide network). Since all the nations are taking benefit of computerized systems, there is possibility that the essential elements of society may be targeted by organizations (criminal/ terrorist) or enemy nations interested to adversely affect another nation’s economy or defence systems. Many nations today have developed to some extent the capability to conduct information warfare. Information warfare is conducted against the information and information processing systems used by an enemy or friend nation. Information of an enemy nation not only can be the targeted, but also it can be used as a weapon.

Information warfare falls into the highly structured threat category which is categorized by:

- A long period of preparation (years is not uncommon).
- Tremendous financial backing.
- A large and organized group of attackers.

Avenues of Attack: There are two general reasons a particular computer system is attacked: either it is specifically targeted by the attacker, or it is an opportunistic target. In the first case, the attacker has chosen the target not because of the hard- ware or software the organization is running but for another reason, perhaps a political reason. An example of this type of attack would be an individual in one country attacking a government system in another. Alternatively, the attacker may be targeting the organization as part of a hacktivist attack. An example, in this case, might be an attacker who defaces the web site of a company that sells fur coats because the attacker feels that using animals in this way is unethical. Perpetrating some sort of electronic fraud is another reason a specific system might be targeted. Whatever the reason, an attack of this nature is decided upon before the attacker knows what hardware and software the organization has.

The second type of attack, an attack against a target of opportunity, is conducted against a site that has software that is vulnerable to a specific exploit. The attackers, in this case, are not targeting the organization; instead, they have learned of vulnerability and are simply looking for an organization with this vulnerability that they can exploit. This is not to say that an attacker might not be targeting a given sector and looking for a target of opportunity in that sector, however. For example, an attacker may desire to obtain credit card or other personal information and may search for any exploitable company with credit card information in order to carry out the attack.

Targeted attacks are more difficult and take more time than attacks on a target of opportunity. The latter simply relies on the fact that with any piece of widely distributed software, there will almost always be somebody who has not patched the system (or has not patched it properly) as they should have.

Steps in Attack: The steps those an attacker takes in attempting to breach a targeted network are alike to the security expert conducting a penetration test would take. Firstly the detail information about the organization is gathered by the attacker. There are several ways to conduct this activity, which includes, studying the organization’s web site, looking for postings on newsgroups, or referring resources. A number of different financial reports are available on the organizations web site which can provide the information and can be useful in attack. Another way to gather information is particularly a social engineering attack. The type of information that the attacker requires is IP addresses, contact numbers, names of individuals, and what networks the organization maintains. This step is known as "profiling" or "reconnaissance." Commands such as "whois" are useful in this step for obtaining information on IP blocks and DNS server addresses. Web search engines such as Google are used as a common tool that is useful in gathering. Next step, First step in the technical part of an attack, is to determine which target systems are available and active. This step moves us from summarizing to actual scanning and is done with methods such as a ping sweep which simply sends a "ping" (an ICMP echo request) to the target machine. If the machine responds, it is reachable. The next step is to perform a port scan to identify which ports are open. This gives the indication of which services may be running on the target machine. Determining the operating system (known as OS fingerprinting) which is running on the target machine, as well as specific application programs, follows, along with determining the services that are available. Various techniques are used to send specifically formatted packets to the ports on a target system to view the response.

This response includes the information that, like which operating system is running and which specific applications are running on the target system. Once this is done, the attacker would have a list of possible target machines, the Operating system running on them, and some specific applications or services to target.

Furthermore when the list of possible vulnerabilities is generated, the attacker is ready to proceed for an actual attack on the target

Self-test question

1. Define the term virus and describe the different phases of virus.
2. Explain threat to security in detail w.r.t. virus, worms, intruders, insiders.
3. Define virus. Explain atleast five types of viruses.
4. Define Virus and Logic bomb
5. Explain worm and virus. Differentiate between worm and virus.
6. Explain followingterms w.r.t. security :

   i) Intruders ii) Insiders.

1.36 **Security Attacks:** A security attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.Security attacks can be classified in various ways. In the common person's view they can be classified as Criminal Attacks (e.g. attack for financial gains), Publicity Attacks (e.g. Damage to a webpage) and Legal Attacks (e.g. manipulating legal system). But in a technical view, security attacks can be classified as passive attacks and active attacks.

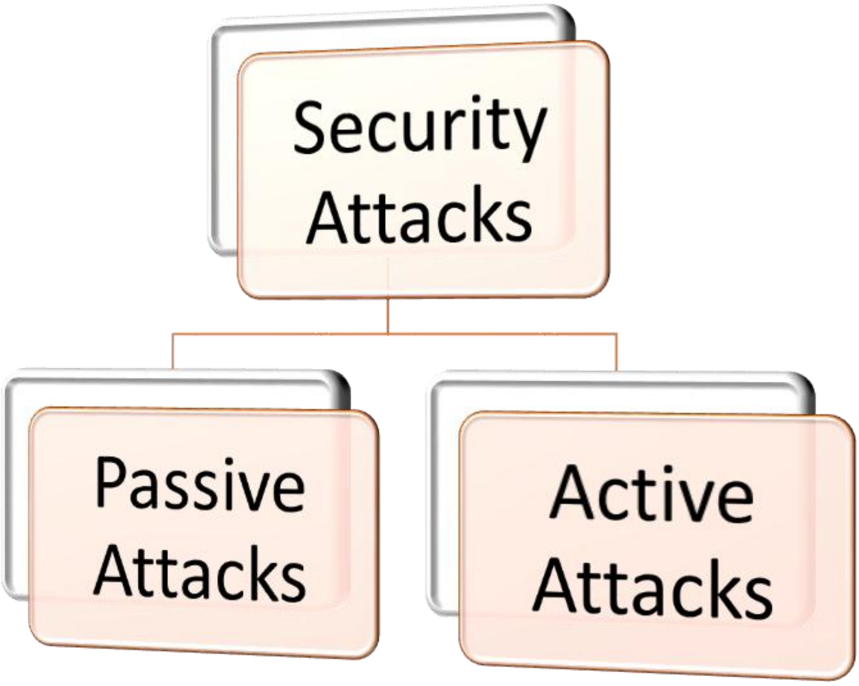


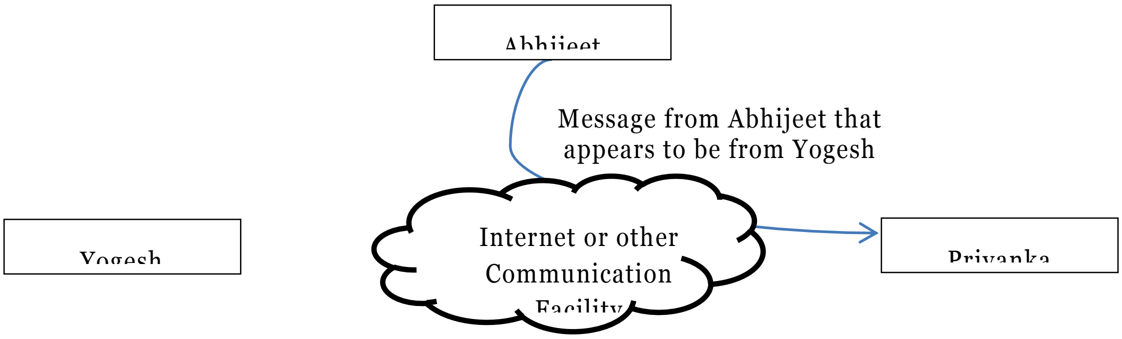
Figure 7.3: Types of Attacks

Active Attacks: Active attack is an attack in which attacker attempts to break the system or alter the data or system resources. He/she tries to modify information in the system. Active attacks involve some modification of the data stream or the creation of a false stream.

Active attacks can be subdivided into four categories as,

- Masquerade
- Replay
- Modification of messages
- Denial of service.

A **masquerade** takes place when one entity pretends (i.e. acts as if) to be a different entity. The concept is shown in figure 7.4 where Abhijeet pretends to be Yogesh and sends a message to Priyanka. This can be thought as impersonation.


Abhijeet
Message from Abhijeet that appears to be from Yogesh
Yogesh
Internet or other Communication Facility
Priyanka

c 7.4: Masquerade

Replay attack involves passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. E.g. If Priyanka wants to authenticate Yogesh before communicating with him. For that, Yogesh sends a password to Priyanka. This password is captured by Abhijeet and in future he may transmit this password to Priyanka so that he can easily masquerade Yogesh.

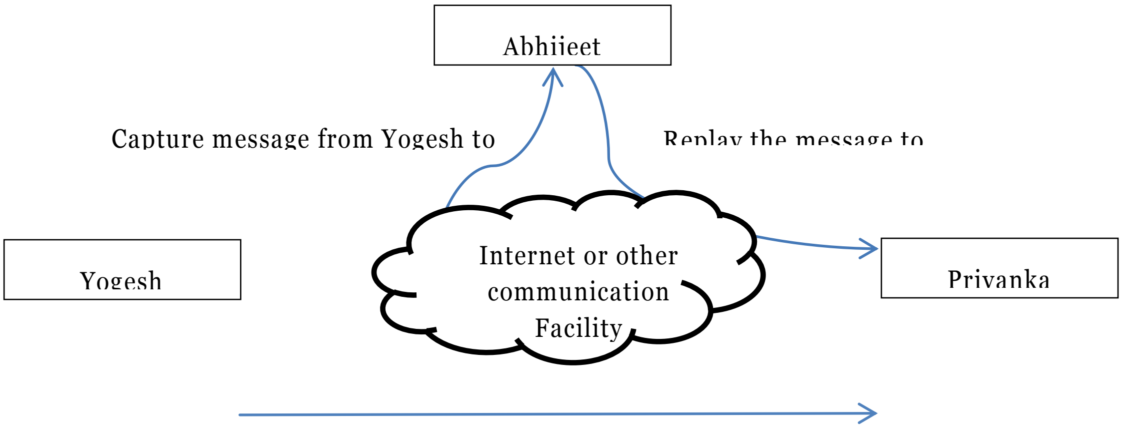

Abhijeet
Capture message from Yogesh to
Replay the message to
Yogesh
Internet or other communication Facility
Priyanka

Figure 7.5: Replay

In the attack called “modification of messages”, for producing an unauthorized effect, one of the following activities takes place.

- Some part of original message is changed
- Message is delayed
- Message is reordered

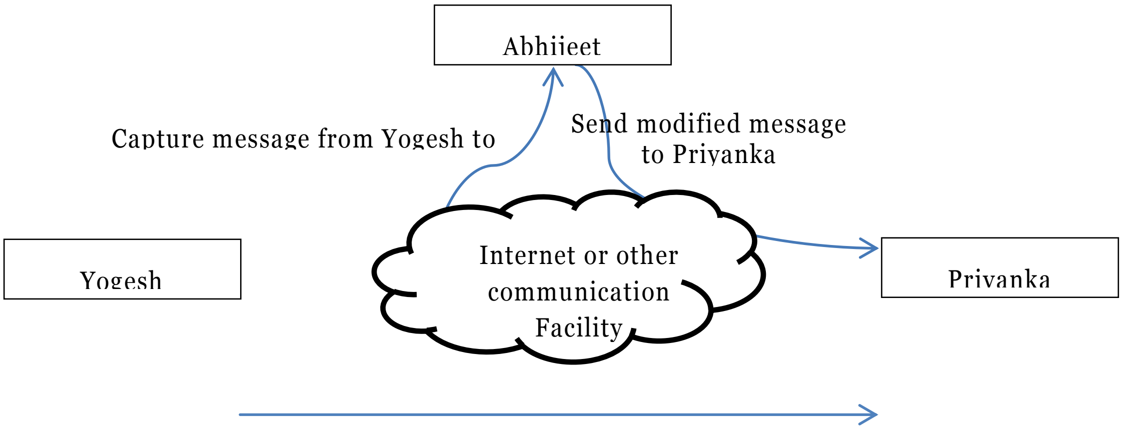

Abhijeet
Capture message from Yogesh to
Send modified message to Priyanka
Yogesh
Internet or other communication Facility
Priyanka

Figure 7.6: Modification of Messages

Example 1: A message meaning "Promote me as anchor for our special show." may be modified to mean "Promote *Abhijeet* as anchor for our special show."

Example 2: A message "Meet me immediately. Otherwise you will be fired from our channel" may be delayed by half an hour.

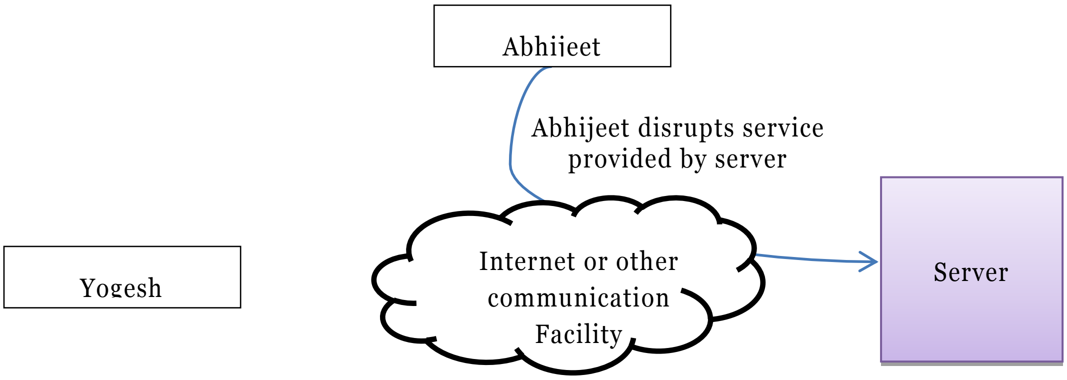

Abhijeet
Abhijeet disrupts service provided by server
Yogesh
Internet or other communication Facility
Server

Figure 7.7: Denial of Service

Denial of service (DoS) attack prevents or inhibits the normal use or management of communications facilities. DoS may prevent the legitimate (i.e. genuine) users from accessing some services.

