THE TAMIL NADU

Dr. AMBEDKAR LAW UNIVERSITY

(State University Established by Act No. 43 of 1997)

SCHOOL OF EXCELLENCE IN LAW

'Perungudi Campus', M.G.R. Salai, Perungudi, Chennai - 600 113.

COMPUTER NETWORKS AND NETWORK SECURITY

COURSE MATERIAL

FOR BCA.LL.B

(For the candidates admitted from academic year 2015 - 2016 onwards)

By

K. SHANTHI

Guest Faculty,

Department of Inter-Disciplinary

School of Excellence in Law

The Tamil Nadu Dr. Ambedkar Law University, Chennai

PREFACE

The merging of computers and communications has had a profound influence on the way computer systems are organized. The old model of a single computer serving all of the organization's computational needs has been replaced by one in which a large number of separate but interconnected computers do the job. These systems are called **computer networks.**

Throughout the book we will use the term "computer network" to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information.

The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used. Networks come in many sizes, shapes and forms, as we will see later. They are usually connected together to make larger networks, with the Internet being the most well-known example of a network of networks.

The course material for the subject "Computer Networks and Network Security" is a simple version of the various topics contained in the syllabus. It deals with the fundamental concepts of computer network. This text is intended for a first course in databases at the undergraduate level.

This material describes the concepts as intuitive descriptions, many of which are based on our running example of a university. Important theoretical results are covered, but formal proofs are omitted.

In place of proofs, figures and examples are used to suggest why a result is true. This material is an extract of sufficient information's collected from various texts on computer networks. This material will be a supportive one along with textbooks and other references.

K.SHANTHI
Guest Faculty,
Department of Inter-Disciplinary
School of Excellence in Law
The Tamil Nadu Dr. Ambedkar Law University,
Chennai

COMPUTER NETWORKS AND NETWORK SECURITY

SUBJECT CODE: HD5B/CHD5B

CONTENTS

UNIT – I

INTRODUCTION

1.1 Overview of Computer Networks

1.1.1 Introduction of Computer Networks

Today the world scenario is changing. Data Communication and network have changed the way business and other daily affair works. Now, they rely on computer networks and internetwork. A set of devices often mentioned as nodes connected by media link is called a Network. A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called Communication channels.

Computer network is a telecommunication channel through which we can share our data. It is also called data network. The best example of computer network is Internet. Computer network does not mean a system with control unit and other systems as its slave. It is called a distributed system

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

1. Performance
2. Reliability
3. Scalability

Performance

It can be measured in following ways :

- **Transit time :** It is the time taken to travel a message from one device to another.
- **Response time :** It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are :

1. Efficiency of software
2. Number of users
3. Capability of connected hardware

Reliability

It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

Security

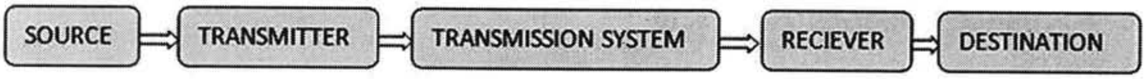
It refers to the protection of data from the unauthorised user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

1.1.2 Properties of Good Network

1. **Interpersonal Communication :** We can communicate with each other efficiently and easily example emails, chat rooms, video conferencing etc.
2. **Resources can be shared :** We can use the resources provided by network such as printers etc.
3. **Sharing files, data :** Authorised users are allowed to share the files on the network.

1.1.3 Basic Communication Model

Communication model is used to exchange data between two parties. For example communication between a computer, server and telephone (through modem).



Source

Data to be transmitted is generated by this device, example: telephones, personal computers etc.

Transmitter

The data generated by the source system are not directly transmitted in the form they are generated. The transmitter transforms and encodes the information in such a form to produce electromagnetic waves or signals.

Transmission System

A transmission system can be a single transmission line or a complex network connecting source and destination.

Receiver

Receiver accepts the signal from the transmission system and converts it to a form which is easily managed by the destination device.

Destination

Destination receives the incoming data from the receiver.

1.1.4 Data Communication

The exchange of data between two devices through a transmission medium is Data Communication. The data is exchanged in the form of 0's and 1's. The transmission medium used is wire cable. For data communication to occur, the communication device must be part of a communication system. Data Communication has two types Local and Remote which are discussed below :

1.1.4.1 Local :

Local communication takes place when the communicating devices are in the same geographical area, same building, face-to-face between individuals etc.

1.1.4.2 Remote :

Remote communication takes place over a distance i.e. the devices are farther. Effectiveness of a Data Communication can be measured through the following features:

1. Delivery : Delivery should be done to the correct destination.
2. Timeliness : Delivery should be on time.
3. Accuracy : Data delivered should be accurate.

1.1.5 Components of Data Communication

1. **Message :** It is the information to be delivered.
2. **Sender :** Sender is the person who is sending the message.
3. **Receiver :** Receiver is the person to him the message is to be delivered.
4. **Medium :** It is the medium through which message is to be sent for example modem.
5. **Protocol :** These are some set of rules which govern data communication.

1.2 Applications

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

1.2.1 Service Provided by the Network for Companies:

- Many organizations have a large number of computers in operation. These computers may be within the same building, campus, city or different cities.
- Even though the computers are located in different locations, the organizations want to keep track of inventories, monitor productivity, do the ordering and billing etc.

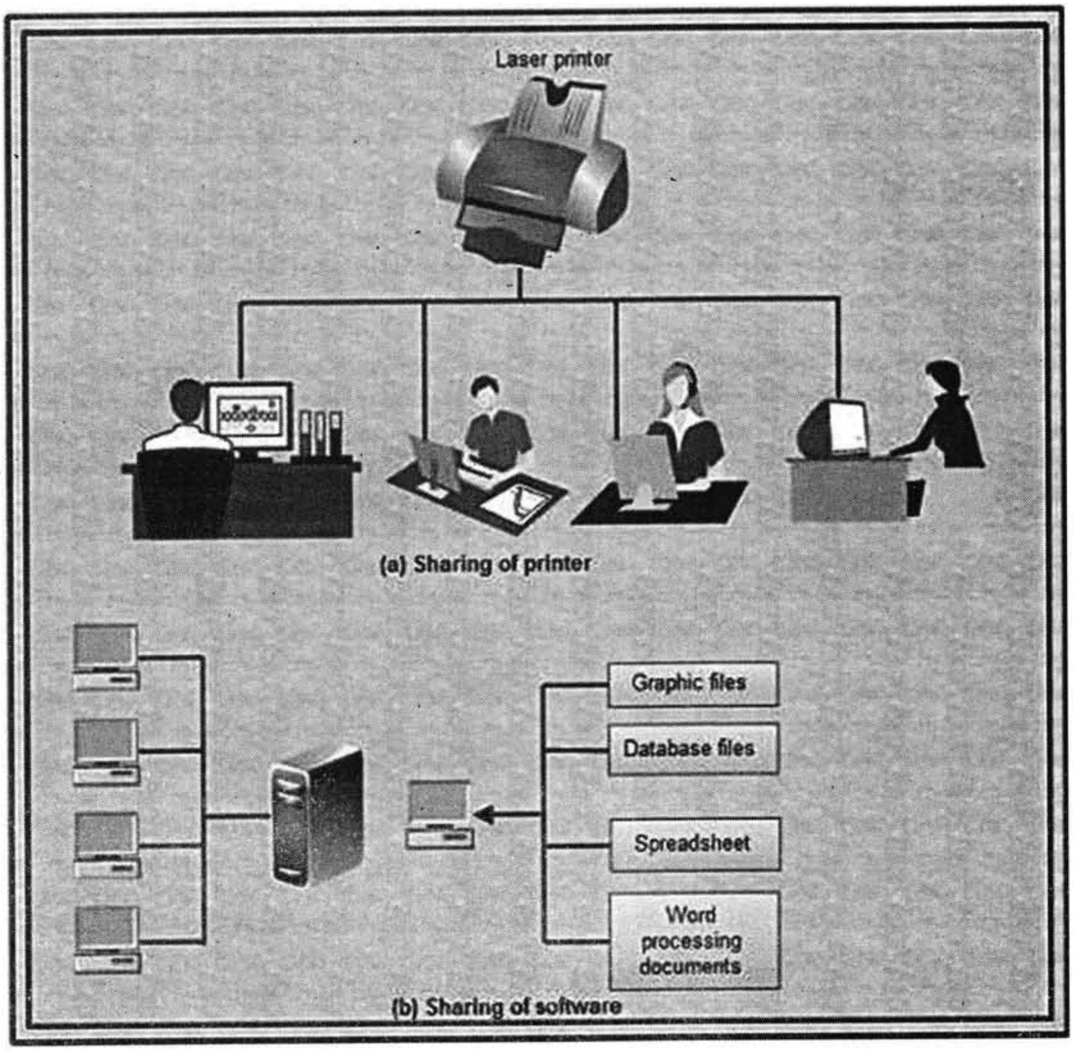
The computer networks are useful to the organizations in the following ways:

1. Resource sharing.
2. For providing high reliability.
3. To save money.
4. It can provide a powerful communication medium.

1. Resource sharing

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

Show in Fig (a) and (b) which shows a printer being shared and different information being shared.



(a) Sharing of printer

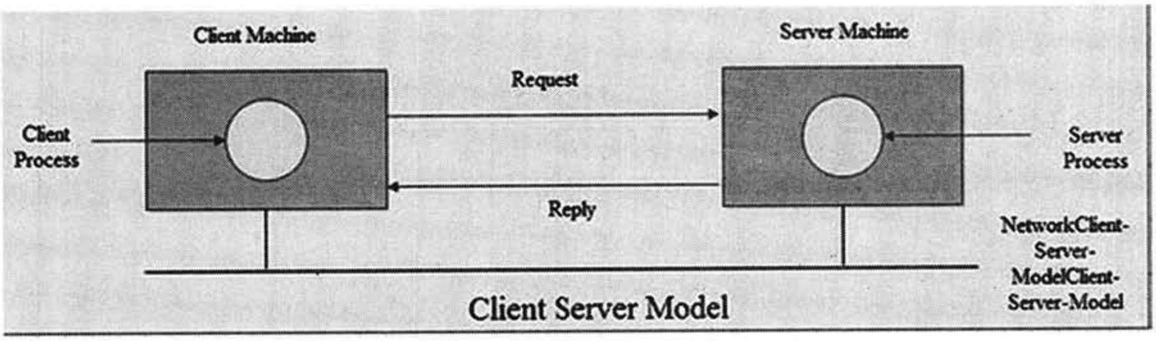
(b) Sharing of software

2. High reliability due to alternative sources of data:

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

3. Money saving:

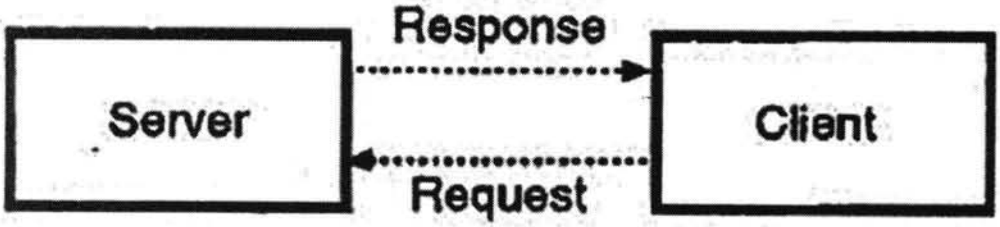
- Computer networking is an important financial aspect for organizations because it saves money.
- Organizations can use separate personal computer one per user instead of using mainframe computer which are expensive.
- The organizations can use the workgroup model (peer to peer) in which all the PCs are networked together and each one can have the access to the other for communicating or sharing purpose.
- The organization, if it wants security for its operation it can go in for the domain model in which there is a server and clients. All the clients can communicate and access data through the server.
- The whole arrangement is called as client -server model.