Example 1: Unauthorized users may send too many login requests to a server using random user-ids continuously so that server will not be able to serve the requests of genuine users.

Example 2: An entity may suppress all messages directed to a particular destination (e.g., the security audit service).

Example 3: Disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Active attacks are very much different of passive attacks. As seen previously, passive attacks are difficult to detect. But measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.

- **Passive Attacks:**Passive attack is an attack in which attacker does not attempt to break the system or change the data. He/she tries to learn or make use of information from the system. As passive attacks do not make changes to the data, they are very difficult to detect. Passive attacks are those where attacker is involved in either eavesdropping (i.e. overhearing) or monitoring of transmissions. Attacker has intention of obtaining information that is being transmitted.

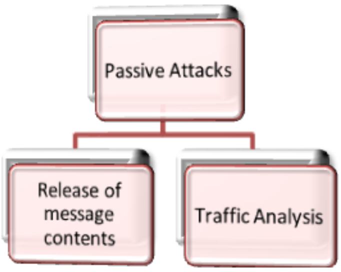


Figure 7.8: Types of Passive Attacks

Two types of passive attacks are the release of message contents and traffic analysis.

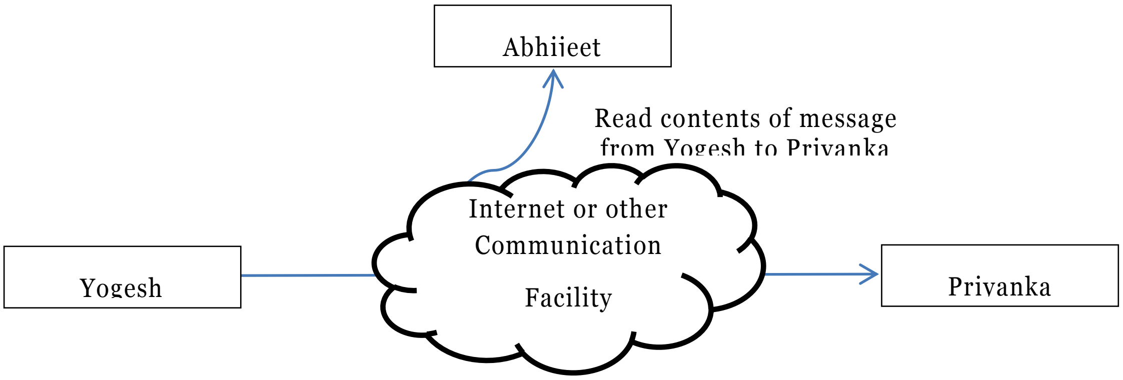

Abhijeet
Read contents of message from Yogesh to Priyanka
Internet or other Communication Facility
Yogesh
Priyanka

Figure 7.9: Release of Message Contents

The release of message contents is shown in figure 7.9. Yogesh is sending some important message (may be a telephone conversation, an electronic mail message or a SMS) to Priyanka. This message may contain sensitive or confidential information. If Abhijeet (as an attacker) eavesdrop the message, confidentiality of the communication is hampered. This should be prevented.

For preventing above attack, sender and receiver may use one of coding techniques for sending and receiving the message so that attacker will not be able to learn the message even if it is captured by him/her. Commonly used coding technique is encryption. Even if the sent messages are coded, attacker (sometimes referred as opponent) may be able to observe the pattern of the sent messages. He/she may determine various things related to the communication viz. length of messages, frequency of messages. Using this information he/she may guess the nature of communication. This type of attack is called as traffic analysis. It is shown in following figure 7.10.

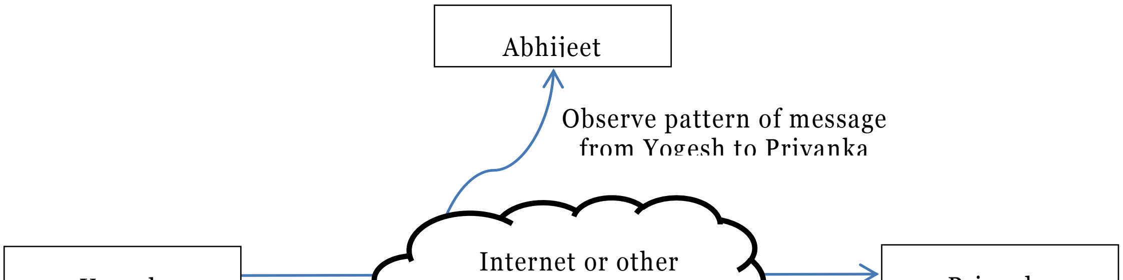


Figure 7.10: Traffic Analysis

As no any modification is done in passive attacks, they are very difficult to detect. When a message is sent neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. So, while dealing with passive attacks, prevention is more important than detection.

Self-test question

1. Describe the following attacks :
   i) Sniffing
   ii) Spoofing
2. Explain following attacks :
   i) Man In Middle Attack
   ii) Denial of Service Attack.

   Also suggest ways to avoid them.
3. List types of attacks. Explain backdoors and trapdoors attack.
4. Enlist any four cybercrimes. Describe any one in detail.
5. Define attack. Explain steps in attack.
6. Explain any four attacks on Computer Systems.
7. Explain DOS and DDOS with neat diagram.
8. With neat sketches explain the following :
   i) SYN Flood Attack
   ii) Main-in-the middle attack.
9. Describe SYN flooding attack with diagram.
10. Describewith diagrams:
    i) Man in the middle attack
    ii) Replay attack

1.37 Password Management:

User Name and Password: The user makes first contact with computer security when he logs on to a computer and is asked to enter username and password. The step is known as identification, where user states who he is. The second step is authentication, where user proves that he is who he claims to be.

Once user has entered his user name and password, computer compares the input against the records stored in password file. Login is success if entered user name and password is correct else system gives login failure message if user name and password is incorrect. Some systems keep a count of failed login tries and prevent or delay further login attempt. Authentication is needed not only at the start of session but also at certain intervals during the session (if a machine is idle for long period) to minimize attempt of an attacker to use unattended computer where another user is logged in.

User has an important role in password protection. Authentication is compromised if user name and password is exposed by user, either be sharing with someone or if written at someplace from where other could find it. So to avoid security breach to the system and organization security user should take care of safety of password and also should not disclose the user name password to anyone.

Managing Passwords: Password is private information shared between user and system authenticating the user. In an organization passwords could be distributed to the users either personally, by email or phone or by user’s choice. Password can be disclosed in several ways. For example a document containing password of an online account may be stolen or lost or any other person asking user’s password through phone or online communication. To resolve this problem, passwords should not be given to the calling person but call back should be done to user on an authorized phone number from recorded phone no in organizations internal address book. Several other ways like a mail by courier with personal delivery, can be adopted so that only authorized user will get the password.

Choosing Password: Often users choose passwords that are easy to remember and the same sequence of characters as they have for their user IDs. Users also normally select names of family members, their pets, or their favourite sports team for their passwords. The more you know about a user, the better your chance of discovering the user’s password.

Generally there are two basic strategies followed by attacker to disclose password.

Exhaustive search (Brute – Force): In this search attacker tries all combinations to discover password.

Intellectual search: In this attacker tries password that may have relation with user like, his name, relative or friends name, vehicle registration no, contact numbers, etc., or tries some popular passwords like ‘admin’, ’manager’. Also tries all passwords from dictionary words.

Then what is the defence, how to choose the password.

- Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.
- Use a random mixture of characters, Upper and lower case (A - Z, a – z) numbers (0 – 9), punctuation (‘*’, ‘#’, ‘!’, ‘$’, etc.) spaces and symbols.
- Don't use a word found in a dictionary, English or foreign.
- Never use the same password twice.

Things to avoid

- Don't just add a single digit or symbol before or after a word. e.g. "apple1"
- Don't double up a single word. e.g. "appleapple"
- Don't simply reverse a word. e.g. "elppa"
- Don't just remove the vowels. e.g. "ppl"
- Key sequences that can easily be repeated. e.g. "qwerty”, “asdf" etc.
- Don't just garble letters, e.g. converting e to 3, L or i to 1, o to 0. as in "z3r0-10v3"

Tips

- Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder.

Bad Passwords

- Don't use passwords based on personal information such as: name, nickname, birthdate, wife's name, pet's name, friends name, home town, phone number, social security number, car registration number, address etc. This includes using just part of your name, or part of your birthdate.
- Don't use passwords based on things located near you. Passwords such as "computer", "monitor", "keyboard", "telephone", "printer", etc. are useless.
- Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".
- Never use a password based on your username, account name, computer name or email address.

Choosing a password

- Use good password generator software.

- Use the first letter of each word from a line of a song or poem.
- Alternate between one consonant and one or two vowels to produce nonsense words. e.g. "taupouti".
- Choose two short words and concatenate them together with a punctuation or symbol character between the words. e.g. "seat%tree"

Changing your password

- You should change your password regularly, I suggest once a month is reasonable for most purposes.
- You should also change your password whenever you suspect that somebody knows it, or even that they may guess it, perhaps they stood behind you while you typed it in.
- Remember, don't re-use a password.

Protecting your password

- Never store your password on your computer except in an encrypted form. Note that the password cache that comes with windows (.pwl files) is NOT secure, so whenever windows prompts you to "Save password" don't.
- Don't tell anyone your password, not even your system administrator
- Never send your password via email or other unsecured channel
- Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- Be very careful when entering your password with somebody else in the same room.

Remembering your password

Remembering passwords is always difficult and because of this many people are tempted to write them down on bits of paper. As mentioned above this is a very bad idea. So what can you do?

- Use a secure password manager
- Use a text file encrypted with a strong encryption utility.
- Choose passwords that you find easier to remember.

Bad Examples

- "fred8" - Based on the user’s name, also too short.
- "christine" - The name of the users girlfriend, easy to guess
- "kciredref" - The users name backwords
- "indescribable" - Listed in a dictionary
- "iNdesCribaBle" - Just adding random capitalisation doesn't make it safe.
- "gandalf" - Listed in word lists
- "zeolite" - Listed in a geological dictionary

- "qwertyuiop" - Listed in word lists
- "merde!" - Listed in a foreign language dictionary

Good Examples

None of these good examples are actually good passwords, that's because they've been published here and everybody knows them now, always choose your own password don't just use somebody else.

- "mItWdOtW4Me" - Monday is the worst day of the week for me.
- How would a potential hacker get hold of my password anyway?

There are four main techniques hackers can use to get hold of your password:

- **Steal it.** That means looking over you should when you type it, or finding the paper where you wrote it down. This is probably the most common way passwords are compromised, thus it's very important that if you do write your password down you keep the paper extremely safe. Also remember not to type in your password when somebody could be watching.
- **Guess it.** It's amazing how many people use a password based on information that can easily be guessed. Psychologists say that most men use 4 letter obscenities as passwords and most women use the names of their boyfriends, husbands or children.
- **A brute force attack.** This is where every possible combination of letters, numbers and symbols in an attempt to guess the password. While this is an extremely labour intensive task, with modern fast processors and software tools this method is not to be underestimated. A Pentium 100 PC might typically be able to try 200,000 combinations every second this would mean that a 6 character password containing just upper and lower case characters could be guessed in only 27½ hours.
- **A dictionary attack.** A more intelligent method than the brute force attack described above is the dictionary attack. This is where the combinations tried are first chosen from words available in a dictionary. Software tools are readily available that can try every word in a dictionary or word list or both until your password is found. Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.

Self-Test (Multiple Choice Questions)

Self-test question

1. Describe different password selection criteria.
2. Explain, what are the components of good password?
3. Give characteristics of good password.

1.38 Role of people in Security (Do’s and Don’ts):

1.38.1 **Password Selection:** One should be very careful while selecting password. The importance of picking a good, secure password can't be highlighted enough. A compromised password can easily be used in ways that you are unlikely to detect, such as remote authentication. It is very important that users should frequently change the passwords associated with their computer accounts, so that it cannot be guessed by someone else. This is essential because the password is only the way that the computer verifies that someone logging in with your account (also known as your login or netid) is really you.

If someone else obtains your password, they can use your account to peruse your private data, including electronic mail; alter or destroy your files; and perform illegal activities in your name. And, in such cases, it is difficult to find out who the culprit is.

A poorly chosen password not only put all of your own files and data at risk but also places your colleagues and co-workers at higher risk by allowing an outsider to masquerade and avoid all restrictions generally in place for external access to the system. Thus, it is not safer to keep an easily guessable password of your account merely because you are ready personally to take the risk.

Given enough time, any password can be discovered merely by trying all possible combinations. For example, all lower case 6-character passwords can be discovered in about 3 to 4 days by brute force search on a machine which can try 1000 passwords per second.

Though, for well-chosen passwords a brute-force attack is still impractical or impossible even by using today's fastest computers, as long as passwords are changed from time to time and as long as the basic guidelines are followed.

1.38.2 **Password Selection Strategies:**

To eliminate guessable passwords while allowing the user to select a password that is memorable, four basic techniques are used:

- **User Education:** Users can be told the importance of using hard to guess passwords and can be provided with rules for choosing strong passwords. This strategy is not successful at most installations, mostly where there is a huge user population or a lot of turnover. Many users may simply ignore the guidelines. Others may not be good judges of what is a strong password. For example, many users may believe that reversing a word or capitalizing the last letter makes a password unpredictable.
- **Computer-Generated Passwords:**Computer-generated passwords too have problems. If the passwords are quite random in nature, users will not be able to memorize them. Even if the password is pronounceable, the user may have problem memorizing it and so it is possible that he will note it down. Generally computer-generated password schemes have a history of poor acceptance by users.
- **Reactive Password Checking:**A reactive password checking strategy is one in which the system periodically runs its own password cracker program to find

guessable passwords. The system revokes any passwords that are been guessed and notifies it to the user. This technique has a number of drawbacks. First, it is resource intensive if the job is done right. Since a determined attacker who is skilled to steal a password file can dedicate full CPU time to the mission for hours or even days, an effective reactive password checker is at a distinct disadvantage. Moreover, any existing passwords remain vulnerable till the reactive password checker finds them.

- **Proactive Password Checking:**The most favourable method to improve password security is a proactive password checker. In this, a user is permitted to select own password. But, at the time of selection, the system verifies whether the password is permissible and, if not, rejects it. Such verification is based on the beliefs that, with adequate direction from the system, users will be able to select memorable passwords rather than selecting large passwords probably that are not likely to be guessed in a dictionary attack. The technique with a proactive password checker is to have a balance between user acceptability and strength.

1.38.3 **Piggybacking:** Piggybacking is the technique of closely following a person who has just used an access card or PIN to gain physical access to a room or building. Piggybacking is an unauthorized entry to a system (either physically or logically) by using an authorized person's access code.

Piggyback can be done physically or electronically. Physical piggybacking is a technique for gaining access to controlled access areas when the control is achieved either by electronically or mechanically locked doors. For example, when a legitimate individual arrives and opens the door, the intruder also gets entered. Success of this technique is based on the excellence of the access control mechanism and the awareness of authorized personnel in refusing assistance with the unauthorized person.

Electronic piggybacking can take place on online computers where individuals use computer system that automatically do authentication. When a terminal is activated, the computer permits access, mostly based on secret password, token, or other exchange of required identification and authentication information (like a protocol). Computer can be compromised when a covert computer is connected to the same line through the telephone switching equipment and is being used when the authorized user is not using the terminal. The computer cannot distinguish between the two systems, it identifies only one terminal and one authorized user.

Electronic piggybacking can also be done when a user signs off or the session is terminated incorrectly, keeping the terminal or session in an active state or departing the computer in a state in which it believes that the user is still active.

1.38.4 **Shoulder Surfing:** Shoulder surfing is a technique in which attacker’s positions themselves in such a way that it could be easy to observe the authorized user typing the correct access code. For example, someone might shoulder surf when the person is entering his computer password, ATM pin, or credit card number. Criminals mostly use this technique to gain access to the personal accounts or get personal information, such as e-mails.

1.38.5 **Dumpster Diving:**Also known as trash picking.Before launching an actual attack attacker needs some information. Target's trash is one of the most likely places where the information can get. The process of going through targets trash for collecting information is known as Dumpster Diving.

If bank statements, credit card statements or other sensitive information are discarded without shredding or destroying it, it may be an opportunity for an attacker to gain information through dumpster diving.

1.38.6 **Installing Unauthorized Software/Hardware:**Organizations should have a policy that restricts the ability of normal users to install software and new hardware on their systems. A common example is a user installing unauthorized communication software and a modem to allow them to connect to their machine at work via a modem from their home. Another common example is a user installing a wireless access point so that they can access the organization's network from many different areas. In these examples, the user has set up a backdoor into the network, circumventing all the other security mechanisms in place. The term "rogue modem" or "rogue access point" may be used to describe these two cases.

A backdoor is an avenue that can be used to access a system while circumventing normal security mechanisms and can often be used to install additional executable files that can lead to more ways to access the compromised system. Security professionals can use widely available tools to scan their own systems periodically for either of these devices to ensure that users haven't created a backdoor.

Another common example of unauthorized software that users install on their systems is games. Unfortunately, not all games come in shrink-wrapped packages. Numerous small games can be downloaded from the Internet. The problem with this is that users don't always know where the software originally came from and what may be hidden inside it. Many individuals have unwittingly installed what seemed to be an innocuous game, only to have downloaded a piece of malicious code capable of many things, including opening a backdoor that allows attackers to connect to, and control, the system from across the Internet.

Because of these potential hazards, many organizations do not allow their users to load software or install new hardware without the knowledge and assistance of administrators. Many organizations also screen, and occasionally intercept, e-mail messages with links or attachments that are sent users. This helps prevent users from, say, unwittingly executing a hostile program that was sent as part of a worm or virus. Consequently, many organizations have their mail server's strip off executable attachments to e-mail so that users can't accidentally cause a security problem.

1.38.7 **Access by Nonemployees:**As has been mentioned, if an attacker can gain physical access to a facility, or interest in the welfare of the chances are very good that the attacker can obtain enough information to penetrate computer systems and networks. Many organizations require employees to wear identification badges when at work. This is an easy method to quickly spot who has permission to have physical access to the organization and who does not. While this method is easy to implement and can be a significant deterrent to unauthorized individuals, it also requires that employees actively challenge individuals who are not wearing the required identification badge. This is one area where organizations fail. Combine an attacker who slips in by piggybacking off of an authorized individual and an environment where employees have not been encouraged to challenge individuals without appropriate credentials and you have a situation where you might as well not have any badges in the first place. Organizations also frequently become complacent when faced with what appears to be a legitimate reason to access the facility, such as when an individual shows up with a warm pizza claiming it was ordered by an employee. It has often been stated by security consultants that it is amazing what you can obtain access to with a pizza box or a vase of flowers. If the organization doesn't enforce good password policies, a casual stroll through an office may yield passwords or other important information.

Another aspect that must be considered is personnel who have legitimate access to a facility but also have intent to steal intellectual property or otherwise exploit the organization. Physical access provides an easy opportunity for individuals to look for the occasional piece of critical information carelessly left out. With the proliferation of devices such as cell phones with built-in cameras, an individual could easily photograph information without it being obvious to employees. Contractors, consultants, and partners frequently not only have physical access to the facility but may also have network access. Other individuals who typically have unrestricted access to the facility when no one around are nighttime custodial crewmembers and security guards. Such positions are often contracted out. As a result, hackers have been known to take temporary custodial jobs simply to gain access to facilities.

1.38.8 **Security Awareness:**Probably the single most effective method to counter potential social engineering attacks, after establishment of the organization's security goals and policies, is an active security awareness program. The extent of the training will vary depending on the organization's environment and the level of threat, but initial employee training on social engineering at the time a person is hired is important, as well as periodic refresher training. Many government organizations have created security awareness posters to constantly remind individuals of this possible avenue of attack. Security newsletters, often in the form of e-mail, have also been used to remind employees of their security responsibilities.

An important element that should be stressed in training about social engineering is the type of information that the organization considers sensitive and which may be the target of a social engineering attack. There are undoubtedly signs that the organization could point to as indicative of an attacker attempting to gain access to sensitive corporate information. All employees should be aware of these indicators. The scope of information that an attacker may ask for is very large, and many questions attackers pose might also be legitimate in another context (asking for the phone number for somebody, for example). Employees should be taught to be cautious about revealing personal information and should especially be alert for questions regarding account information, personally identifiable information, or passwords.

1.38.9 **Individual User Responsibilities (Do's and Don'ts):** Individual user responsibilities vary between organizations and the type of business the organization is involved in, but there are certain very basic responsibilities that all users should be instructed to adopt:

- Lock the door to your office or workspace.
- Do not leave sensitive information inside your car unprotected.
- Secure storage media containing sensitive information in a secure storage device.
- Shred paper containing organizational information before discarding it.
- Do not divulge sensitive information to individuals (including other employees) who do not have an authorized need to know it.
- Do not discuss sensitive information with family members. (The most common violation of this rule occurs in regard to HR information, as employees, especially supervisors, may complain to their spouse about other employees or problems that are occurring at work.)
- Protect laptops that contain sensitive or important organization information wherever the laptop may be stored or left. (It's a good idea to ensure that sensitive information is encrypted on the laptop so that, should the equipment be lost or stolen, the information remains safe.)
- Be aware of who is around you when discussing sensitive corporate information. Does everybody within earshot have the need to hear this information?
- Enforce corporate access control procedures. Be alert to, and do not allow, piggybacking, shoulder surfing, or access without the proper credentials.
- Be aware of the correct procedures to report suspected or actual violations of security policies.
- Follow procedures established to enforce good password security practices. Passwords are such a critical element that they are frequently the ultimate target of a social engineering attack. Though such password procedures may seem too oppressive or strict, they are often the best line of defence.

As a final note on user responsibilities, corporate security officers must cultivate an environment of trust in their office, as well as an understanding of the importance of security. If users feel that security personnel are only there to make their life difficult or dredge up information that will result in an employee's termination, the atmosphere will quickly turn adversarial and be transformed into an "us versus them" situation.

Security personnel need the help of all users and should strive to cultivate a team environment in which users, when faced with a questionable situation, will not hesitate to call the security office. In situations like this, security offices should remember the old adage of "don't shoot the messenger."

Self-Test (Multiple Choice Questions)

Self-test question

1. Explain at least four roles of peoples in security.
2. What is meant by Dumpster diving? How it is used for attacking? Give the ways to avoid/prevent this.
3. Explain four password selection strategies.
4. Enlist any four consequences when the system is accessed by non - employee.
5. Explain individual user responsibilities in Computer Security.
6. Describe piggy backing and shoulder surfing.
7. Describe importance of security awareness in Society.

1.39 Summary

1.40 Exercise (short answer questions)

1. Describe security principles based on CIA.
2. Describe dumpster diving with its prevention mechanism.
3. Describe packet sniffing and packet spoofing attacks.
4. Explain the role of people with respect to password selection in detail.
5. Explain any four the password selection strategies.
6. Compare Insider and Intruders of four points and describe who is more dangerous.
7. Describe the role of people in security.
8. State any four different types of problems occur due to installation of unauthorized software/hardware.

1.41 References

1.41.1 Books

1.41.2 Wikipedia

1.41.3 MOOCs

1.41.4 YouTube Videos

1.41.5 OER

Unit8: Cryptography & Network Security

1.42 Learning Objectives: After successful completion of this unit, you will be able to:

- Understand cryptography.
- Understand transposition techniques
- Understand symmetric and asymmetric cryptography

- Understand Firewall technique
- Understand security topologies
- Understand intrusion detection system

1.43 Introduction:

Cryptology: Cryptology is the art or science that deals with data communication and storage in secure and secret form. It encompasses study of both cryptography and cryptanalysis.The term cryptology is derived from the Greek kryptós (“hidden”) and lógos (“word”). Security obtains from legitimate users being able to transform information by virtue of a secret key or keys—i.e., information known only to them. The resulting cipher, although generally inscrutable and not forgeable without the secret key, can be decrypted by anyone knowing the key either to recover the hidden information or to authenticate the source. Secrecy, though still an important function in cryptology, is often no longer the main purpose of using a transformation, and the resulting transformation may be only loosely considered a cipher.

Cryptography: Cryptography (from the Greek kryptós and gráphein, “to write”) was originally the study of the principles and techniques by which information could be concealed in ciphers and later revealed by legitimate users employing the secret key.Cryptography is one of the oldest techniques at least 4,000 years to convert readable text to unreadable and not understandable. Before 1900 B.C., Egyptian used symbols and pictures in a random fashion, to hide the meaning from those who did not know the meaning. The Greek’s been wrapping a tape around a stick, and then write the message on the wound tape. When the tape was unwound, the writing was meaningless. To decipher the message, the receiver of the message would of course have a stick of the same diameter. The Roman method of cryptography was known as the Caesar Cipher, the earliest known, and the simplest cipher technique. It works on the idea of shifting letters by an agreed upon number (three was a common historical choice), The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet and thus writing the message using the letter-shift. The receiving group would then shift the letters back by the same number and decipher the message.

Terms used in cryptography:

Plain Text: It is the original understandable message. Plain text is the contents of an ordinary sequential file readable as textual material. Plaintext is the input to an encryption algorithm. Plain text means its text that hasn't been formatted (i.e., a plain text file)

Example: Hello how are you.

Cipher text: It isthe transformed message.Cipher text is the output of the process performed on plaintext using an encryption algorithm. When plain text message is modified using any suitable scheme, the resulting message is called Cipher text or Cipher.Cipher text is the unreadable output of an encryption algorithm

Example: Y0ewfmGI4/0X/RYpTijcCU52t1wxCqk5

Secret Key: Key is the critical information used by the cipher, which must be known only to the sender & receiver.A secret key is used to set some or all of the various parameters used by the encryption algorithm.

Encryption: It is the process of transforming plaintext to cipher text using a cipher and a key. It is also known as encipheringor encoding.

Decryption: Decryption is the process of converting cipher text back to plaintext.It is also known as deciphering or decoding.

Cryptology: It involves both cryptography and cryptanalysis.Cryptology is the science of coding and decoding secret or hidden messages.

Cryptography (secret (crypto) writing (-graphy)): Cryptography is the art or science encompassing the principles and methods of converting an understandable message into one that is meaningless and then retransforming that message back to its original form. Cryptography is the art or science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or broadcast it through insecure networks (like Internet) so the information cannot be read by anyone except the intended receiver.