Client: The individual workstations in the network are called as clients.

Server: The central computer which is more powerful than the clients and which allows the clients to access its software and database is called as the server. Server computers typically are more powerful than client computers or are optimized to function as servers.

Communication in client-server configuration:



Client/server communication

- The client places a request on the server machine when he wants an access to the centralized resources.
- The server responds to this request and sends the signal accordingly to the client.
- The software run at the client computer is called as client program. This software configures the computer to act as a client.
- Similarly the software run on the server computer IS called as server program. It configures a computer to act as a server.

4. Communication medium:

- A computer network provides a powerful communication medium among widely separated employees.
- Using network it is easy for two or more employees, who are separated by geographical locations to work on a report, document or R and D simultaneously i.e. on -line.

Networks for People:

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

The computer networks offer the following services to an individual person:

1. Access to remote information

2. Person to person communication

3. Interactive entertainment.

1. Access to remote information:

Access to remote information involves interaction· between a person and a remote database. Access to remote information comes in many forms like:

(i) Home shopping, paying telephone, electricity bills, e-banking, on line share market etc.

(ii) Newspaper is. On-line and is personalized, digital library consisting of books, magazines, scientific journals etc.

(iii) World wide web which contains information. about the arts, business, cooking, government, health, history, hobbies, recreation, science, sports etc.

2. Person to person communication:

Person to person communication includes:

(i) Electronic-mail (e-mail)

(ii) Real time e-mail i.e. video conferencing allows remote users to communicate with no delay by seeing and hearing each other. Video-conferencing is being used for remote school, getting medical opinion from distant specialists etc.

(iii) Worldwide newsgroups in which one person posts a message and all other subscribers to the newsgroup can read it or give their feedbacks.

3. Interactive entertainment:

Interactive entertainment includes:

(i) Multiperson real-time simulation games.

(ii) Video on demand.

(iii) Participation in live TV programmes likes quiz, contest, discussions etc.

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

1.3 Line Configuration

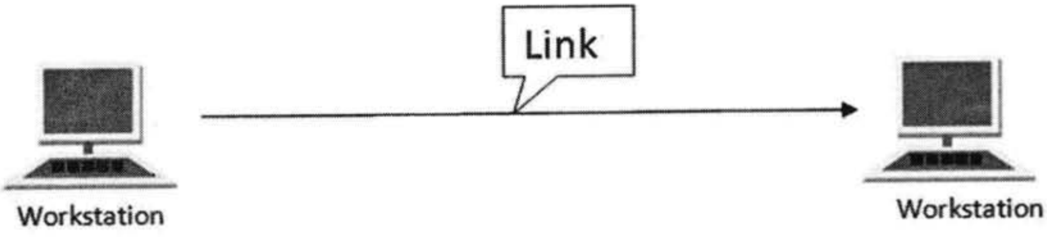
Network is a connection made through connection links between two or more devices. Devices can be a computer, printer or any other device that is capable to send and receive data. There are two ways to connect the devices :

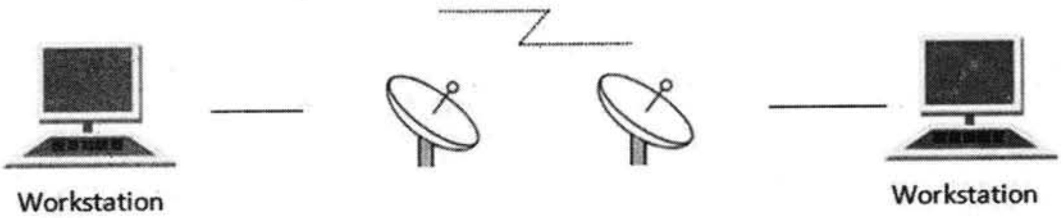
1. Point-to-Point connection
2. Multipoint connection

1.3.1 **Point-To-Point Connection**

It is a protocol which is used as a communication link between two devices. It is simple to establish. The most common example for Point-to-Point connection (PPP) is a computer connected by telephone line. We can connect the two devices by means of a pair of wires or using a microwave or satellite link.

Example: Point-to-Point connection between remote control and Television for changing the channels.



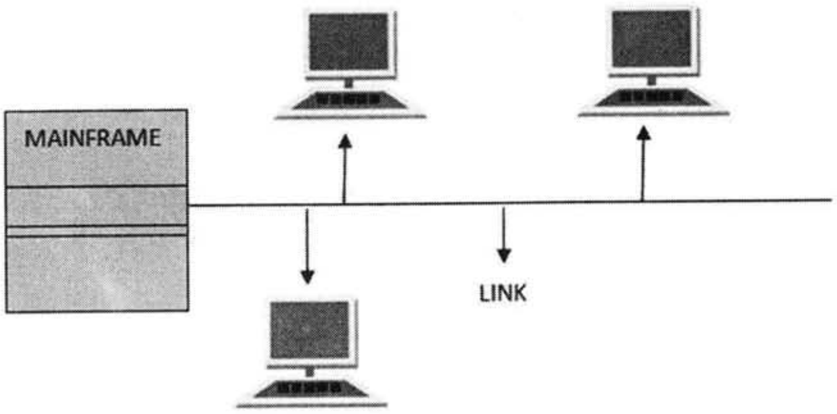


1.3.2 **MultiPoint Connection**

It is also called Multidrop configuration. In this connection two or more devices share a single link.

There are two kinds of Multipoint Connections :

- If the links are used simultaneously between many devices, then it is spatially shared line configuration.
- If user takes turns while using the link, then it is time shared (temporal) line configuration.



1.4 Topology

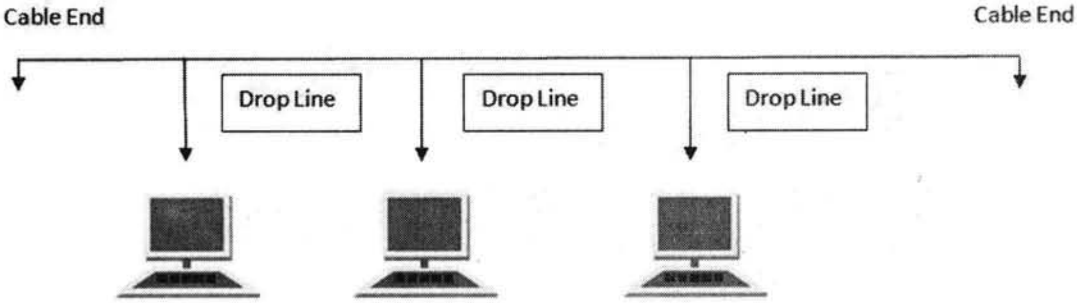
Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

1.4.1 Types of Network Topology

- BUS Topology
- RING Topology
- STAR Topology
- MESH Topology
- TREE Topology
- HYBRID Topology

1.4.2 BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



1.4.2.1 Features of Bus Topology

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

1.4.2.2 Advantages of Bus Topology

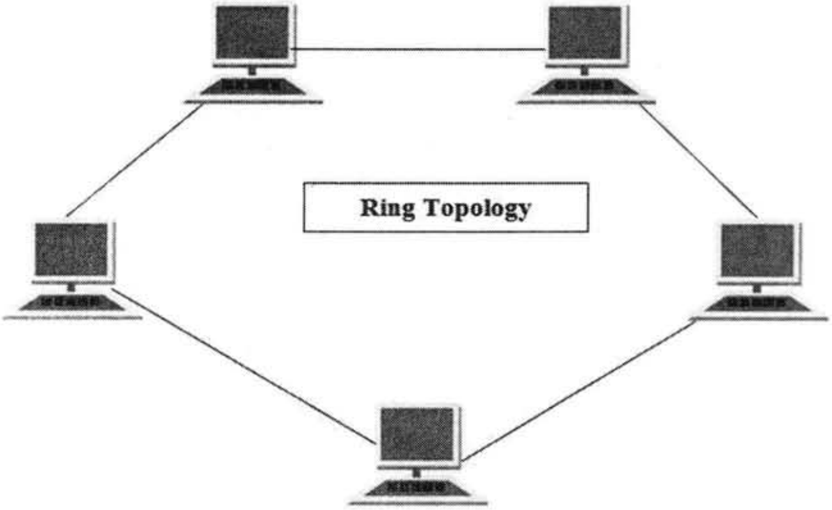
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

1.4.2.3 Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

1.4.3 RING Topology

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. Exactly two neighbours for each device.



1.4.3.1 Features of Ring Topology

1. A number of repeaters are used for 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.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. 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.

1.4.3.2 Advantages of Ring Topology

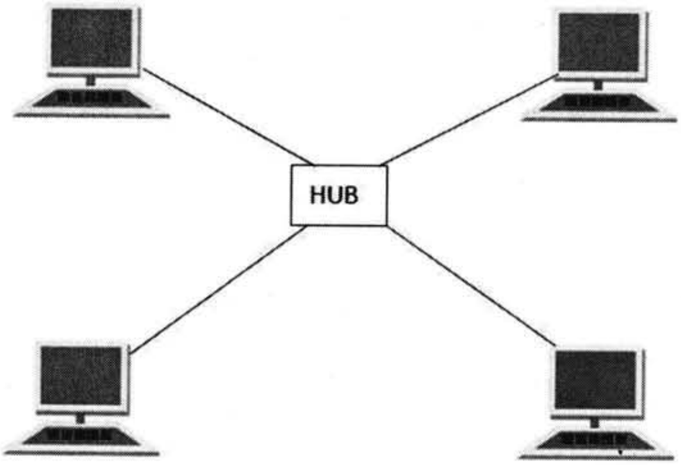
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

1.4.3.3 Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

1.4.4 STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



1.4.4.1 Features of Star Topology

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

1.4.4.2 Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.

3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

1.4.4.3 Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

1.4.5 MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.
There are two techniques to transmit data over the Mesh topology, they are :

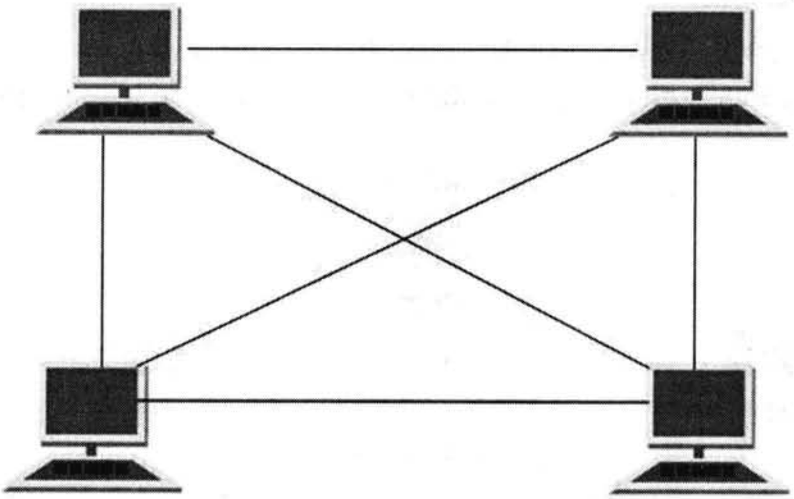
1. Routing
2. Flooding

1.4.5.1 Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

1.4.5.2 Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



1.4.5.3 Types of Mesh Topology

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

1.4.5.4 Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

1.4.5.5 Advantages of Mesh Topology

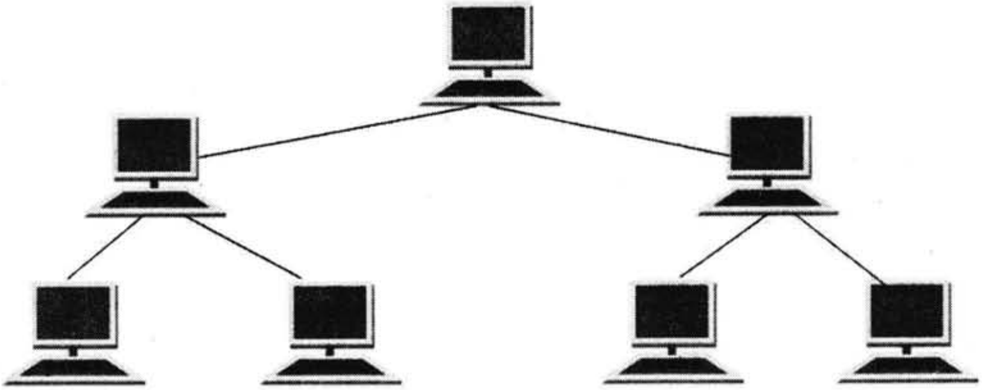
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