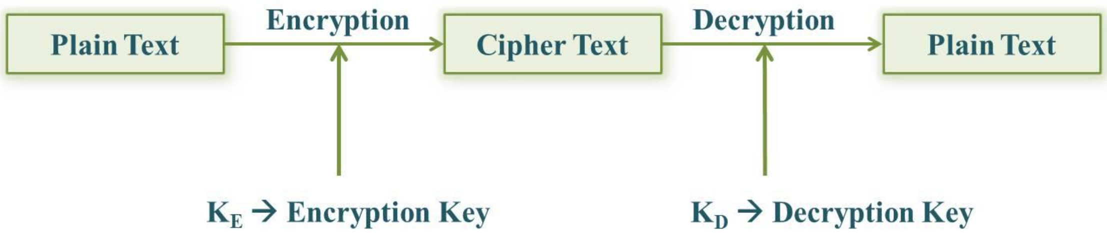
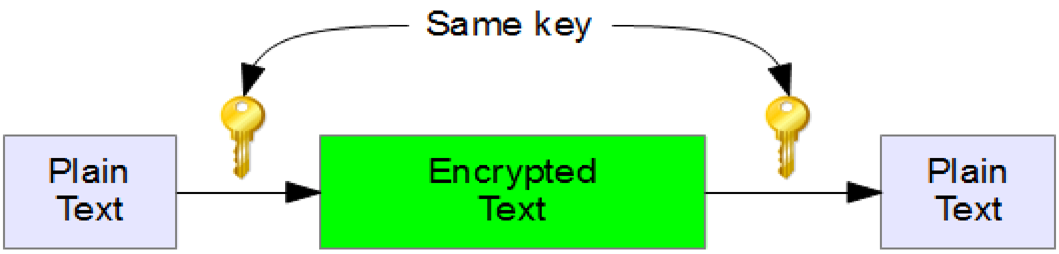


Figure 8.1 Cryptography

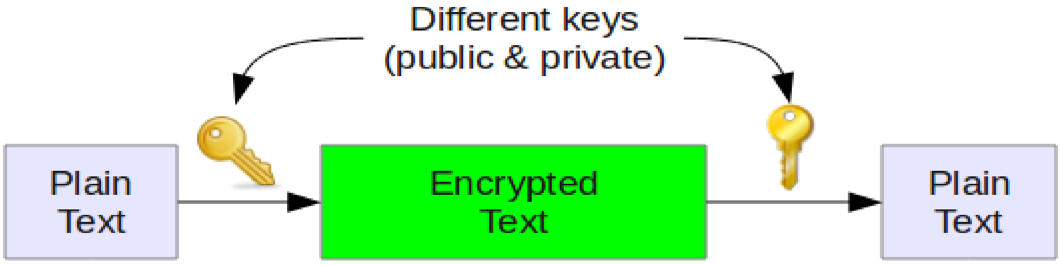
There are three types of cryptography techniques:

- **Secret key Cryptography:**This technique uses only a single key for encryption as well as decryption. The sender uses a key to encrypt a message whereas the receiver uses the same key to decrypt the message. Since only single key is used this technique is also known as symmetric key encryption.

  The maindifficultyof this technique is the distribution of key as this technique usesonly single key for encryption or decryption.



- **Public key cryptography:**This technique uses only a two keysone for encryption and other for decryption. The sender uses a key (Key 1) to encrypt a message whereas the receiver uses different key (Key 2) to decrypt the message. Since a pair of two different keys is used this technique is also known asymmetric key encryption.



- **Hash Functions:** No key is used in this technique. Rather, a fixed length hash value which is calculated on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be changed,compromised or affected by virus or by any attacker.

Cryptanalysis: Cryptanalysis (from the Greek kryptós and analýein, “to loosen” or “to untie”) is the science (and art) of recovering or forging cryptographically secured information without knowledge of the key.It is the study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. It is also called as code breaking.Whereas cryptography is the science of securing data, cryptanalysis is the science of exploring and breaching secure communication. Traditional cryptanalysis includes an interesting combination of analytical thinking, application of mathematical tools, pattern finding, patience, willpower, and good luck. Cryptanalysts are also called attackers.

Self-Test (Multiple Choice Questions)

Self-test question

1.44 Cryptography Techniques:The two basic building blocks of all encryption techniques are:

- SubstitutionTechniques
- Transposition Techniques

1.44.1 Substitution Techniques: Substitution techniques map plaintext characters or bits into cipher text characters. In substitution technique, the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is considered as a sequence of bits, then substitution includes replacing plaintext bit patterns with cipher text bit patterns.

Example: Caesar's cipher, monoalphabetic and polyalphabetic, and one-time pad.

Caesar's Cipher: Simplest and very first known substitution cipher used by Roman Emperor Julius Caesar. The Caesar cipher includes replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,

Plain Text : HELLO HOW ARE YOU

Cipher Text: KHOOR KRZ DUH BRX

In this technique alphabet is wrapped around, i.e. A is following letter Z as shown below

Plain Text	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Cipher Text	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**
Plain Text	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Cipher Text	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**

If numbers are assigned to each alphabet the A will be assign 0 and Z will be assign 25. Then algorithm can be expressed as follows.

For each plaintext letter **P**, substitute the cipher text letter **C,** Encryption E and Decryption D and Key K (Generally K = 3):

Then,

C = E (3, P) = (P + 3) mod 26

If a shift is of any amount, then the general Caesar algorithm is

C = E (K, P) = (P + K) mod 26

Where, K is any value from 1 to 25. The decryption algorithm is as follow

P = D (K, C) = (C - K) mod 26

Limitation of Caesar's Cipher: If an adversary knows that that a given cipher text is a Caesar cipher, then it is easy to discover plain text by performing a brute-force cryptanalysis: simply adversary has to try all the 25 possible keys only.

Three important characteristics of this problem enables adversary to use a brute-force cryptanalysis:

1. The encryption and decryption algorithms are known.

2. There are only 25 keys to try.

3. The language of the plaintext is known and easily recognizable.

Monoalphabetic Cipher: Monoalphabetic cipher is a cipher based on substitution. Mono, means one, indicates that each letter has a single replacement. Monoalphabetic ciphers are ciphers in which the same plaintext letters are always replaced by the same cipher text letters.

To construct a monoalphabetic cipher, some ordering ofthe alphabet is done, such as SOMERDINGXHBVLTUJWKYZFACPQ, and is paired with a plaintext alphabet,

Plaintext alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher text alphabet: SOMERDINGXHBVLTUJWKYZFACPQ

Then encipher and decipher is done by translating from the plaintext to cipher text alphabets and back, as usual. In this example **ALPHABET** becomes **SBUNSORY**.

However it is not particularly easy to remember apparently random orderings of 26 letters.

Caesar Cipher is one of the examples of Monoalphabetic Cipher.

Polyalphabetic: Polyalphabetic cipher is a cipher based on substitution. In monoalphabetic cipher each letter has a single replacement, and this is the main drawback of monoalphabetic cipher. In polyalphabetic cipher same letter is replaced by several ciphertext letters, depending on which alphabet is used. This technique makes cryptanalysis harder since have more alphabets to guess.

Vigenère cipher is the best known and one of the simplest, Polyalphabetic ciphers. In this technique, the collection of related Monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter a.

A general equation of the encryption process is

$$C_i = (P_i + K_i \, mod \, m) mod \, 26$$

And general equation of the decryption process is

$$P_i = (C_i - K_i \, mod \, m) mod \, 26$$

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword. For example, if the keyword is*cipher*, the message “thisprocesscanalsobeexpressed” is encrypted as

Key : CIPHERCIPHERCIPHERCIPHERCIPHE

Plaintext : THISPROCESSCANALSOBEEXPRESSED

Ciphertext:**VPXZTIQKTZWTCVPSWFDMTETIGXELH**

Expressed numerically, we have the following result.

Key	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15
Plain Text	19	7	8	18	15	17	14	2	4	18	18	2	0	13	0
Cipher Text	21	15	23	25	19	8	16	10	19	25	22	19	2	21	15
Key	7	4	17	2	8	15	7	4	17	2	8	15	7		
Plain Text	11	18	14	1	4	4	23	15	17	4	15	15	4		
Cipher Text	18	22	5	3	12	19	4	19	8	6	23	4	11		

The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword.

One-Time Pad: The one-time pad is a long sequence of random letters. These letters are combined with the plaintext message to produce the ciphertext. To decipher the message, a person must have a copy of the one-time pad to reverse the process. A one-time pad should be used only once (hence the name) and then destroyed. This is the first and only encryption algorithm that has been proven to be unbreakable.

To encipher a message, you take the first letter in the plaintext message and add it to the first random letter from the one-time pad. For example, suppose you are enciphering the letter S (the 19th letter of the alphabet) and the one-time pad gives you C (3rd letter of the alphabet). You add the two letters and subtract 1.

When you add S and C and subtract 1, you get 21 which is U. Each letter is enciphered in this method, with the alphabet wrapping around to the beginning if the addition results in a number beyond 26 (Z). To decipher a message, you take the first letter of the ciphertext and subtract the first random letter from the one-time pad. If the number is negative you wrap around to the end of the alphabet.

Example

Plaintext : **SECRETMESSAGE**

One-time pad:**CIJTHUUHMLFRU**

Ciphertext : **UMLKLNGLEDFXY**

1.44.2 Transposition Techniques: Transposition means rearranging the order of arrival of the elements of the plaintext. Transposition is also referred to as permutation. In this technique cipher text is generated by changing the position of the letters or elements of the plaintext.

For example rail fence and columnar techniques

Rail Fence Technique: Rail fence cipher is examples of transposition cipher. The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. The encryption key for a rail fence cipher is a positive integer. For example, to encipher the message "hello how are you" with a rail fence of key 2, we write the following:

H L O O A E O

E L H W R Y U

The encrypted message is HLOOAEOELHWRYU

To encipher the same message "hello how are you" with a rail fence of key3, we write the following:

H O A O

E L H W R Y U

L O E

The encrypted message is HOAOELHWRYULOE

Simple Columnar:A columnar transposition, also known as a row-column transpose, is a very simple cipher technique. In this technique, the message is written out in rows of a fixed length. The message is then read out by column by column, where the columns are chosen in some scrambled order. The number of columns and the order in which they are chosen is defined by a keyword. For example, the word CIPHER is 6 letters long. Therefore, there are 6 columns that will be read of in the following order: 1 4 5 3 2 6. The order is chosen by the alphabetical order of the letters in the keyword.

Single Columnar Cipher (Regular Case): In a single columnar transposition cipher (regular case) the empty spaces are filled with random letters.

For Example

Plaintext: Hello how are you. Meet me tomorrow.

Key:CIPHER

C	I	P	H	E	R
1	4	5	3	2	6
H	E	L	L	O	H
O	W	A	R	E	Y
O	U	M	E	E	T
M	E	T	O	M	M
O	R	R	O	W	X

The six columns are now written out in the order as defined by the keyword:

HOOMOEEMWLREOOEWUERLAMTRHYTMX

In irregular case the empty spaces are not filled with random letters.

For example

C	I	P	H	E	R
1	4	5	3	2	6
H	E	L	L	O	H
O	W	A	R	E	Y

O	**U**	**M**	**E**	**E**	**T**
M	**E**	**T**	**O**	**M**	**M**
O	**R**	**R**	**O**	**W**	

The six columns are now written out in the order as defined by the keyword:

HOOMOEEMWLREOOEWUERLAMTRHYTM

Double Columnar Transposition: To make the message even more difficult to discover, the ciphertext produced by this algorithm and run it through the encryption again using a different keyword. This transposes the columns twice and makes the message extremely difficult to decipher.

After first encryption again same process for next encryption

C	**I**	**P**	**H**	**E**	**R**
1	**4**	**5**	**3**	**2**	**6**
H	**O**	**O**	**M**	**O**	**E**
W	**U**	**E**	**R**	**L**	**A**
M	**T**	**R**	**L**	**R**	**E**
O	**O**	**O**	**E**	**E**	**M**
W	**H**	**Y**	**T**	**M**	**X**

The six columns are now written out in the order as defined by the keyword:

HWMOWOLREMMRLETOUTOHOEROYEAEMX

Solved Problems

Solved problem

Self-Test (Multiple Choice Questions)

Self-test question

1.45 **Hashing – concept:** A hash, also called a digest, is a number generated from a string of text and is a unique string of data. The process of creating a hash is called hashing. The resulting hash is unique to the original message. A hash function takes a random block of data and generates a fixed-sized bit string, the hash value. If data is changed (due to any accidental or intentional) the hash value will also change. The data to be

encrypted is often called as message, and the generated hash value is called as message digest or simply digest.
Hash function is one of the most commonly used encryption method.A hash function *H* accepts a random-length block of data M as input and generates a fixed-size hash value*h*,

***h* = *H* (*M*)**

A good hash function generates a hash code that is evenly distributed and apparently random by applying function to a large set of inputs.The principal object of a hash function is data integrity. Achange (either accidental or intentional) to any bit or bits in data M results, with high probability, in a change to the hash code.

A cryptographic hash function is an algorithm for which it is computationally infeasible (since no attack is considerably more efficient than brute force) to find:

- A data object that represents to a pre-specified hash result (one-way property)
- Two data objects that represent to the same hash result (collision-free property).
- Output does not reveal information of input

Because of these properties, hash functions are often used to determine whether or not data has changed.

Figure X shows the overall working of a cryptographic hash function. The input is padded out to an integer multiple of some fixed length and the padding contains the value of the length of the original message in bits. The length field is a security measure to increase the difficulty for an attacker to generate another message with the same hash value.