1.4.5.6 Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

1.4.6 TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



1.4.6.1 Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

1.4.6.2 Advantages of Tree Topology

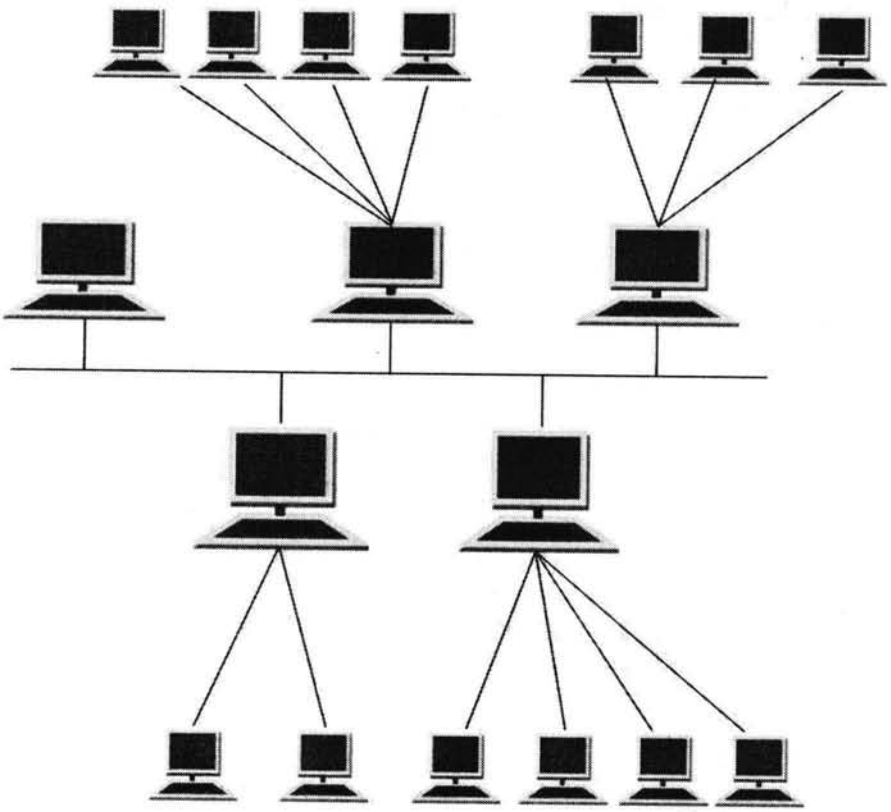
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

1.4.6.3 Disadvantages of Tree Topology

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

1.4.7 HYBRID Topology

It is two different types of topologies which is a mixture of two or more 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).



1.4.7.1 Features of Hybrid Topology

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

1.4.7.2 Advantages of Hybrid Topology

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

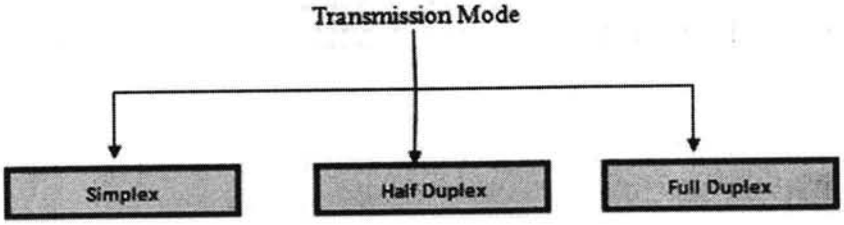
1.4.7.3 Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

1.5 Transmission Modes

Transmission mode means transferring of data between two devices. It is also called communication mode. These modes direct the direction of flow of informatión. There are three types of transmission mode. They are :

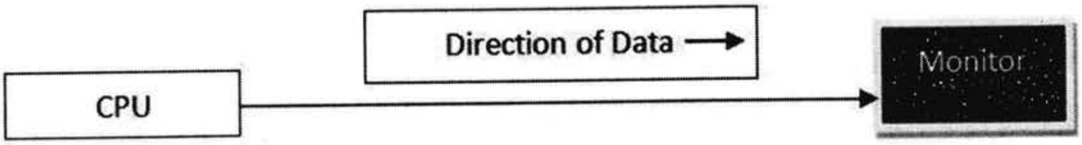
- Simplex Mode
- Half duplex Mode
- Full duplex Mode



1.5.1 SIMPLEX Mode

In this type of transmission mode data can be sent only through one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems.

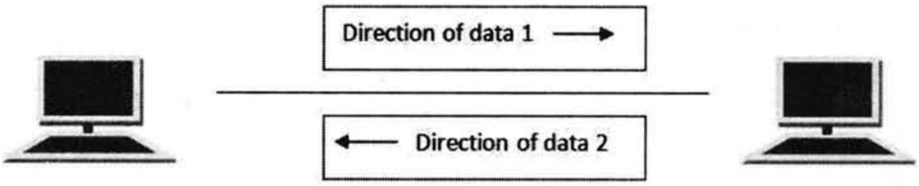
Examples of simplex Mode is loudspeaker, television broadcasting, television and remote, keyboard and monitor etc.



1.5.2 HALF DUPLEX Mode

In half duplex system we can send data in both directions but it is done one at a time that is when the sender is sending the data then at that time we can't send the sender our message. The data is sent in one direction.

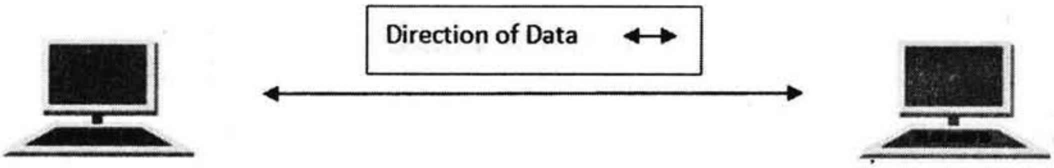
Example of half duplex is a walkie- talkie in which message is sent one at a time and messages are sent in both the directions



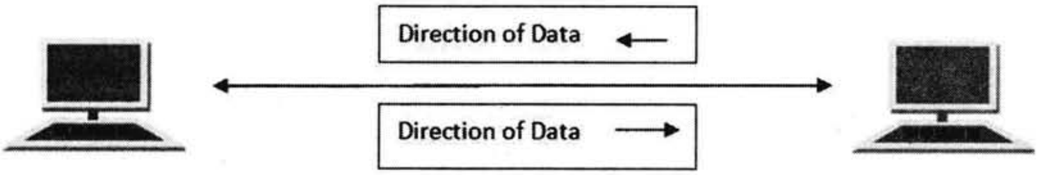
1.5.3 FULL DUPLEX Mode

In full duplex system we can send data in both directions as it is bidirectional. Data can be sent in both directions simultaneously. We can send as well as we receive the data.

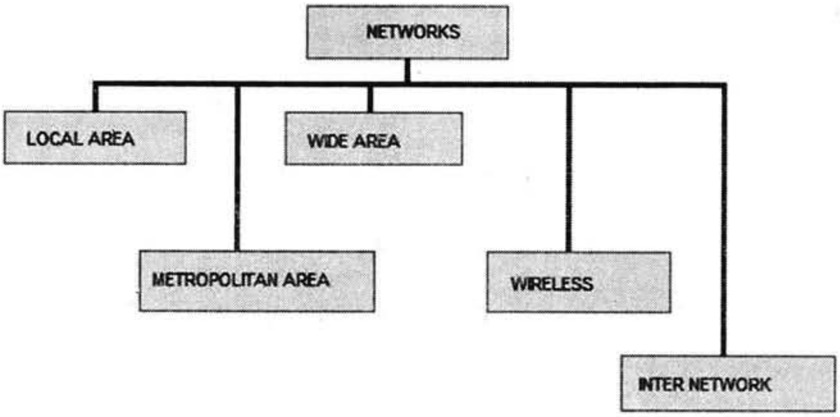
Example of Full Duplex is a Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



In full duplex system there can be two lines one for sending the data and the other for receiving data.



1.6 Categories of Network: LAN, MAN, WAN

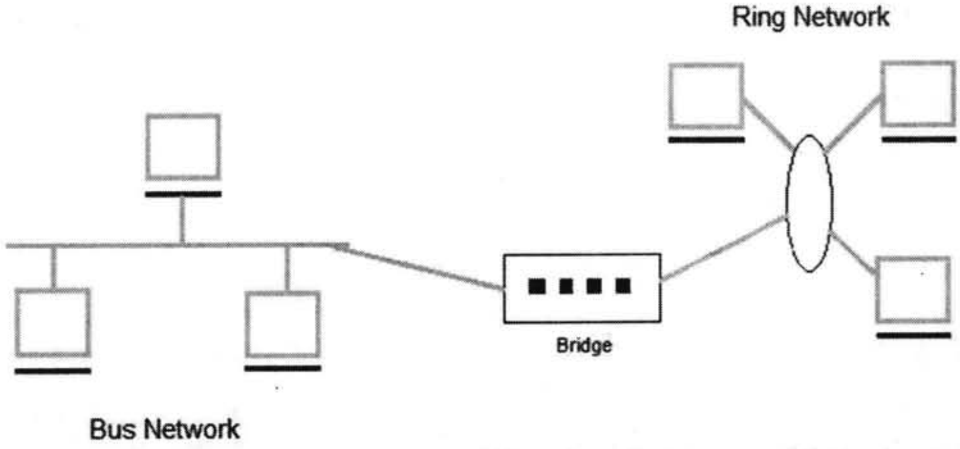


1.6.1 Local Area Network (LAN)

It is also called LAN and designed for small physical areas such as an office, group of buildings or a factory. LANs are used widely as it is easy to design and to troubleshoot. Personal computers and workstations are connected to each other through LANs. We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.

LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building.

LAN networks are also widely used to share resources like printers, shared hard-drive etc.



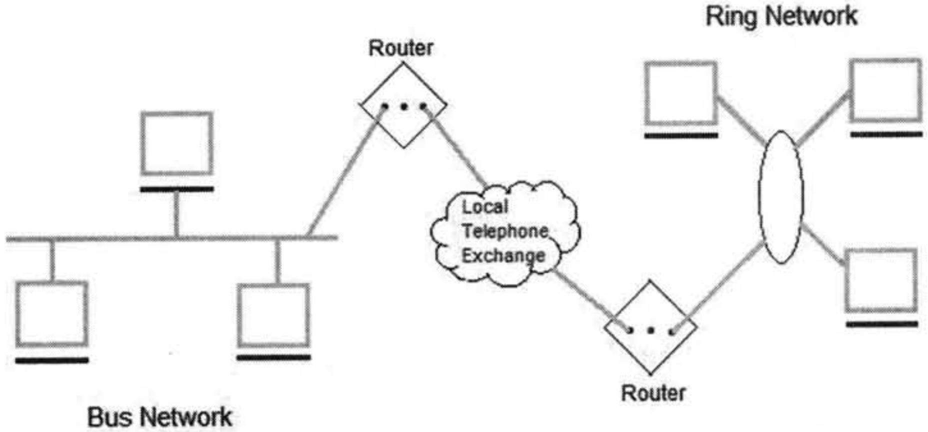
(Different Topologies interconnected in a Local Area Network)

1.6.1.1 Applications of LAN

- One of the computer in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- Connecting Locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc are some common applications of LAN.