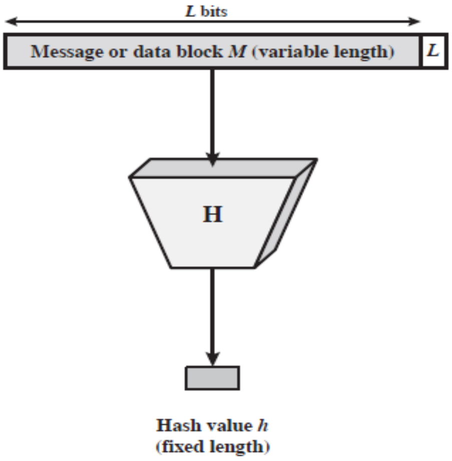


Figure 8.2: Black Diagram of Cryptographic Hash Function; h = H (M)

Self-Test (Multiple Choice Questions)

Self-test question

1.46 **Firewalls (Introduction):**A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. Firewalls prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet (i.e., the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

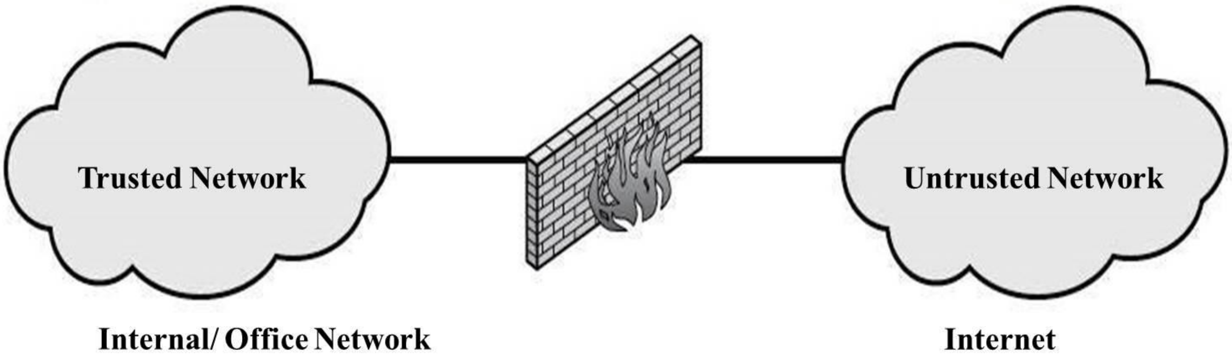


Figure 8.3 Firewall

- **Why Firewall:**The firewall is needed because it can be an effective means for protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.

  Information systems in various, government agencies and other organizationshave undergone a continuous evolution.The following are important developments:
  - Centralized data processing system, with a central mainframe supporting anumber of directly connected terminals
  - Local area networks (LANs) interconnecting PCs and terminals to each otherand the mainframe
  - Premises network, consisting of a number of LANs, interconnecting PCs,servers, and perhaps a mainframe or two
  - Enterprise-wide network, consisting of multiple, geographically distributedpremises networks interconnected by a private wide area network (WAN)
  - Internet connectivity, in which the various premises networks all hook into theInternet and may or may not also be connected by a private WAN

- Features and Characteristics of Firewall:
  - Monitor all traffic to and from your PC and prevent trusted applications from being “Hi-Jacked” to steal local or network-accessible files.
  - The Process Monitor adds an important layer of defence to conventional firewall protection by identifying process-level behaviour characteristics of intrusion techniques and malware activity.

- Control which applications can access the Internet, and whether to permit/block every application with each usage or make permissions permanent. Specific IPs and/or Websites can be blocked or allowed access.
- Define application specific or global packet filtering rules that can be applied to incoming, outgoing or bi-directional traffic.
- View or create advanced firewall reports sorted by Web, Mail, or System access attempts spanning Hours, Days, Weeks, or customized time periods.
- **Different protection levels based on the location of the computer**

  When your PC connects to a network, the firewall applies a security level in accordance with the type of network. If you want to change the security level assigned initially, you can do this at any time through the firewall settings.
- **Protection of wireless networks (Wi-Fi)**

  This blocks intrusion attempts launched through wireless networks (Wi-Fi). When an intruder attempts to access, a pop-up warning is displayed that allows you to immediately block the attack.
- **Access to the network and the Internet**

  It specifies which programs installed on your computer can access the network or the Internet.
- **Protection against intruders**

  It prevents hacker attacks that try to access your computer to carry out certain actions.
- **Blocks**

  The firewall can block the access of the programs that you specify should not be able to access the local network or the Internet. It also blocks access from other computers that try to connect to programs installed on your computer.
- **Definition of rules**

  This defines rules that you can use to specify which connections you want to allow and the ports and zones through which the connection can be established.

Characteristics (Design Goals)

Some Characteristics of firewall are

The definition of a firewall depends on how and to what extent a firewall is used in a network. In general, the design goals for afirewall are:

- All traffic from inside to outside, and vice versa, must passthrough the firewall.
- Only authorized traffic, defined by the local security policy, willbe allowed to pass the firewall. A firewall usually has a goodlogging facility and notification abilities.
- The firewall itself is immune to penetration. This implies thatuse of a secure operating system, keep patching the systemregularly, secure administrative access, etc.

To control access and enforce the security policy firewalls usesfour general techniques.

- **Service control:** Determines the types of internet services thatcan be accessed. The firewall may filter traffic on the basis ofIP address and TCP port number.
- **Direct control:** Determines the direction in which particularservices requests may be initiated and allowed to go throughthe firewall.
- **User control:** Controls access to a service according to whichuser is attempting to access it. This is usually applied to insideusers. For incoming traffic from outside of the firewall, someprotocols are required such as IPSec.
- **Behaviour control:** Controls how particular services are used. For example, it may enable external access to only a portion of the information on a local Web server.

- **Limitations:**

  It should be noted that firewalls only can protect certain kind ofattacks from the internet. They have their limitations as follows.

  - The firewall cannot protect against attacks that bypass the firewall. For example, dial-out connection will not go through the firewall.
  - The firewall does not protect against internal threats.
  - The firewall cannot protect against the transfer of virus-infected programs of files. It would be impractical for the firewall to scan all incoming files, e-mails, etc.
  - An improperly secured wireless LAN can be accessed from outside the organization. An internal firewall that separates portions of an enterprise network cannot protect against wireless communications between local systems on different sides of the internal firewall.
  - A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally.

- **Types of Firewall:** A firewall plays an important role on any network as it provides a protective barrier against most types of attack coming from the outside world. Firewalls can be either hardware or software. The ideal firewall configuration consists of both.

  Hardware: Hardware firewalls can be very effective with fewer configurations, and they can protect every single machine on a local network. Most hardware firewalls are having at least of four network ports which connect other computers.

Hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination. This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.

In many cases, hardware firewalls are excellent solutions for organizations that want a single security protection that protects multiple systems. Since they are specialized devices, hardware firewalls can be expensive, complicated, difficult to upgrade, and tricky to configure.

Software: Software firewalls are more perfect for individual users or small businesses that have dial-up or broadband Internet connections than hardware firewall. Instead of using a custom and often expensive hardware firewall, a software firewall can be installed on an individual's PC, notebook, or workgroup server.

Like any other software,software firewalls can be installed on your computer and are easy to customize. It allowsto control over its function and protection features. A software firewall protects computer from outside attempts to control or gain access to the computer, and, depending on the choice of software firewall, it also provides protection against the most common Trojan programs or e-mail worms. Many software firewalls have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on the systems. Moreover, software firewalls also incorporates privacy controls, web filtering and much more. The drawbackof software firewalls is that they only protects the computer on which they are installed, not a network, so each computer will need to have a software firewall installed on it.

Packet Filter: Work at the network level of the OSI model. Each packet is compared to a set of criteria before it is forwarded.Packet filtering firewalls is low cost and low impact on network performance.

A packet filtering firewall implements a set of rules to each incoming and outgoing IP packet and then decides to forward or discard the packet. The packet filter firewall is typically designed to filter packets traveling in both directions (inside and outside internal network). Filtering rules are based on the information contained in a network packet:

- Source IP address: The IP address of the system that transmitted the IP packet
- (e.g., 192.168.7.1)
- Destination IP address: The IP address of the system the IP where the packet is trying toreach (e.g., 192.168.7.92)
- Source and destination transport-level address: The transport-level (e.g., TCPor UDP) port number, which defines applications such as SNMP or TELNET
- IP protocol field: Defines the transport protocol

- Interface: For a firewall with three or more ports, which interface of the firewallthe packet came from or which interface of the firewall the packet is heading for

The packet filter is typically established as a list of instructions based on matches to the fields in the TCP/IP header. If there is a match to one of the rules, that rule is invoked to decide whether to forward or discard the packet. If there is no match to any rule, then a default action is taken. There are two default policies:

- Default = discard: That which is not expressly permitted is prohibited.
- Default = forward: That which is not expressly prohibited is permitted.

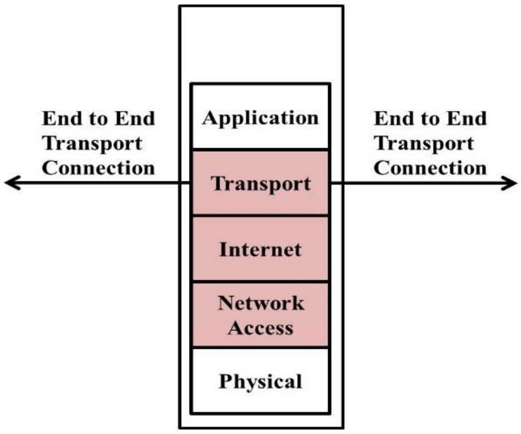

End to End Transport Connection
Application
Transport
Internet
Network Access
Physical
End to End Transport Connection

Figure 8.4: Packet Filtering Firewall

Disadvantages of packet filter firewalls:

- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions.
- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited.
- Most packet filter firewalls do not support advanced user authentication schemes.
- Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing. Spoofing attacks are generally employed by intruders to bypass the security controls implemented in a firewall platform.
- Due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations.

Some attacks that can be implemented on packet filtering and their counter measures are asbelow:

- **IP Address Spoofing**: In this intruder transmits packets from the external network with a source IP address field including an address of an internal host. The attacker expects that the use of a spoofed address will permit for the breach of systems that deploy simple source address security, where packets from the particular reliable internal hosts are accepted. The counter measure is to discard such packets those have an inside source address and if that packet comes from an external interface.

- **Source Routing Attacks:** In this source station states the route, that a packet would take as it go across the Internet, attacker hopes that this will bypass security measures that do not analyze the source routing information. The counter measure is to discard all packets that will use this option.
- **Tiny Fragment Attacks:** In this intruder uses the IP fragmentation technique to create very small fragments and force the TCP header information into a separate packet fragment. This attack is constructed to avoid filtering rules that are depending on TCP header information. Usually, a packet filter is making filtering decision on the first fragment of a packet. All following fragments of that packet are filtered out merely on the basis that they are part of the packet whose first fragment was rejected. The attacker expects that the filtering firewall will examines only first fragment and that the remaining fragments will pass through. A tiny fragment attack can be overcome by applying a rule that first fragment of a packet must hold a predefined minimum amount of the transport header. If the first fragment is discarded, the filter can remember the packet and will discard all subsequent fragments.

Proxy Server: A firewall proxy server is an application that acts as mediator between tow end systems. Firewall proxy server works at the application layer of the firewall, where the both ends of a connection are bound to complete the session via the proxy. This is accomplished by creating and running a process on the firewall that displays a service as if it is running on the end host.

Working of Proxy Servers: A firewall proxy server basically turns a two-party session into a four-party session, with the internal process matching the two real hosts. Since they function at the application layer, proxy servers are also known as application layer firewalls. A proxy service must run for every type of Internet application the firewall should support a Simple Mail Transport Protocol (SMTP) proxy for e-mail, an HTTP proxy for Web services and so on. Mostly proxy servers are always one way arrangements running from the internal network to the outside network. In different words, if an internal user desires to open a Web site on the Internet, the packets making up that request are handled by the HTTP server prior being forwarded to the Web site. Packets returned from the Web site in turn are processed by the HTTP server before being forwarded back to the internal user host.

Since firewall proxy servers integrate all activity for an application into a single specific server, it presents the perfect opportunity to execute a variety of useful functions. By running the application right on the firewall,shows the opportunity to examinethe packets for much more than just source / destination addresses and port numbers. Therefore almost all modern firewalls include some form of proxy-server architecture.

For example, incoming packets are headed to a server set up strictly to disburse information (FTP server) and can be checked to see if they are containing any write commands (Like PUT command). In this way, the proxy server might allow only the connections that contain read commands.

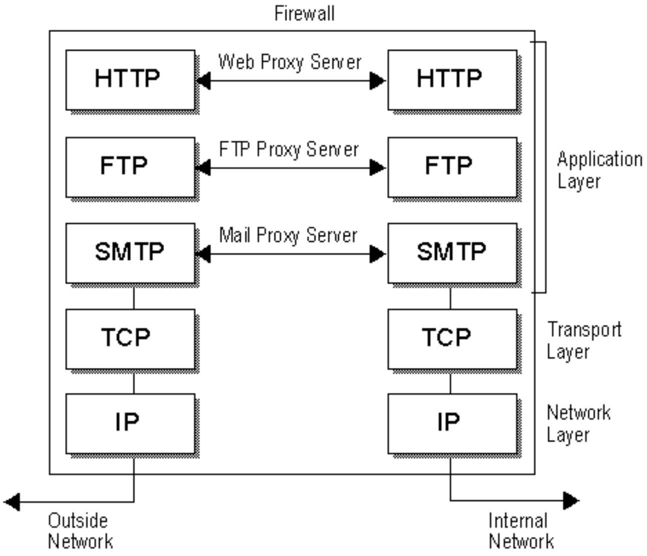


Figure 8.5: Proxy Server Firewall

Hybrid Firewall: Hybrid Firewalls combine the components of the other types of firewalls, i.e. the elements of packet filtering and proxy services, or of packet filtering and circuit level gateways. A hybrid firewall system might actually contain two or more separate firewall devices: with each as a separate firewall system, although they are connected, they work together. For example, a hybrid firewall system may contain a packet filtering firewall which is set up to monitor all appropriate requests and then transfer the requests to a proxy server, which in turn, requests services from a Web server inside the organization’s networks. An additional benefit to the hybrid firewall method is that it supports an organization to manage a security upgrade without completely changing its current firewalls.