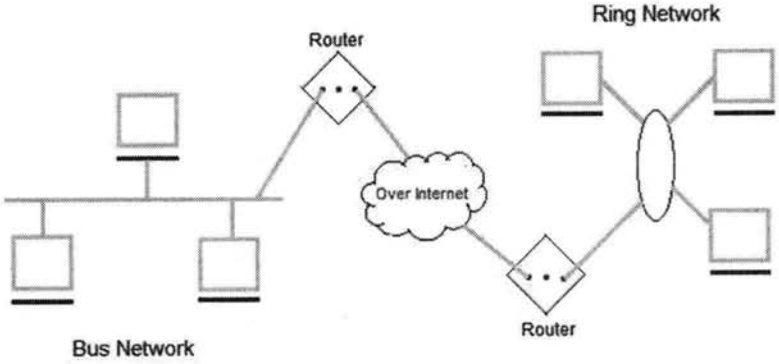
1.6.2 Metropolitan Area Network (MAN)

It is basically a bigger version of LAN. It is also called MAN and uses the similar technology as LAN. It is designed to extend over the entire city. It can be means to connecting a number of LANs into a larger network or it can be a single cable. It is mainly hold and operated by single private company or a public company.



1.6.3 Wide Area Network (WAN)

It is also called WAN. WAN can be private or it can be public leased network. It is used for the network that covers large distance such as cover states of a country. It is not easy to design and maintain. Communication medium used by WAN are PSTN or Satellite links. WAN operates on low data rates.



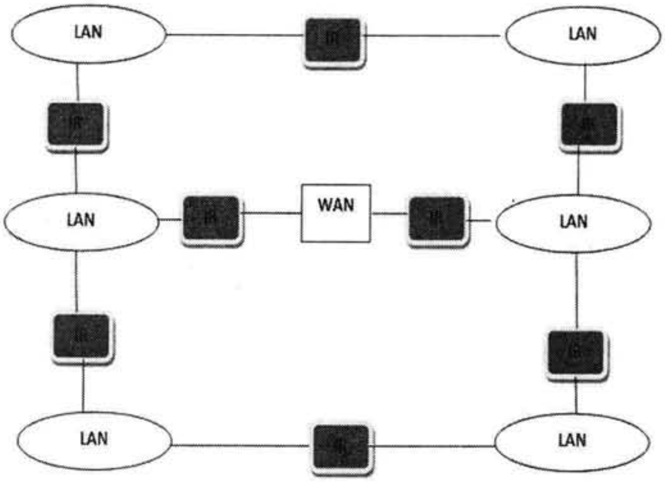
1.6.4 Wireless Network

It is the fastest growing segment of computer. They are becoming very important in our daily life because wind connections are not possible in cars or aeroplane. We can access Internet at any place avoiding wire related troubles.. These can be used also when the telephone systems gets destroyed due to some calamity/disaster. WANs are really important now-a-days.

WiFi Network Connection
Connected
Connected
Connected
Transmitting Connection Signals

1.6.5 Inter Network

When we connect two or more networks then they are called internetwork or internet. We can join two or more individual networks to form an internetwork through devices like routers gateways or bridges.



INTERNETWORK

1.7 Reference Models – OSI and TCP/IP Models

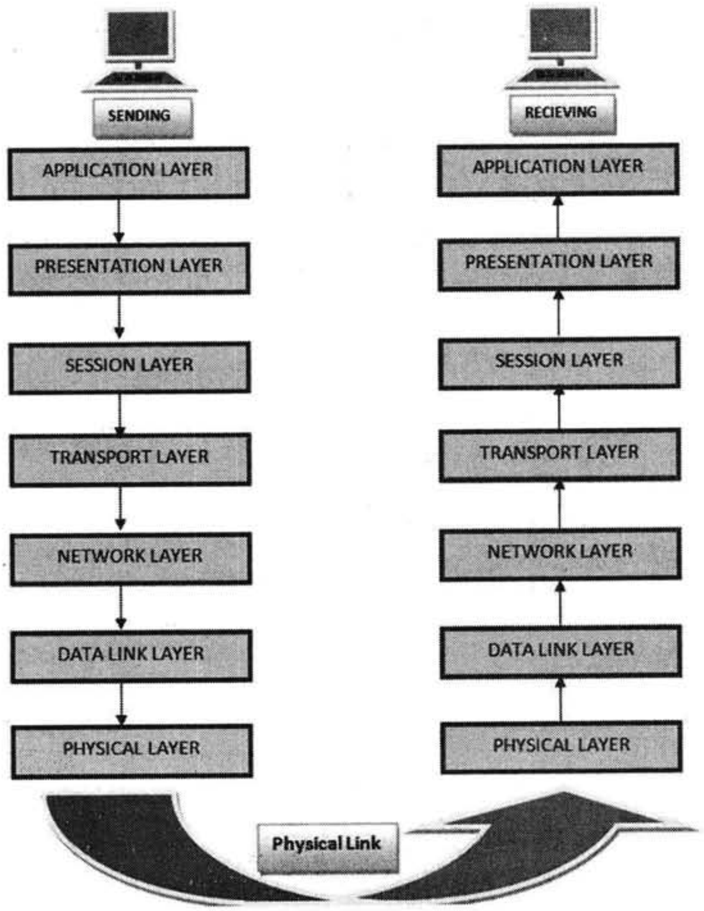
The most important reference models are :

1. OSI reference model.
2. TCP/IP reference model.

1.7.1 ISO-OSI Model:

There are numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other. ISO has developed this. ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system.



1.7.1.1 Feature of OSI Model :

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

1.7.2 Functions of Different Layers :

1.7.2.1 Layer 1: The Physical Layer :

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

1.7.2.2 Layer 2: Data Link Layer :

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

1.7.2.3 Layer 3: The Network Layer :

1. It routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

1.7.2.4 Layer 4: Transport Layer :

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer

3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

1.7.2.5 Layer 5: The Session Layer :

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

1.7.2.6 Layer 6: The Presentation Layer :

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It performs Data compression, Data encryption, Data conversion etc.

1.7.2.7 Layer 7: Application Layer :

1. It is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

1.7.2.8 Merits of OSI reference model:

1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

1.7.2.9 Demerits of OSI reference model:

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

1.7.3 <u>TCP/IP REFERENCE Model</u>

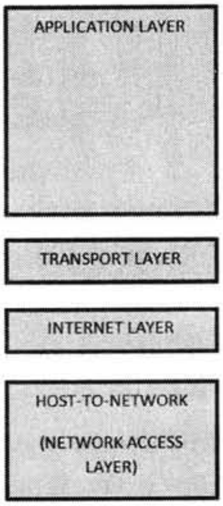
TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. These protocols offer simple naming and addressing schemes.

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.



Description of different TCP/IP protocols

1.7.3.1 Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

1.7.3.2 Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.

1.7.3.3 Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

1.7.3.4 Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.

4. DNS(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

1.7.3.5 Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

1.7.3.6 Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP

	model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers

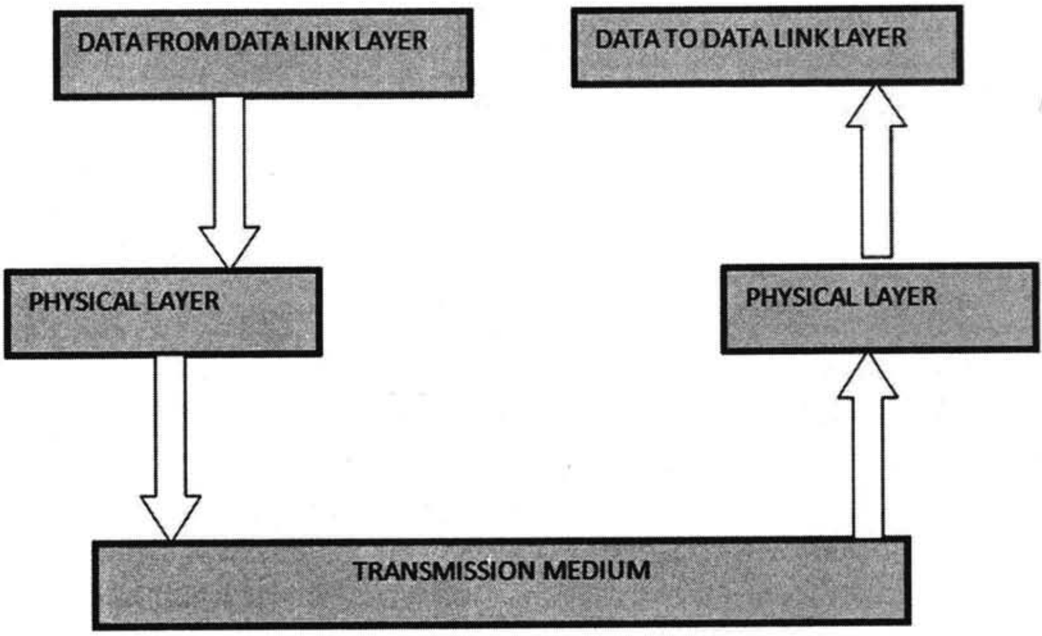
1.8 Physical Layer

Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations. This layer defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.

Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data. The binary data is then sent over the wired or wireless media.

1.8.1 Functions of Physical Layer

1. **Representation of Bits:** Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.
2. **Data Rate:** This layer defines the rate of transmission which is the number of bits per second.
3. **Synchronization:** It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.
4. **Interface:** The physical layer defines the transmission interface between devices and transmission medium.
5. **Line Configuration:** This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.
6. **Topologies:** Devices must be connected using the following topologies: Mesh, Star, Ring and Bus.
7. **Transmission Modes:** Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex, Full Duplex.
8. Deals with baseband and broadband transmission.



1.8.2 Signals

When data is sent over physical medium, it needs to be first converted into electromagnetic signals. Data itself can be analog such as human voice, or digital such as file on the disk. Both analog and digital data can be represented in digital or analog signals.

Digital Signals

Digital signals are discrete in nature and represent sequence of voltage pulses. Digital signals are used within the circuitry of a computer system.

Analog Signals

Analog signals are in continuous wave form in nature and represented by continuous electromagnetic waves.

1.8.3 Transmission Impairment

When signals travel through the medium, they tend to deteriorate. This may have many reasons as given:

Attenuation

For the receiver to interpret the data accurately, the signal must be sufficiently strong. When the signal passes through the medium, it tends to get weaker. As it covers distance, it loses strength.

Dispersion

As signal travels through the media, it tends to spread and overlaps. The amount of dispersion depends upon the frequency used.

Delay distortion

Signals are sent over media with pre-defined speed and frequency. If the signal speed and frequency do not match, there are possibilities that signal reaches destination inarbitrary fashion. In digital media, this is very critical that some bits reach earlier than the previously sent ones.

Noise

Random disturbance or fluctuation in analog or digital signal is said to be Noise in signal, which may distort the actual information being carried. Noise can be characterized in one of the following class:

Thermal Noise

Heat agitates the electronic conductors of a medium which may introduce noise in the media. Up to a certain level, thermal noise is unavoidable.