Application Level Gateways: Work at the application level of the OSI model. Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific. Gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through.

An application level gateway, also called an application proxy, works as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denyingall other features.

Application-level gateways tend to be more secure than packet filters. Ratherthan trying to deal with the numerous possible combinations that are to be allowedand forbidden at the TCP and IP level, the application-level gateway need onlyscrutinize a few allowable applications. In addition, it is easy to log and audit allincoming traffic at the application level.

A prime disadvantage of this type of gateway is the additional processingoverhead on each connection. In effect, there are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examineand forward all traffic in both directions.

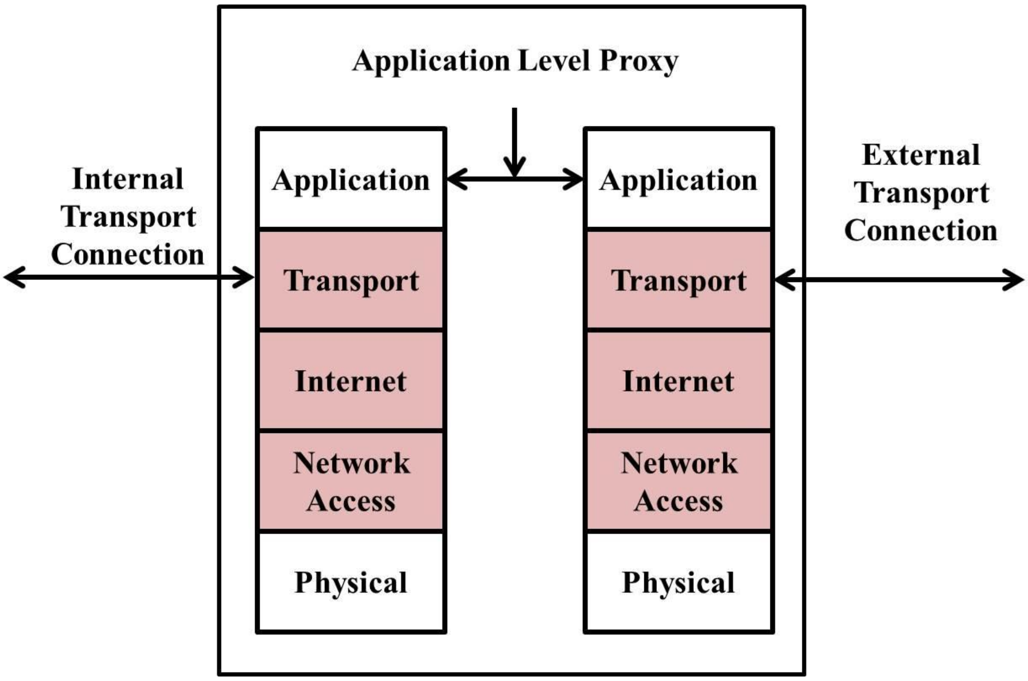


Figure 8.6: Application Level Gateway Firewall

Circuit Level Gateway: The circuit-level gateway or circuit-level proxy firewall can be a standalone system or it can be a dedicated function, performed by an application-level gateway for specific applications. Like application gateway, circuit-level gateways do not permit an end-to-end TCP connection.The gateway sets up two TCP connections, one with itself and TCP user on an inner host and one between itself and witha TCP user onan outside host. When the two connections areset up, the gateway typically transmits TCP segments from one connection to the other without checking thecontents. The security function includes of deciding which connections should beallowed.

A normal use of circuit-level gateways is a condition in which the system administrator relies on the internal users.The gateway can be configured to support application level or proxy service on incoming connections and circuit-level functions foroutgoing connections. In this configuration, the gateway can acquire the processingoverhead of checking incoming application data for prohibited functions but doesnot acquire that overhead on outgoing data.

An example of a circuitlevel gateway application is the SOCKS package.

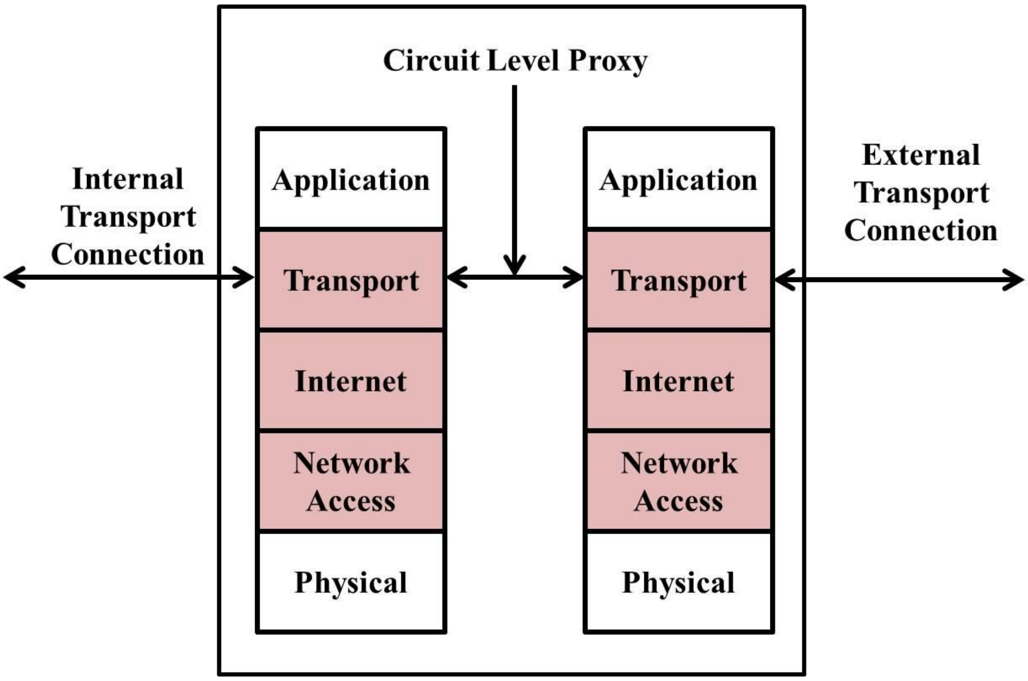


Figure 8.7: Circuit Level Gateway Firewall

Solved problem

Self-Test (Multiple Choice Questions)

Self-test question

1.47 **Virtual Private Network:** A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The VPN uses "virtual" connections routed through the Internet from the business's private network to the remote site or employee. By using a VPN, businesses ensure security -- anyone intercepting the encrypted data can't read it.

A virtual private network (VPN) is the expansion of a private network that includes links that are across shared or public networks like the Internet. A VPN allows data transmission between two computers within a shared or public internetwork in a way that compete with the properties of a point-to-point private link. To configure and create a virtual private network is known as virtual private networking.

To compete with a point-to-point link, data is encapsulated, or wrapped, with a header that gives routing information permitting it to navigate the shared or public internetwork to reach its destination. The data being sent is encrypted for confidentiality. Packets those are captured on a shared or public network are useless without the encryption keys. The section of the connection in which the private data is encapsulated is known as the tunnel. The section of the connection in which the private data is encrypted is known as the virtual private network (VPN) connection.

A VPN connection across the Internet is similar to a wide area network (WAN) link between the sites. It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

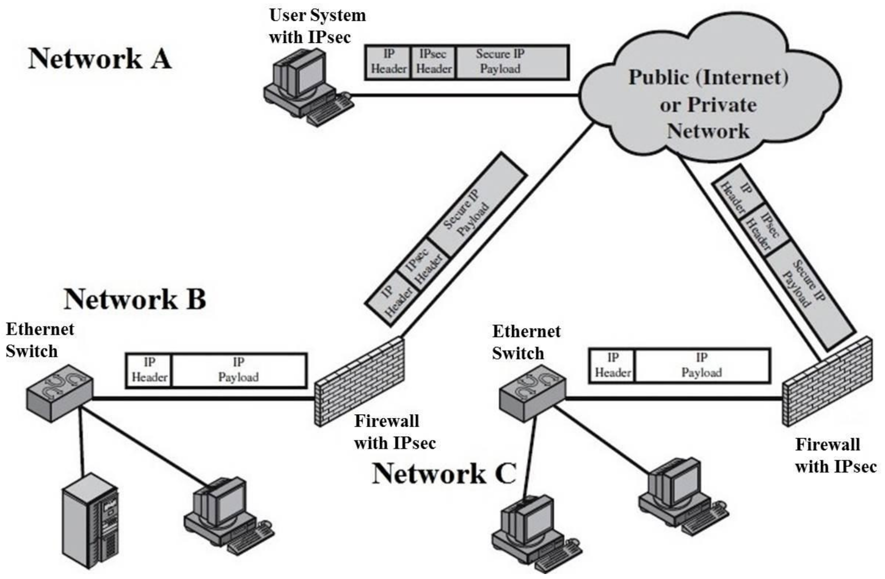


Figure 8.8: Virtual Private Network

VPNs allow employees to securely access their company's intranet while traveling outside the office and also allow users working at home or on the road to connect in a secure fashion to connect company’s remote corporate server via internet. VPN technology also allows a corporation to connect to branch offices or to other companies over a public network (such as the Internet), while maintaining secure communications. From the user’s perspective, the VPN connection is a point-to-point connection between the user’s computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

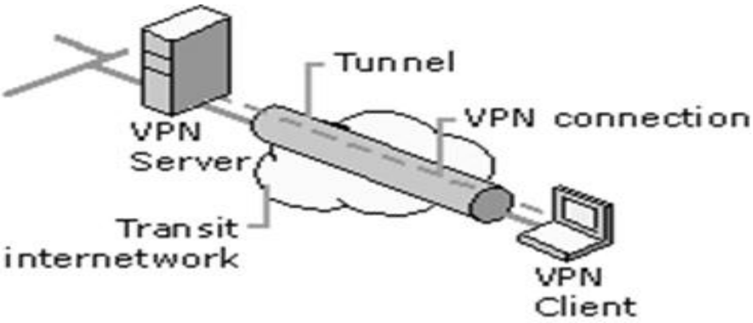


Figure 8.9: VPN Tunnel

It is the most common way to connect computers between multiple offices was by using a leased line. Though leased lines are reliable and secure, the leases are expensive, with costs rising as the distance between offices increases.

Overall, the secure connection across the internetwork appears to the user as a private network communication in spite of the fact that the communication is over a public internetwork, hence known as virtual private network.

Section text

Solved Problems

Solved problem

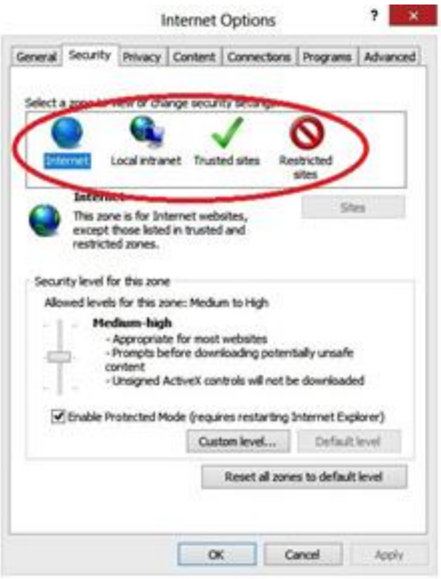
Self-Test (Multiple Choice Questions)

Self-test question

1.48 Security topologies: Topologies are created by separating networks into security zones which provides both a multi-layereddefence strategy and different levels of adequate security with the purpose of each specific zone.

Topologies are divided as below:

- Security Zones
- DMZ
- Internet



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Allowed levels for this zone: Medium to High

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

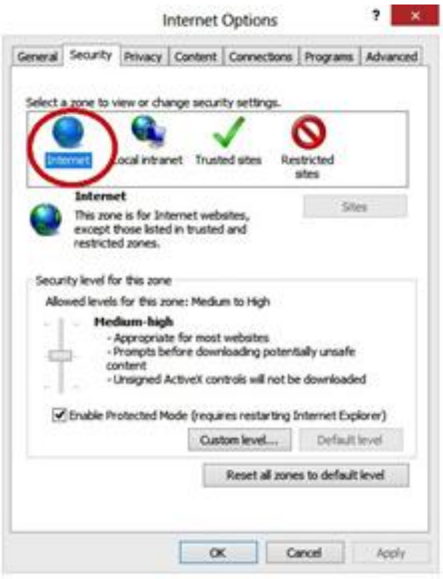
☑ Enable Protected Mode (requires restarting Internet Explorer)

Figure 8.10: Security Zones

- Intranet
- VLAN

Security Zones:

One of the many dangers of the Internet is that serious threats can propagate quickly. The rapid adoption of Internet-based technologies has brought with it a number of security challenges, such as the risk of downloading infected or dangerous code from malicious web sites.



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Allowed levels for this zone: Medium to High

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

Figure 8.11: Internet Zone

Microsoft introduced a concept called “Security Zones” with Internet Explorer 4. Within Internet Explorer’s Security Zones, web sites are categorized into one of five zones: **Internet**, **Local Intranet**, **Trusted Sites**, **Restricted Sites**, and **Local Machine**. Each zone is responsible for a different type of content. Each zone can be configured with a unique security level: **High**, **Medium**, **Medium-Low**, **Low** or **Custom**. The number of possible configurations presents an option for securing every type of web page, whether it is on your PC, on your intranet, or on the Internet.

Security Zones are configured using the Internet applet in the Control Panel. This dialog box can also be visited through Internet Explorer by selecting **Tools** then **Internet Options**. The Security tab will display Security Zone information.