Intermodulation

When multiple frequencies share a medium, their interference can cause noise in the medium. Intermodulation noise occurs if two different frequencies are sharing a medium and one of them has excessive strength or the component itself is not functioning properly, then the resultant frequency may not be delivered as expected.

Crosstalk

This sort of noise happens when a foreign signal enters into the media. This is because signal in one medium affects the signal of second medium.

Impulse

This noise is introduced because of irregular disturbances such as lightening, electricity, short-circuit, or faulty components. Digital data is mostly affected by this sort of noise.

1.8.4 Channel Capacity

The speed of transmission of information is said to be the channel capacity. We count it as data rate in digital world. It depends on numerous factors such as:

- Bandwidth: The physical limitation of underlying media.
- Error-rate: Incorrect reception of information because of noise.
- Encoding: The number of levels used for signaling.

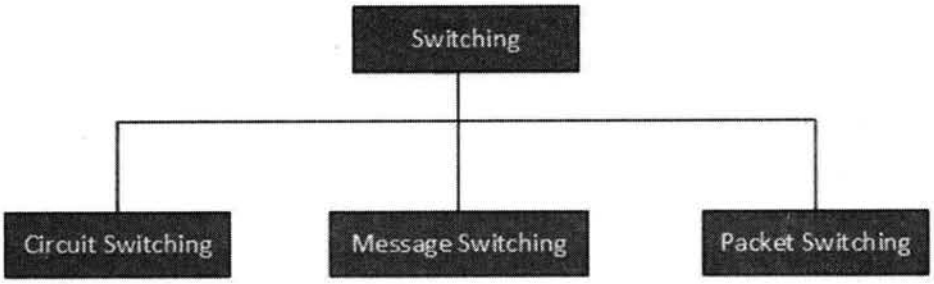
1.8.5 Multiplexing

Multiplexing is a technique to mix and send multiple data streams over a single medium. This technique requires system hardware called multiplexer (MUX) for multiplexing the streams and sending them on a medium, and de-multiplexer (DMUX) which takes information from the medium and distributes to different destinations.

1.8.6 Switching

Switching is a mechanism by which data/information sent from source towards destination which are not directly connected. Networks have interconnecting devices, which receives data from directly connected sources, stores data, analyze it and then forwards to the next interconnecting device closest to the destination.

Switching can be categorized as:



1.9 Theoretical Basis for Data Communication

1.9.1 Fourier Analysis

Fourier showed that a periodic function g(t) can be represented mathematically as an infinite series of sines and cosines:

$$\begin{array}{lll} & 1 & 1 \\ 1 & & \\ c & & \\ g(t) = 2+ & {}^{x}\, a_n \sin(2\ \ nf\, t) + & {}^{x}\, b_n \cos(2\ \ nf\, t) \\ & n{=}1 & n{=}1 \end{array}$$

1. f is the function's fundamental frequency
2. $T = \frac{1}{f}$ is the function's period
3. a_n and b_n are the amplitudes of the nth harmonics

The series representation of g(t) is called its Fourier series expansion.

In communications, we can always represent a data signal using a Fourier series by imagining that the signal repeats the same pattern forever.

Moreover, we can compute the coefficients a_n and b_n :

2 z T g(t)sin(2 nf

a_n = t)dt

T0

2 z T g(t)cos(2 nf

b_n = t)dt

T0

2

c = z T g(t)dt

T 0

For instance, suppose we use voltages (on/off) to represent \1"s and \0"s, and we transmit the bit string \011000010'. The signal would look as follows:

Recall (from calculus):

1. the derivative of sin(x) = cos(x)dx
2. the derivative of cos(x) = -sin(x)dx

2

a_n = z T g(t)sin(2 nf t)dt

T0

z

2 [sin(2 nf t)dt + z

= 3 7 sin(2 nf t)dt]

T 1 6

2 1

= cos(2 nf t)j$_1{}^{3\,;\,7}_{\;;\,6}$

T 2 nf

1 [cos(2 nf 3) cos(2 nf) + cos(2 nf 7) cos(2 nf

= 6)]

nf T

f = 1=8

= ^1_n[cos(n=4)) cos(3 n=4) + cos(6 n=4) cos(7 n=4)]

Similarly,

b_n = ^1_n [sin(3 n=4)) sin(n=4) + sin(7 n=4) sin(6 n=4)]

And

2 z T g(t)dt 2 6 3

c = = 3 = =

T 0 T T 4

Points to note about the Fourier expansion

1. The more terms in the expansion, the more exact our representation becomes.

2. The expression q $a^2{}_n + b^2{}_n$ represents the amplitude or energy of the signal (e.g., the harmonics contribution to the wave).

   In our example, the amplitude consists of a_n and continually gets smaller. (The b_n term is always zero.) Here, as in most cases, the rst harmonics are the most important ones.

The following facts are important:

1. Signals attenuate (strength of signal falls o with distance) during transmission. How much attenuation occurs? The exact amount is dependent on physical properties of the medium.

2. Distortion results because attenuation is non-uniform across the frequency spectrum; some frequencies distort more than others. That is, the signal doesn't distort uniformly. If every component decreased by the same amount, the signal would be weaker, but not distorted, and amplifying the signal would restore it. Because the received signal is distorted, however, amplification simply magnifies the distortion and probably won't help.

3. A transmission medium carries signals lying within in a spectrum or range of frequencies; the absolute width of the spectrum is called the bandwidth of the channel. In other words, most channels completely attenuate (e.g. chop o) frequencies beyond some threshold value.

1.9.2 Factors determining the rate of data transmission

1. The baud rate (also known as the modulation rate) refers to the maximum rate at which the signal changes value (e.g., switches voltages). For example, if \0"s and \1"s were represented as +5V, -5V, respectively, the baud rate would refer to the number of times per second the signal switches as its transmitting a string of alternating 0's and 1's. Note that we can potentially achieve a higher data rate by switching the voltage faster.[1]
2. The encoding method determines the amount of information carried in one baud.

   In our example we encoded only one bit of information (0 or 1). How can we encode 2 bits worth of information in one baud? Use 4 different voltage levels. For example, 0, 1, 2, 3 could be represented as -10, -5, +5 and +10 volts respectively.

Note: baud rate is not the same thing as the data rate. For a given baud rate, we can increase the data rate by changing the encoding method (subject to Nyquist and Shannon limits, of course.)

1.9.3 Voice Grade Lines

What kind of data rate can we achieve using voice-grade phone lines?

The phone system is designed to carry human voices (not data!), and its bandwidth line is limited to about 3 kHz.

Suppose that we have a bit rate of b bits/sec (assume only encode one bit of data per baud).

1. For 8 bits of data, the fundamental frequency F would be b=8 Hz.
2. Because the phone line attenuates frequencies above 3 kHz, the number of the highest harmonic passed through is 3000=F = 3000=(b=8) = 24000=b.
3. At 1200 baud, the fundamental frequency is 1200=8 = 150Hz, and the highest numbered harmonic passed is 24000=1200 = 20. That is, only the first 20 terms of the Fourier series are relevant; the phone line will chop off all higher numbered terms.

The following table gives more values

Baud Rate	Fundamental Harmonic (Hz)	Number of Harmonics sent
1200	150	20
2400	300	10
4800	600	5
9600	1200	2.5
19200	2400	1.25
38400	4800	.625

Will we be able to send data at 38,400 baud? No! It should be clear that sending data at 38400 baud over a voice grade line simply won't work. Even at 9600 baud only the first and second harmonic are transmitted, and the signal will be severely distorted. It is unlikely that the receiver will be able to recognize the signal as intended.

Must use better encoding schemes for higher data rates.

Maximum Data Rate of a Channel

Nyquist (1924) studied the problem of data transmission for a finite bandwidth noiseless channel. Nyquist states:

1. If a signal has been run through a low-pass filter of bandwidth H , the filtered signal

can be completely reconstructed by making 2H samples.
The important corollary to Nyquist's rule is that sampling more often is pointless because the higher frequencies have been filtered out.

2. If the encoding signal method consists of V states:
   maximum data rate = $2H \log_2 V$ bps

What's the maximum data rate over phone lines? Going back to our telephone example, Nyquist's theorem tells us that a one-bit signal encoding can produce no better than:
$2\ \ 3000\ \ \log_2 2 = 6000$bps.

But there is a catch. In practice, we don't come close to approaching this limit, because Nyquist's rule applies only to noiseless channels.

Noise on a Channel

In practice, every channel has background noise. Specifically:

1. Thermal noise results from thermal agitation of electrons in a conductor. It cannot be eliminated, and depends on the temperature, bandwidth, and Boltzman's constant K. Is uniformly distributed across the frequency spectrum and thus called white noise.

2. Inter modulation noise results when different frequencies share the same transmission medium; unwanted signals often appear at frequencies that are the sum or differences of the two frequencies.

3. Crosstalk noise results from unwanted coupling between signal paths. Hearing another conversation (faintly) on a telephone connection is an example of crosstalk.

4. Impulse noise consists of sharp, short-lived disturbances, from such sources such as lightning.

How do we measure (or quantify the amount of) background noise? The signal-to-noise ratio is a measure of the unwanted noise present on a line. It is expressed in decibels (db) and given by:

$$S{=}N(\text{db}) = 10 \log_{10} \frac{\text{signal power}}{\text{noise power}}$$

1.9.4 Shannon's Theorem

Shannon's theorem gives the maximum data rate for channels having noise (e.g., all real channels). Shannon's theorem states that the maximum data rate of a noisy channel of bandwidth H , signal-to-noise ratio of S=N is given by:

max data rate = H $\log_2$ (1 + S=N)

Note: the signal to noise ratio S=N used in Shannon's theorem refers to the ratio of signal power to noise power, not the ratio expressed in dbs (decibels). Unlike Nyquist's limit, Shannon's limit is valid regardless of the encoding method.

Let's consider a phone line again. A typical value for the S=N ratio for phone lines is 30db.

$$S{=}N = 10^{\frac{S=N(db)}{10}} = 10^3 = 1000.$$

Thus, the maximum data rate = 3000 $\log_2(1 + 1000)$ 30; 000 bps.
But wait | don't modems deliver data at 38.4 and 56 kbps? Many modem companies advertise that their modem deliver higher data rates, are they lying? Not necessarily. Read the ne print. Most likely, the modem uses data compression, and the high data rate is achieved only with text data

Let's summarize what Nyquist and Shannon say:

- Nyquist: sampling a received signal more frequently than 2H (where H is the bandwidth of the channel) is pointless.
- Nyquist: maximum data rate = 2H$\log_2$V bps, where H is the bandwidth of the channel, and V is the number of distinct encodings for each baud. This result is a theoretical upper bound on the data rate in the absence of noise.
- Shannon: maximum data rate = H$\log_2$(1 + S=N), where S/N is the ratio of signal power to noise power. Note that Shannon's result is independent of the number of distinct signal encodings. Nyquist's theorem implies that we can alway increase the data rate by increasing the number of distinct encodings; Shannon's limit says that is not so for a channel with noise

1.10 Guided Transmission Media

It is the transmission media in which signals are confined to a specific path using wire or cable. The types of Bounded/ Guided are discussed below.

1.10.1 Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 µs/km.
- Repeater spacing is 2km.

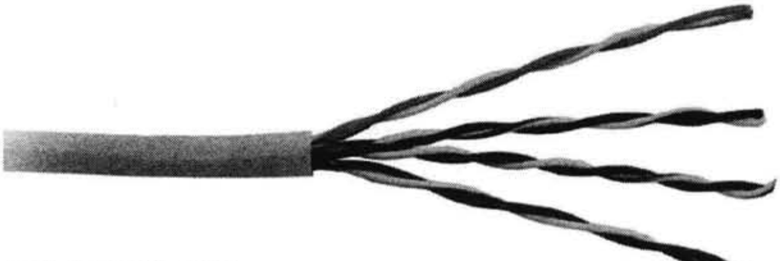
Twisted Pair is of two types :

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

1.10.2 Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.