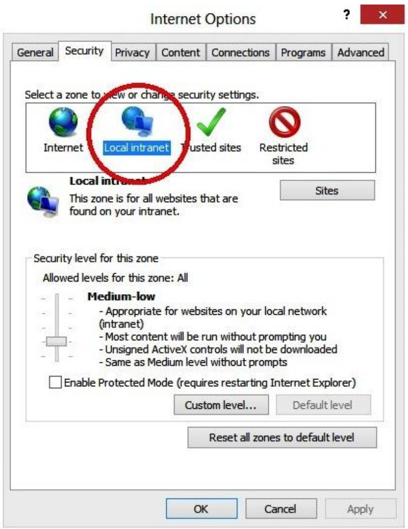
Internet Zone: By default, this zone contains anything that is not on your computer or an intranet, or assigned to any other zone. The default security level for the Internet zone is Medium. You can change your privacy settings for the Internet zone on the Privacy tab in Internet Options. This is the zone on which you cannot add sites.

The default security setting of the Internet zone is medium. This setting protects from at most web sites. Still it is possible for a malicious web site to access sensitive data from the system, or to cause harm to the system or network. For example, a setting of medium could make Internet Explorer vulnerable to frame spoofing or site spoofing.

One other important thing to keep in mind is that always new vulnerabilities are being discovered. But as long as the possibility remains, it is needed to take steps for protection.Even if we don't download software from a web site, elements of a web page on that site may consist of executable code which is downloaded behind the scenes, and run on the computer. This poses enough of a security risk that you'll want to control what sites remain in the Internet zone, and what level of security you use for this zone.

Local Intranet Zone: This zone is for all websites those are found on Local Intranet. This zone contains local domain names, as well as the addresses of any proxy server exceptions that may have configured. In order for security in this zone to be effective, the Local Intranet zone should be set up in conjunction with a proxy server and a firewall. All sites in the Local Intranet zone should be inside the firewall, and all proxy servers should be configured to deny external DNS name resolution for this zone. Configuring this zone properly requires detailed knowledge of your network configuration, including proxy servers and firewalls. Even when properly configured, however, some versions of Internet Explorer may inadvertently place Internet sites into the Local Intranet zone. By default, both the Internet zone and the Local Intranet zone are set to medium security, so ordinarily this isn't a problem.

To add a site to the Local Intranet zone, first click the sites button and then click the advanced button, enter the URL and click Add. You can also specify whether or not you want to use HTTPS (Hypertext Transfer Protocol Secure) for server verification.



Internet Options

Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

Security level for this zone

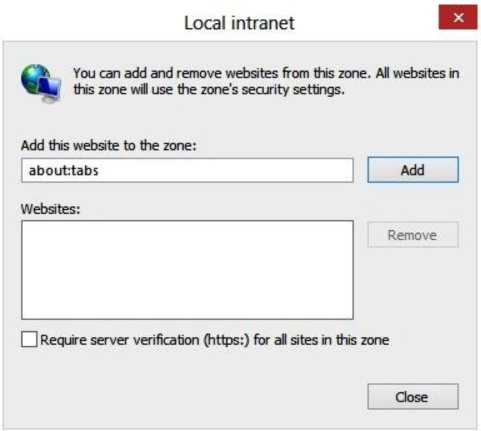
Allowed levels for this zone: All

Medium-low

- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

□ Enable Protected Mode (requires restarting Internet Explorer)

Figure 8.12: Local Intranet Zone



Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

about:tabs

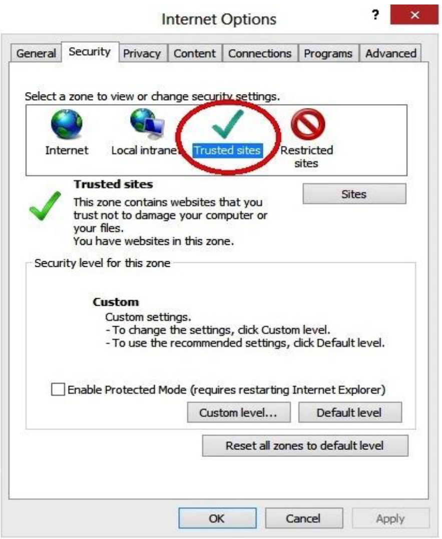
Websites:

□ Require server verification (https:) for all sites in this zone

Figure 8.13: Add remove websites from Local Intranet Zone

Trusted Sites Zone: As the name implies, the Trusted Sites zone is intended for use with those sites which you trust not to damage your system or steal your information. By default, it is set to low security. There isn't a lot more than can be said about the Trusted Sites zone, except to say that you should use this zone sparingly and carefully. You might even consider applying a customized level of security, as opposed to using the default low security. Even if you completely trust the content and code on a web site, it is still a good idea to protect yourself by disabling features you may not need or use. Trusted web sites can always add content that is stored on other, non-trusted sites. In addition, it is entirely possible that an unintentional mistake in the coding of an applet or the writing of scripts could produce undesirable effects. Certainly this won't be as destructive as a malicious script or a rogue applet, but it could produce several annoyances, including a system crash.

To add a site to the Trusted Sites zone, click the Sites button and add the desired site. Like sites in the Local Intranet zone, you can also specify that HTTPS be used for these sites.



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.

You have websites in this zone.

Security level for this zone

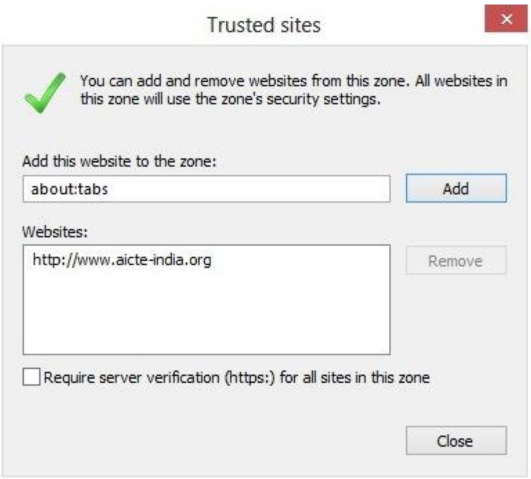
Custom

Custom settings.

- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

Figure 8.14: Trusted Sites Zone



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

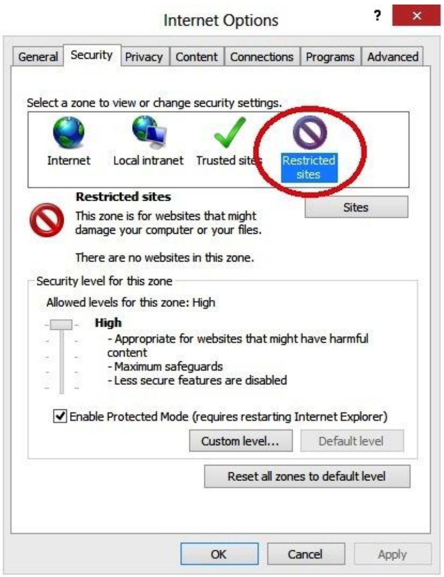
Add this website to the zone: about:tabs

Websites: http://www.aicte-india.org

□ Require server verification (https:) for all sites in this zone

Figure 8.15: Add remove websites from Trusted Sites Zone

Restricted Sites Zone: Restricted Sites zone provides a mechanism for containing web sites that may cause damage to or steal information from your system or your network. Obviously the best protection would be to simply not visit the sites, but you may find some exceptions. There may be web sites out there who plain text content you wish to view without the concern of silent executable code being delivered to your computer.Like the Local Intranet and Trusted Sites zones, you can add sites to the Restricted Site zone by clicking Sites, entering an URL and clicking add. Unlike the other two zones, you cannot specify whether or not restricted sites are required to use HTTPS.



Select a zone to view or change security settings.

Restricted sites

This zone is for websites that might damage your computer or your files.

There are no websites in this zone.

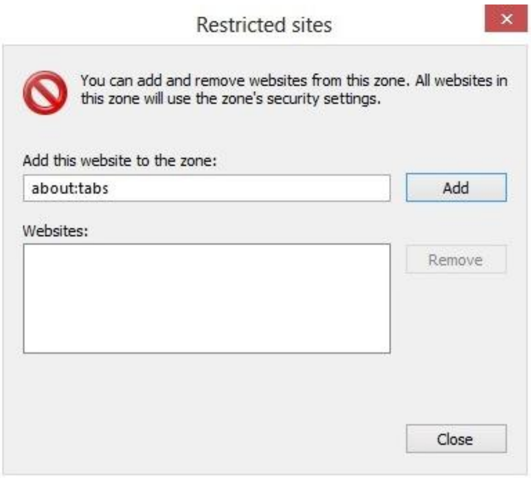
Security level for this zone

Allowed levels for this zone: High

High
- Appropriate for websites that might have harmful content
- Maximum safeguards
- Less secure features are disabled

☑ Enable Protected Mode (requires restarting Internet Explorer)

Figure 8.16: Restricted Sites Zone



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone: about:tabs

Websites:

Figure 8.17: Add remove websites from Restricted Sites Zone

DMZ: In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could be served to the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ host's security, the Web pages might be corrupted but no other company information would be exposed.

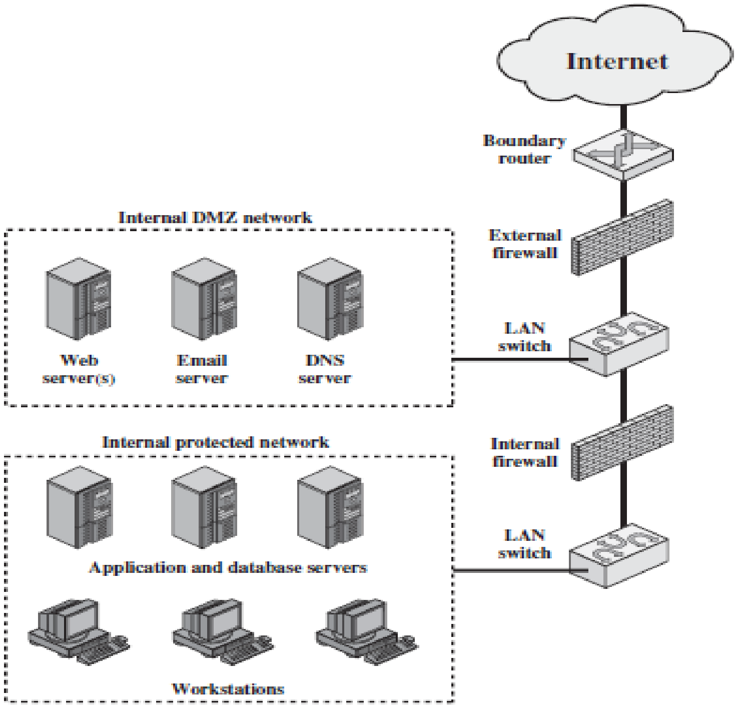


Figure 8.18: DMZ

Internet: It is the worldwide network of computers which is accessible to anyone. Internet is a huge global system which connects computer networks across the world together. Many of private, public, academics, business, and government networks across the world connect with each other over the internet and share great amount of information, resources and services. Internet is used to access web pages, send e-mails, listen to songs or watch movies online. It holds a wide range of information.

To connect to the net internet uses the standard Internet protocol suite (TCP/IP). It has various information resources and services, like different web pages of the World Wide Web (WWW), games, movies, songs, pictures, e-mail, social networking, etc. It has even introduced new services like Voice over Internet Protocol (VoIP) and Internet Protocol Television (IPTV). The Internet is currently being used by billions of people worldwide.

The Internet holds information from all streams; traditional, such as newspaper, book and other print publishing; and modern such as blogging and web feeds. It also enables new type of human communications through, instant messaging, e-mail, Internet forums, and social networking. It has got so much popularity that in fact almost all types of business communication as well as personal are done online through e-mail, instant messaging and social networking.

Intranet: An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network. Typically, an intranet includes connections through one or more gateway computers to the outside Internet. The main purpose of an intranet is to share company information and computing resources among employees. An intranet can also be used to facilitate working in groups and for teleconferences.

An intranet uses TCP/IP, HTTP, and other Internet protocols and in general looks like a private version of the Internet. With tunnelling, companies can send private messages through the public network, using the public network with special encryption/decryption and other security safeguards to connect one part of their intranet to another.

Typically, larger enterprises allow users within their intranet to access the public Internet through firewall servers that have the ability to screen messages in both directions so that company security is maintained. When, part of an intranet is made accessible to customers, partners, suppliers, or others outside the company, that part becomes part of an extranet.

VLAN: A VLAN acts like an ordinary LAN, but connected devices don't have to be physically connected to the same segment. A virtual local area network (VLAN) is a logical set of computers, servers and network devices that seems to be on the same network (LAN) in spite of their physical distance. A VLAN permits a network of computers and users to interconnect in a virtual environment as if they are in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to acquire scalability, security and ease of network management and can rapidly adapt to change in network needs and repositioning of workstations and server nodes.

Advanced switches allow the functionality and implementation of VLANs. The objective of implementing a VLAN is to upgrade and enhance the performance of a network and apply suitable security features.

A VLAN permits several networks to function virtually as an LAN. One of the most advantages of VLAN is that it eliminates latency in the network, which saves network resources and increases network efficiency. Moreover, VLANs are created to provide segmentation and help in issues such as security, network management and scalability. Traffic patterns may also be controlled simply by using VLANs.