UnShielded Twisted Pair Cable

1.10.2.1 Advantages :

- Installation is easy
- Flexible
- Cheap

- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

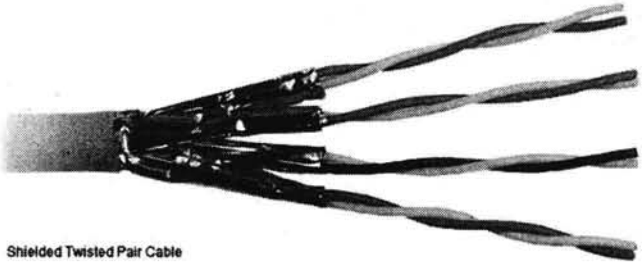
1.10.2.2 Disadvantages :

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

1.10.3 Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (explained in KEY TERMS Chapter).

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.



Shielded Twisted Pair Cable

1.10.3.1 Advantages :

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

1.10.3.2 Disadvantages :

- Difficult to manufacture
- Heavy

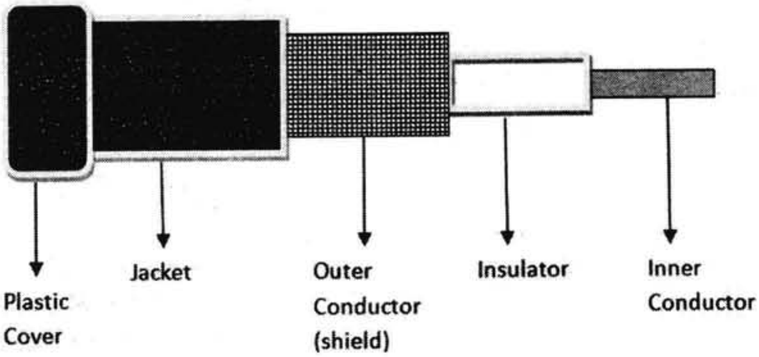
1.10.4 Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.



There are two types of Coaxial cables :

1.10.4.1 BaseBand

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

1.10.4.2 BroadBand

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

1.10.4.3 Advantages :

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

1.10.4.4 Disadvantages :

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

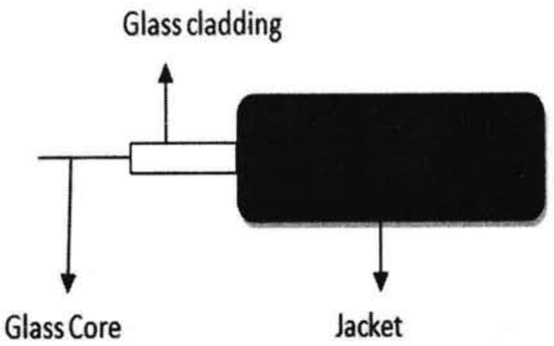
1.10.5Fiber Optic Cable

These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates.

In multimode fibres, the core is 50microns, and In single mode fibres, the thickness is 8 to 10 microns.

The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fibers are grouped together in bundles protected by an outer shield.

Fiber optic cable has bandwidth more than **2 gbps (Gigabytes per Second)**



1.10.5.1 Advantages :

- Provides high quality transmission of signals at very high speed.
- These are not affected by electromagnetic interference, so noise and distortion is very less.
- Used for both analog and digital signals.

1.10.5.2 Disadvantages :

- It is expensive
- Difficult to install.
- Maintenance is expensive and difficult.
- Do not allow complete routing of light signals.

Review Questions

1. Draw the ISO-OSI reference model and explain the functionalities of each layer in detail.
2. Compare the OSI reference model with TCP reference model. Explain how the layers can be grouped.
3. What is the difference between half-duplex and full-duplex transmission modes?
4. Name the four basic network topologies, and cite an advantage of each type.
5. For n devices in a network, what is the number of cable links required for a mesh, ring, bus, and star topology?
6. What are some of the factors that determine whether a communication system is a LAN or WAN?
7. Discuss the various transmission media in detail.
8. Explain the application areas of computer networks
9. Examine Shannon's Theorem
10. Describe the functions of the physical layer in detail.

UNIT – II

DATA LINK LAYER

2.1 Data Link Layer

Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data link layer has two sub-layers:

- **Logical Link Control:** It deals with protocols, flow-control, and error control.
- **Media Access Control:** It deals with actual control of media.

2.1.1 Functionality of Data-link Layer

Data link layer does many tasks on behalf of upper layer. These are:

- **Framing** - Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver end, data link layer picks up signals from hardware and assembles them into frames.
- **Addressing** - Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
- **Synchronization** - When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

- **Error Control** - Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
- **Flow Control** - Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.
- **Multi-Access** - When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

2.2 Error Detection and Error Correction

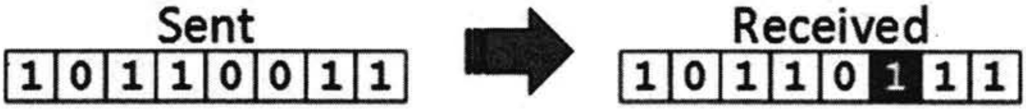
There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing. Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors

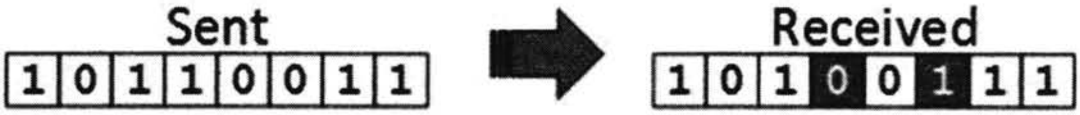
There may be three types of errors:

Single bit error



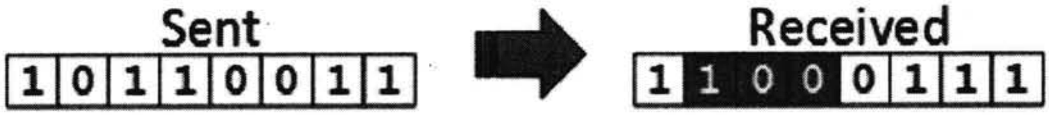
In a frame, there is only one bit, anywhere though, which is corrupt.

Multiple bits error



Frame is received with more than one bits in corrupted state.

Burst error



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

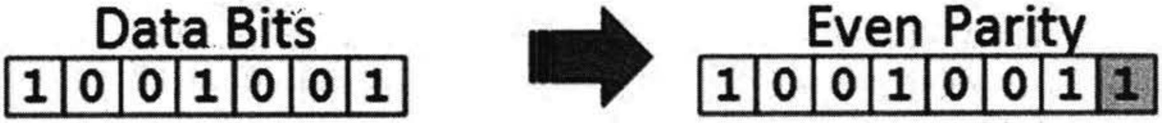
2.2.1 Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver end fails, the bits are considered corrupted.

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.

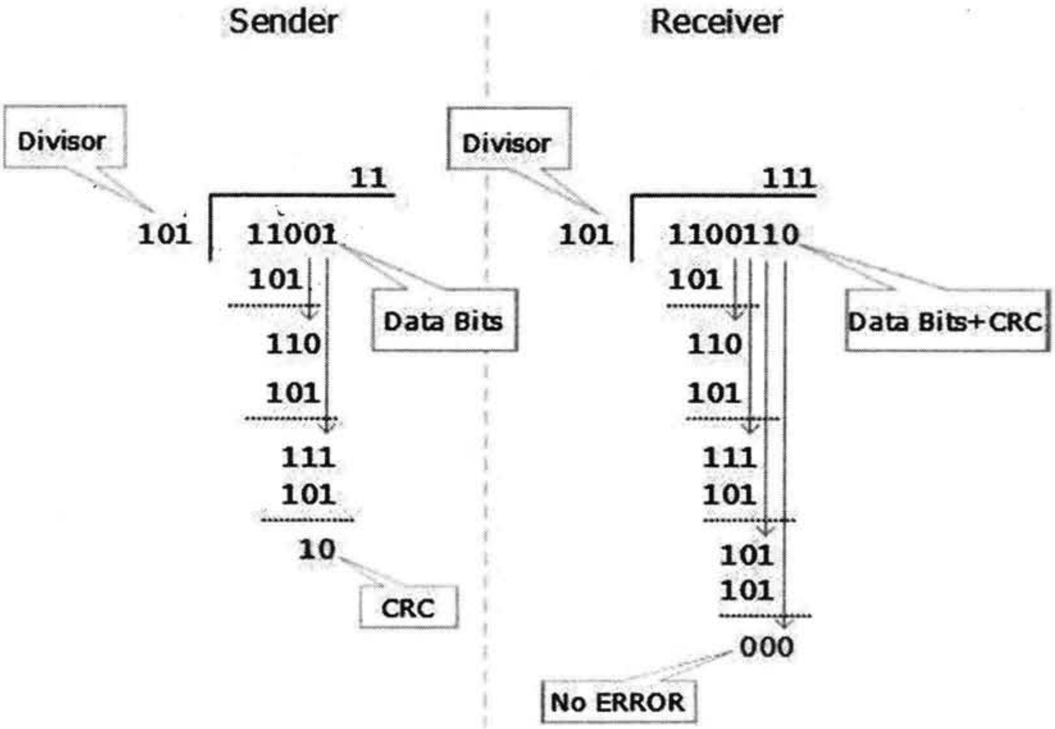


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erroneous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.



At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there is some data corruption occurred in transit.

2.2.2 Error Correction

In the digital world, error correction can be done in two ways:

Backward Error Correction

When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.

Forward Error Correction

When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection. For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is in error and one more bit to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

$$\mathbf{2^r >= m + r + 1}$$

2.3 Elementary Data Link Protocols

Data-link layer is responsible for implementation of point-to-point flow and error control mechanism.

Flow Control

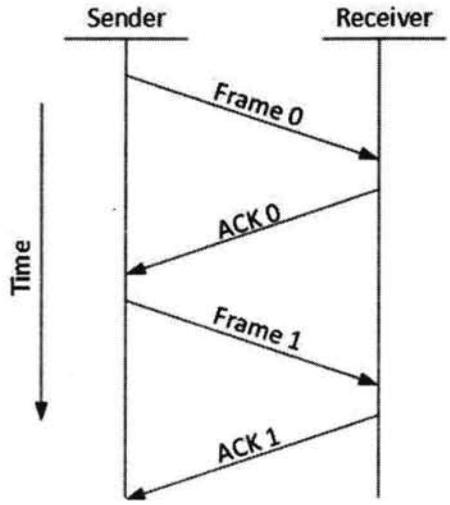
When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data.

What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

Stop and Wait

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



2.4 Sliding Window

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Error Control

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss.

In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

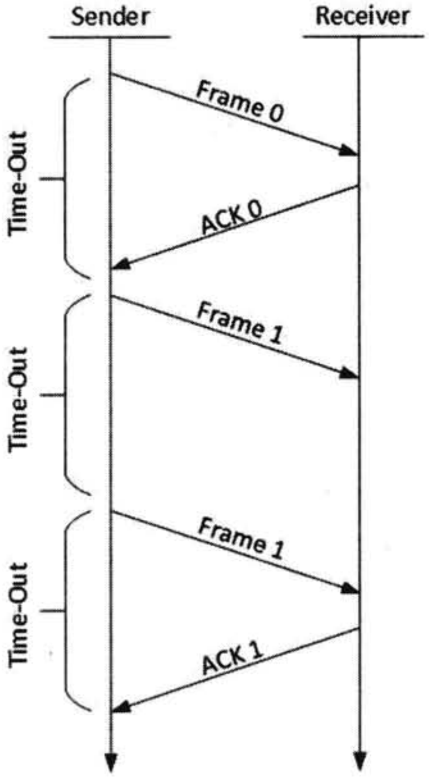
Requirements for error control mechanism:

- **Error detection:** The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK:** When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK:** When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.

- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout, the sender retransmits the frame, thinking that the frame or its acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

Stop and wait ARQ



The following transition may occur in Stop-and-Wait ARQ:

- ❖ The sender maintains a timeout counter.
- ❖ When a frame is sent, the sender starts the timeout counter.
- ❖ If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- ❖ If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- ❖ If a negative acknowledgement is received, the sender retransmits the frame.

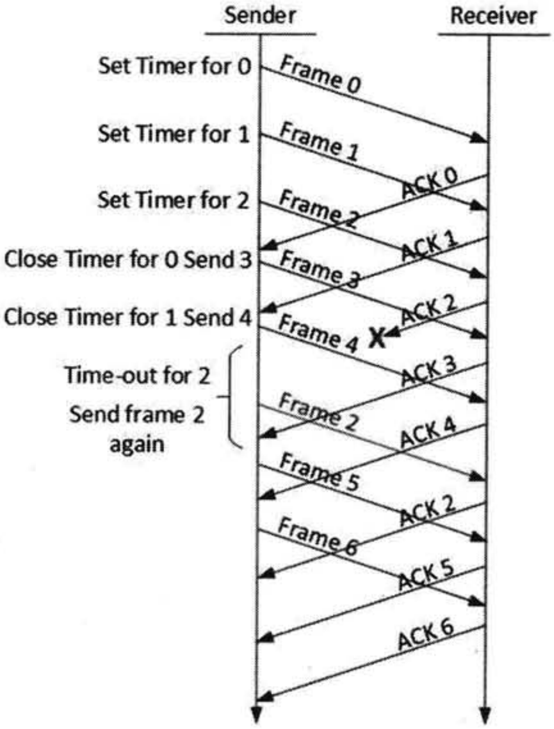
Go-Back-N ARQ

Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.

The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

Selective Repeat ARQ



In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.

In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

The sender in this case, sends only packet for which NACK is received.

2.4 Medium Access Layer

The **medium access control** or **media access control** (**MAC**) layer is the lower sublayer of the data link layer (layer 2) of the seven-layer OSI model. The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. an Ethernet network. The hardware that implements the MAC is referred to as a *media access controller*.

The MAC sublayer acts as an interface between the logical link control (LLC) sublayer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

A MAC layer is not required in full-duplex point-to-point communication, but address fields are included in some point-to-point protocols for compatibility reasons.

The LLC layer is standardized by the IEEE as the 802.2 since the beginning 1980 Its purpose is to allow level 3 network protocols (for eg IP) to be based on a single layer (the LLC layer) regardless underlying protocol used, including WiFi, Ethernet or Token Ring, for example.

All WiFi data packets so carry a pack LLC, which contains itself packets from the upper network layers. The header of a packet LLC indicates the type of layer 3 protocol in it: most of the time, it is IP protocol, but it could be another protocol, such as IPX (Internet Packet Exchange) for example. Thanks to the LLC layer, it is possible to have at the same time, on the same network, multiple Layer 3 protocols.

In LAN nodes uses the same communication channel for transmission. The MAC sub-layer has two primary responsibilities:

Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception. Media access control, including initiation of frame transmission and recovery from transmission failure.

2.4.1 Functions performed in the MAC sublayer

According to IEEE Std 802-2001 section 6.2.3 "MAC sublayer", the primary functions performed by the MAC layer are:[1]

- Frame delimiting and recognition
- Addressing of destination stations (both as individual stations and as groups of stations)
- Conveyance of source-station addressing information
- Transparent data transfer of LLC PDUs, or of equivalent information in the Ethernet sublayer
- Protection against errors, generally by means of generating and checking frame check sequences
- Control of access to the physical transmission medium

In the case of Ethernet, according to 802.3-2002 section 4.1.4, the functions required of a MAC are:[2]

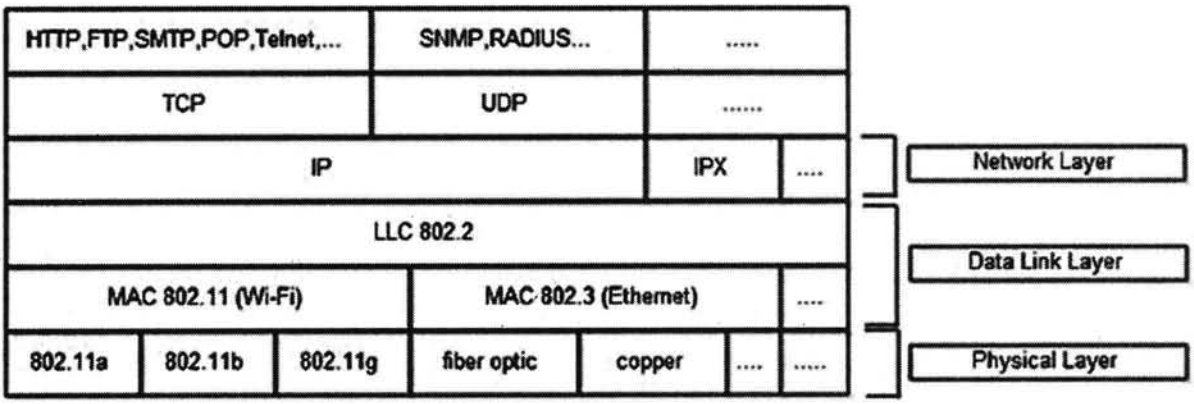
- receive/transmit normal frames
- half-duplex retransmission and backoff functions
- append/check FCS (frame check sequence)
- interframe gap enforcement
- discard malformed frames
- prepend(tx)/remove(rx) preamble, SFD (start frame delimiter), and padding
- half-duplex compatibility: append(tx)/remove(rx) MAC address

2.4.2 Addressing mechanism.

The local network addresses used in IEEE 802 networks and FDDI networks are called media access control addresses; they are based on the addressing scheme that was used in early Ethernet implementations. A MAC address is intended as a unique serial number. MAC addresses are typically assigned to network interface hardware at the time of manufacture. The most significant part of the address identifies the manufacturer, who assigns the remainder of the address, thus provide a potentially unique address.

This makes it possible for frames to be delivered on a network link that interconnects hosts by some combination of repeaters, hubs, bridges and switches, but not by network layer routers. Thus, for example, when an IP packet reaches its destination (sub)network, the destination IP address (a layer 3 or network layer concept) is resolved with the Address Resolution Protocolfor IPv4, or by Neighbor Discovery Protocol (IPv6) into the MAC address (a layer 2 concept) of the destination host.

Examples of physical networks are Ethernet networks and Wi-Fi networks, both of which are IEEE 802 networks and use IEEE 802 48-bit MAC addresses.



Network layers.

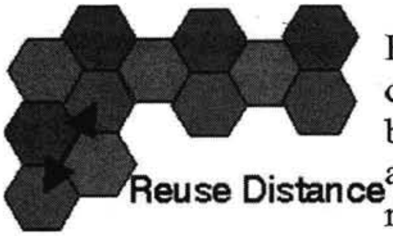
2.5 Channel Allocation Problem

Channel allocation deals with the allocation of channels to cells in a cellular network. Once the channels are allocated, cells may then allow users within the cell to communicate via the available channels. Channels in a wireless communication system typically consist of timeslots, frequency bands and/or CDMA pseudo noise sequences, but in an abstract sense, they can represent any generic transmission resource. There are three major categories for assigning these channels to cells (or base-stations).

They are

- Fixed Channel Allocation,
- Dynamic Channel Allocation and
- Hybrid Channel Allocation which is a combination of the first two methods.

2.5.1 Fixed Channel Allocation



Fixed Channel Allocation (FCA) systems allocate specific channels to specific cells. This allocation is static and can not be changed. For efficient operation, FCA systems typically allocate channels in a manner that maximizes frequency reuse. Thus, in a FCA system, the distance between cells using the same channel is the minimum reuse distance for that system. The problem with FCA systems is quite simple and occurs whenever the offered traffic to a network of base stations is not uniform. Consider a case in which two adjacent cells are allocated *N* channels each. There clearly can be situations in which one cell has a need for *N+k* channels while the adjacent cell only requires *N-m*channels (for positive integers *k* and *m*). In such a case, *k* users in the first cell would be blocked from making calls while *m* channels in the second cell would go unused. Clearly in this situation of non-uniform spatial offered traffic, the available channels are not being used efficiently. FCA has been implemented on a widespread level to date.

2.5.2 Dynamic Channel Allocation

Dynamic Channel Allocation (DCA) attempts to alleviate the problem mentioned for FCA systems when offered traffic is non-uniform. In DCA systems, no set relationship exists between channels and cells. Instead, channels are part of a pool of resources. Whenever a channel is needed by a cell, the channel is allocated under the constraint that frequency reuse requirements cannot be violated. There are two problems that typically occur with DCA based systems.

- First, DCA methods typically have a degree of randomness associated with them and this leads to the fact that frequency reuse is often not maximized unlike the case for FCA systems in which cells using the same channel are separated by the minimum reuse distance.
- Secondly, DCA methods often involve complex algorithms for deciding which available channel is most efficient. These algorithms can be very computationally intensive and may require large computing resources in order to be real-time.

2.5.3 Hybrid Channel Allocation Schemes

The third category of channel allocation methods includes all systems that are hybrids of fixed and dynamic channel allocation systems. Several methods have been presented that fall within this category and in addition, a great deal of comparison has been made with corresponding simulations and analyses.

The developed hybrid methods are,

Channel Borrowing is one of the most straightforward hybrid allocation schemes. Here, channels are assigned to cells just as in fixed allocation schemes. If a cell needs a channel in excess of the channels previously assigned to it, that cell may borrow a channel from one of its neighbouring cells given that a channel is available and use of this channel won't violate frequency reuse requirements. Note that since every channel has a predetermined relationship with a specific cell, channel borrowing (without the extensions mentioned below) is often categorized as a subclass of fixed allocation schemes. The major problem with channel borrowing is that when a cell borrows a channel from a neighboring cell, other nearby cells are prohibited from using the borrowed channel because of co-channel interference. This can lead to increased call blocking over time. To reduce this call blocking penalty, algorithms are necessary to ensure that the channels are borrowed from the most available neighboring cells; i.e., the neighboring cells with the most unassigned channels.

Two extensions of the channel borrowing approach are **Borrowing with Channel Ordering** (BCO) and **Borrowing with Directional Channel Locking** (BDCL).

- Borrowing with Channel Locking was designed as an improvement over the simpler Channel Borrowing approach as described above [Elnoubi]. BCO systems have two distinctive characteristics [Elnoubi]:
  1. The ratio of fixed to dynamic channels varies with traffic load.
  2. Nominal channels are ordered such that the first nominal channel of a cell has the highest priority of being applied to a call within the cell.

  The last nominal channel is most likely to be borrowed by neighboring channels. Once a channel is borrowed, that channel is locked in the co-channel cells within the reuse distance of the cell in question. To be "locked" means that a channel can not be used or borrowed. Zhang and Yum [Zhang] presented the BDCL scheme as an improvement over the BCO method. From a frequency reuse standpoint, in a BCO system, a channel may be borrowed only if it is free in the neighboring cochannel cells. This criteria is often too strict.