Advantages of VLANs are:

- Allowing network administrators to apply additional security to network communication
- Making expansion and relocation of a network or a network device easier
- Providing flexibility because administrators are able to configure in a centralized environment while the devices might be located in different geographical locations
- Decreasing the latency and traffic load on the network and the network devices, offering increased performance

Disadvantages of VLANs are:

- High risk of virus issues because one infected system may spread a virus through the whole logical network
- Equipment limitations in very large networks because additional routers might be needed to control the workload
- More effective at controlling latency than a WAN but less efficient than a LAN

Self-Test (Multiple Choice Questions)

Self-test question

1.49 Intrusion Detection: Intrusion detection systems (IDS)

Introduction: When a hacker tries to enter illegally into your system to access information, services and resources of the system, it is known as intrusion, and an intrusion detection system is a system, which detects such intrusions.Unauthorized intrusion into a computer system or network is one of the most serious threats to computer security.

Intrusion detection systems are developed to detect an intrusion and give warning so that defensive action can be taken to prevent or minimize damage. To prevent intrusion an intrusion password management is very necessary, and preventing unauthorized users from having access to the passwords of authorized users.

Examples of intrusion:

- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and pass- words
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Dialling into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password
- Using an unattended, logged-in workstation without permission

Intrusion detection systems (IDS): An Intrusion detection system is like a burglar alarm. An Intrusion detection system keeps watch on the activities going on around it and tries to identify unwanted activity. Intrusion detection systems are divided into two categories, depending on how they monitor activity:

- **Host Based IDS:**A host-based Intrusion detection system examines activity on an individual system, such as a mail server, web server, or individual PC. It is concerned only with an individual system and usually has no visibility into the activity on the network or systems around it.
- **Network Based IDS:**A network-based Intrusion detection system examines activity on the network itself. It has visibility only into the traffic crossing the network link it is monitoring and typically has no idea of what is happening on individual systems.

Whether or not it is network- or host-based, an intrusion detection system will typically consist of several specialized components working together as illustrated in **Figure 4.16.** These components are often logical and software-based rather than physical and will vary slightly from vendor to vendor and product to product. Typically, an Intrusion detection system is having following logical components:

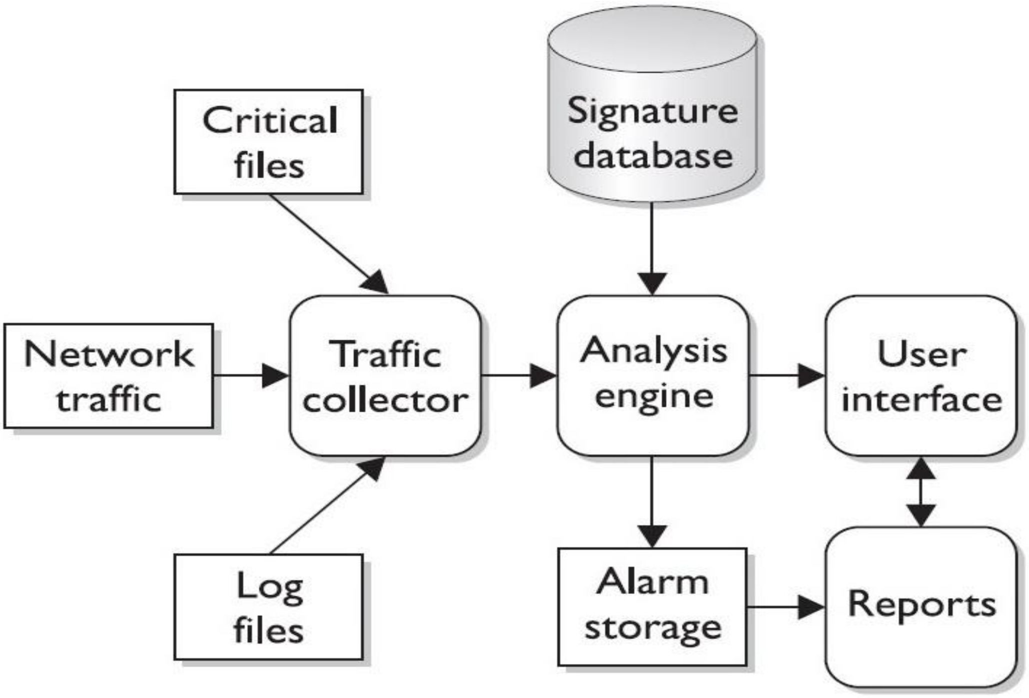


Figure 8.19: Logical depiction of IDS components

- **Traffic collector**: This component collects activity/events for the IDS to examine. On host-based IDS, this could be log files, audit logs, or traffic coming to or leaving a specific system. On network-based IDS, this is typically a mechanism for copying traffic off the network link—basically functioning as a sniffer.
- **Analysis engine:** This component examines the collected network traffic and compares it to known patterns of suspicious or malicious activity stored in the signature database. The analysis engine is the “brains” of the IDS.

- **Signature database:** The signature database is a collection of patterns and definitions of known suspicious or malicious activity.
- **User interface and reporting:** This is the component that interfaces with the human element, providing alerts when appropriate and giving the user a means to interact with and operate the IDS.

Host-Based Intrusion Detection Systems: Host-based are designed to examine activity on a specific host. A host-based IDS (HIDS) is a system that examines log files, audit trails, and network traffic coming in to or leaving a specific host. Host-based IDSs can operate in real time, looking for activity as it occurs, or batch mode, looking for activity on a periodic basis. Host-based systems uses local system resources to operate, i.e. host-based IDS will use some of the memory and CPU cycles of the system. Most host-based intrusion detection systems focus on the log files or audit trails generated by the local operating system. On UNIX systems, the examined logs are those created by syslog such as messages, kernel logs, and error logs. On Windows systems, the examined logs are typically the three event logs: Application, System, and Security. Within the log files, the intrusion detection system is looking for certain activities that typify hostile actions or misuse such as:

- Logins at odd hours
- Login authentication failures
- Adding new user accounts
- Modification or access of critical system files
- Modification or removal of binary files (executable)
- Starting or stopping processes
- Privilege escalation
- Use of certain programs

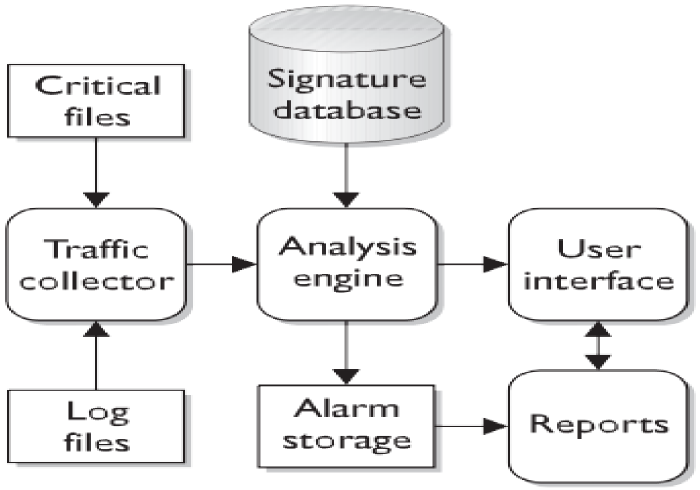


Figure 8.20: Components of HIDS

Traffic collector on a host-based IDS pulls in the information the other components, such as the analysis engine, need to examine. For most host-based systems, the traffic collector pulls data from information the local system has already generated, such as error messages, log files, and system files. The traffic collector is responsible for reading those files, selecting which items are of interest, and forwarding them to the analysis engine. On some host-based systems, the traffic collector will also examine specific attributes of critical files such as file size, date modified, or checksum.

The analysis engine is perhaps the most important component of the IDS, as it must decide what activity is "okay" and what activity is "bad." The analysis engine is a sophisticated decision and pattern matching mechanism—it looks at the information given to it by the traffic collector and tries to match it against known patterns of activity stored in the signature database. If the activity matches a known pattern, the analysis engine can react, usually by issuing an alert or alarm. An analysis engine may also be capable of remembering how the activity it is looking at right now compares to traffic it has already seen or may see in the near future so that it can match more complicated, multistep malicious activity patterns. An analysis engine must also be capable of examining traffic patterns as quickly as possible, as the longer it takes to match a malicious pattern, the less time the IDS or human operator has to react to malicious traffic. Most IDS vendors will build a "decision tree" into their analysis engines to expedite pattern matching.

The signature database is a collection of predefined activity patterns that have already been identified and categorized—activity patterns that typically indicate suspicious or malicious activity. When the analysis engine has a traffic pattern to examine, it will compare that pattern to the appropriate signatures in the database. The signature database can contain anywhere from a few to a few thousand signatures, depending on the vendor, type of IDS, space available on the system to store signatures, etc.

The user interface is the visible component of the intrusion detection systemthis isthe part that humans interact with. The user interface varies widely depending on the product and vendor and could be anything from a detailed graphical interface to a simple command line. Regardless of the type and complexity, the interface is provided to allow the user to interact with the system: changing parameters, receiving alarms, tuning sig- natures and response patterns, etc.

Advantages of Host-Based IDSs:

- They can be very operating system–specific and have more detailed signatures.
- They can reduce false positive rates.
- They can examine data after it has been decrypted.
- They can be very application specific.
- They can determine whether or not an alarm may impact that specificsystem.

Disadvantages of Host-Based IDSs:

- The IDS must have a process on every system you want to watch.

- The IDS can have a high cost of ownership and maintenance.
- The IDS uses local system resources.
- The IDS has a much focused view and cannot relate to activity around it.
- The IDS, if logged locally, could be compromised or disabled.

Network based IDS: A network-based IDS, as the name suggests, focuses on network traffic the bits and bytes traveling along the cables and wires that interconnect the systems. A network IDS (NIDS) must examine the network traffic as it passes by and be able to analyze traffic according to protocol, type, amount, source, destination, content, traffic already seen, etc. This analysis must happen quickly, and the IDS must be able to handle traffic at whatever speed the network operates on to be effective. Network-based IDSs are typically deployed so that they can monitor traffic in and out of an organization's major links: connections to the Internet, remote offices, partners, etc. Like host-based systems, network-based IDSs look for certain activities that characterize adverse activities or movements such as:

- Denial of service attacks
- Port scans or sweeps
- Malicious content in the data payload of a packet or packets
- Vulnerability scanning
- Trojans, viruses, or worms
- Tunnelling
- Brute-force attacks

Figure 8.21shows the logical layout of a networkbased IDS.

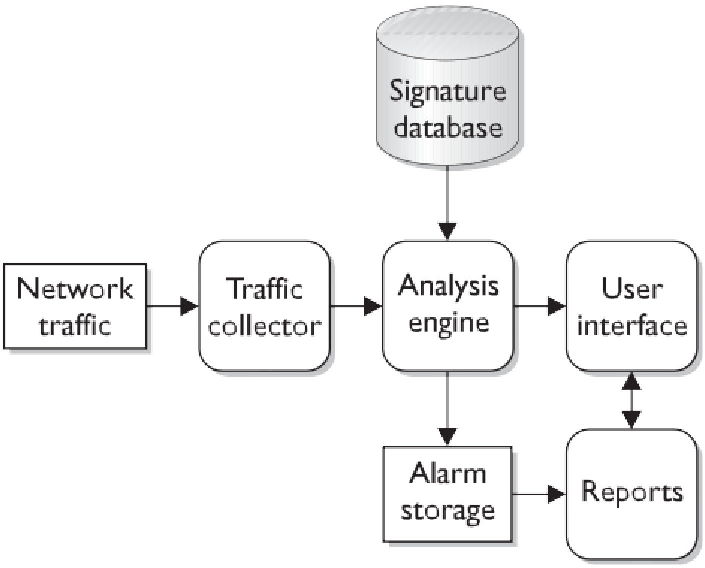


Figure 8.21:Components of NIDS

Logical components of a network-based intrusion detection system are similar like those of the host-based system.

Major Components of NIDS are:

- Traffic Collector
- Analysis Engine
- Reports
- User Interface

Traffic Collector: It is specially designed to extract traffic fromthe network. Traffic collector usually works in the same way as network traffic snifferit simply reads every packet that passes through or within the network to which it is connected to. The traffic collector logically attaches itself to a network interface card (NIC) and directs the NIC to receive every packet it can. A NIC that receives and sort out every packet in spite of the packet's origin and destination is said to be in "promiscuous" mode.

Analysis Engine: It has the similar function as it has in hostbased IDS, with some significant differences. The network analysis engine is capable of collecting packets and examining them individually and, ifessential, reassembling them into an entire traffic session. The patterns and signatures being matched are morecomplex than hostbased signatures, thus the analysis engine should be capable of remembering what traffic has passed before the current traffic is being analysed so that it can be able to determine whether or not that traffic fits into a larger pattern of malicious activity.Also, the networkbased analysis engine must be able to sustain with the flow of traffic on the network, recreating network sessions and matching patterns in real time.

Signature Database: It is usually much larger than host based signature database. Whileanalysing network patterns, the IDS must be able to identifythe traffic targeted at various applications and operating systems and also the traffic from a wide variety of threats (like worms, assessment tools, attack tools, etc.). Some of the signatures themselves may be quite large, since the IDS has to look at network traffic appearing in a specific order over a period of time in order to match a specific malicious pattern.

User Interface: The working functionality of user interface is similar like host based IDS.

Advantages of Network-Based IDS

There are several advantages of networkbased IDS:

- It takes fewer systems to provide IDS coverage
- Deployment, maintenance, and upgrade costs are usually lower

- A network-based IDS has visibility into all network traffic and can correlate attacks among multiple systems

Disadvantages of a Network Based IDS

There are several disadvantages of network based IDS:

- It is ineffective when traffic is encrypted
- It cannot see traffic that does not cross it
- It must be able to handle high volumes of traffic

Self-Test (Multiple Choice Questions)

Self-test question

1.50 Summary
1.51 Exercise (short answer questions)
1.52 References
1.52.1 Books
1.52.2 Wikipedia
1.52.3 MOOCs
1.52.4 YouTube Videos
1.52.5 OER