In Borrowing with Directional Channel Locking, borrowed channels are only locked in nearby cells that are affected by the borrowing. This differs from the BCO scheme in which a borrowed channel is locked in every cell within the reuse distance. The benefit of BDCL is that more channels are available in the presence of borrowing and subsequent call blocking is reduced. A disadvantage of BDCL is that the statement "borrowed channels are only locked in nearby cells that are affected by the borrowing" requires a clear understanding of the term "affected." This may require microscopic analysis of the area in which the cellular system will be located. Ideally, a system can be general enough that detailed analysis of specific propagation measurements is not necessary for implementation.

2.6 Multiple Access Protocols.

Protocols are used by Medium Access Layer:

2.6.1 ALOHA

ALOHA is a system for coordinating and arbitrating access to a shared communication channel. It was developed in the 1970s at the University of Hawaii. The original system used terrestrial radio broadcasting, but the system has been implemented in satellite communication systems. A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time.

In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

2.6.2 Carrier Sensed Multiple Access (CSMA)

CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it. There are two methods for avoiding these so-called collisions, listed here :

2.6.3 CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

CD (collision detection) defines what happenswhen two devices sense a clear channel, then attempt totransmit at the same time. A collision occurs, and bothdevices stop transmission, wait for a random amount oftime, and then retransmit. This is the technique used to access the 802.3 Ethernet network channel.

This method handles collisions as they occur, but if the bus is constantly busy, collisions can occur so often that performance drops drastically. It is estimated that network traffic must be less than 40 percent of the bus capacity for the network to operate efficiently. If distances are long, time lags occur that may result in inappropriate carrier sensing, and hence collisions.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) : In CA collision avoidance), collisions are avoided because each node signals its intent to transmit before actually doing so. This method is not popular because it requires excessive overhead that reduces performance.

- **Ethernet : IEEE 802.3 Local Area Network (LAN) Protocols :** Ethernet protocols refer to the family of local-area network (LAN)covered by the IEEE 802.3. In the Ethernet standard, there are twomodes of operation: half-duplex and full-duplex modes. In the halfduplex mode, data are transmitted using the popular Carrier-SenseMultiple Access/Collision Detection (CSMA/CD) protocol on a shared medium.

- The main disadvantages of the half-duplex are the efficiency and distance limitation, in which the link distance is limited by the minimum MAC frame size. This restriction reduces the efficiency drastically for high-rate transmission. Therefore, the carrier extension technique is used to ensure the minimum frame size of 512 bytes in Gigabit Ethernet to achieve a reasonable link distance. Four data rates are currently defined for operation over optical fiber and twisted-pair cables :

- 10 Mbps - 10Base-T Ethernet (IEEE 802.3)
- 100 Mbps - Fast Ethernet (IEEE 802.3u)
- 1000 Mbps - Gigabit Ethernet (IEEE 802.3z)
- 10-Gigabit - 10 Gbps Ethernet (IEEE 802.3ae).

The **Ethernet System** consists of three basic elements :

(1) The physical medium used to carry Ethernet signals between computers,

(2) a set of medium access control rules embedded in each Ethernet interface that allow multiple computers to fairly arbitrate access to the shared Ethernet channel, and

(3) an Ethernet frame that consists of a standardized set of bits used to carry data over the system.

As with all IEEE 802 protocols, the ISO data link layer is divided into two IEEE 802 sub-layers, the Media Access Control (MAC) sub-layer and the MAC-client sub-layer. The IEEE 802.3 physical layer corresponds to the ISO physical layer.

Each Ethernet-equipped computer operates independently of all other stations on the network: there is no central controller. All stations attached to an Ethernet are connected to a shared signaling system, also called the medium. To send data a station first listens to the channel, and when the channel is idle the station transmits its data in the form of an Ethernet frame, or packet.

After each frame transmission, all stations on the network must contend equally for the next frame transmission opportunity. Access to the shared channel is determined by the medium access control (MAC) mechanism embedded in the Ethernet interface located in each station. The medium access control mechanism is based on a system called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

As each Ethernet frame is sent onto the shared signal channel, all Ethernet interfaces look at the destination address. If the destination address of the frame matches with the interface address, the frame will be read entirely and be delivered to the networking software running on that computer. All other network interfaces will stop reading the frame when they discover that the destination address does not match their own address.

2.6.4 IEEE 802.4 Token Bus

In token bus network station must have possession of a token before it can transmit on the network. The IEEE 802.4 Committee has defined token bus standards as broadband networks, as opposed to Ethernet's baseband transmission technique. The topology of the network can include groups of workstations connected by long trunk cables.

These workstations branch from hubs in a star configuration, so the network has both a bus and star topology. Token bus topology is well suited to groups of users that are separated by some distance. IEEE 802.4 token bus networks are constructed with 75-ohm coaxial cable using a bus topology. The broadband characteristics of the 802.4 standard support transmission over several different channels simultaneously.

The token and frames of data are passed from one station to another following the numeric sequence of the station addresses. Thus, the token follows a logical ring rather than a physical ring. The last station in numeric order passes the token back to the first station. The token does not follow the physical ordering of workstation attachment to the cable. Station 1 might be at one end of the cable and station 2 might be at the other, with station 3 in the middle.

While token bus is used in some manufacturing environments, Ethernet and token ring standards have become more prominent in the office environment.

2.6.5 IEEE 802.5 Token Ring

Token ring is the IEEE 802.5 standard for a token-passing ring network with a star-configured physical topology. Internally, signals travel around the network from one station to the next in a ring. Physically, each station connects to a central hub called a MAU (multistation access unit). The MAU contains a "collapsed ring," but the physical configuration is a star topology. When a station is attached, the ring is extended out to the station and then back to the MAU .

If a station goes offline, the ring is reestablished with a bypass at the station connector. Token ring was popular for an extended period in the late 1980s and 1990s, especially in IBM legacy system environments. IBM developed the technology and provided extensive support for connections to SNA systems. More recently, Ethernet, Fast Ethernet, and Gigabit Ethernet technologies have pushed token ring and other LAN technologies to the sidelines.

2.7 Network Layer

Layer-3 in the OSI model is called Network layer. Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking.

Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

Layer-3 Functionalities

Devices which work on Network Layer mainly focus on routing. Routing may include various tasks aimed to achieve a single goal. These can be:

- Addressing devices and networks.
- Populating routing tables or static routes.
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- Internetworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provides connection oriented and connection less mechanism.

Network Layer Features

With its standard functionalities, Layer 3 can provide various features as:

- Quality of service management
- Load balancing and link management
- Security
- Interrelation of different protocols and subnets with different schema.
- Different logical network design over the physical network design.
- L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

Internet protocol is widely respected and deployed Network Layer protocol which helps to communicate end to end devices over the internet. It comes in two flavors. IPv4 which has ruled the world for decades but now is running out of address space. IPv6 is created to replace IPv4 and hopefully mitigates limitations of IPv4 too.

2.8 Design Issues

The network layer has been designed with the following goals:

1. The services provided should be independent of the underlying technology. Users of the service need not be aware of the physical implementation of the network - for all they know, they're messages could be transported via carrier pigeon! This design goal has great importance when we consider the great variety of networks in operation. In the area of Public networks, networks in underdeveloped countries are nowhere near the technological prowess of those in the countries like the US or Ireland. The design of the layer must not disable us from connecting to networks of different technologies.
2. The transport layer (that is the host computer) should be shielded from the number, type and different topologies of the subnets he uses. That is, all the transport layer want is a communication link, it need not know how that link is made.
3. Finally, there is a need for some uniform addressing scheme for network addresses.

With these goals in mind, two different types of service emerged: **Connection oriented and connectionless.** A connection-oriented service is one in which the user is given a "reliable" end to end connection. To communicate, the user requests a connection, then uses the connection to his hearts content, and then closes the connection. A telephone call is the classic example of a connection oriented service.

In a connection-less service, the user simply bundles his information together, puts an address on it, and then sends it off, in the hope that it will reach its destination. There is no guarantee that the bundle will arrive. So - a connection less service is one reminiscent of the postal system. A letter is sent, that is, put in the post box. It is then in the "postal network" where it gets bounced around and hopefully will leave the network in the correct place, that is, in the addressee's letter box.

With a connection oriented service, the user must pay for the length (ie the duration) of his connection. Usually this will involve a fixed start up fee. Now, if the user intends to send a constant stream of data down the line, this is great - he is given a reliable service for as long as he wants. However, say the user wished to send only a packet or two of data - now the cost of setting up the connection greatly overpowers the cost of sending that one packet. Consider also the case where the user wishes to send a packet once every 3 minutes. In a connection-oriented service, the line will thus be idle for the majority of the time, thus wasting bandwidth. So, connection-oriented services seem to be useful only when the user wishes to send a constant stream of data.

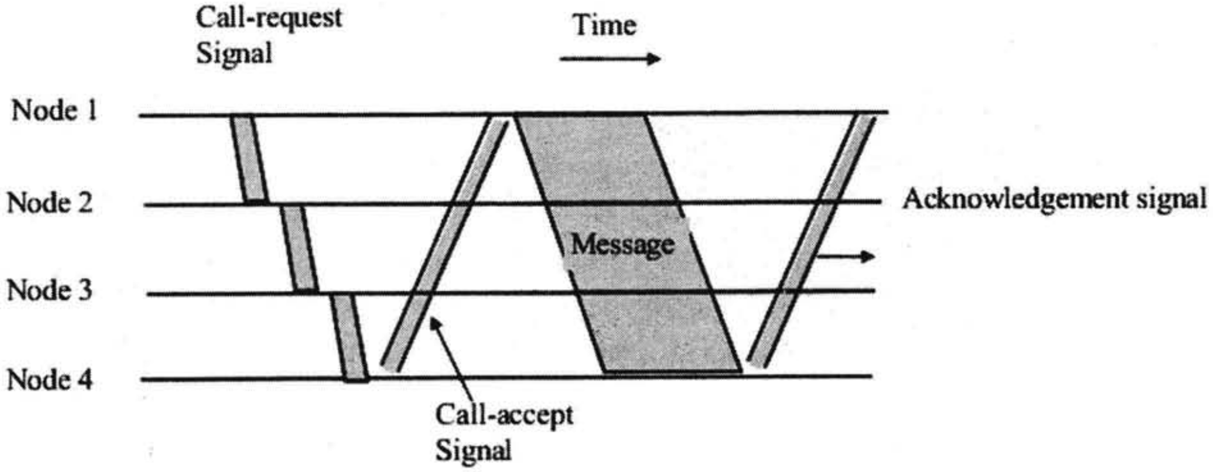
One would therefore think that the reliable nature of the connection oriented service would prompt people to choose it over the connectionless service - this is in fact not the case. One can never ensure that the network is 100% reliable, in fact for many applications we must assume that the network is not reliable at all. With this in mind, many applications perform their own error detection, flow and congestion control at a higher level in the protocol stack, that is, on their own machine, in the transport layer. The network layer should provide a raw means of sending packets from a to b, and that is all. Proponents of this argument are quick to point out that the standard of our networks has increased greatly in the past years, that packets of information rarely ever do get lost, so much of the correction facilities in the network layer are redundant and serve only to complicate the layer and slow down transfer.

Its interesting to note here that it is easy to provide a connection oriented service over an inherently connectionless service, so in fact defining the service of the network layer as connectionless is the general solution. However, at the time of defining the network layer, the controversy between the two camps was (and still is) unresolved, and so instead of deciding on one service, the ISO allowed both.

Circuit Switching:

A dedicated path between the source node and the destination node is set up for the duration of communication session to transfer data. That path is a connected sequence of links between network nodes. On each physical link, a logical channel is dedicated to the connection. Communication via circuit switching involves three phases,

1. **Circuit Establishment:** Before any signals can be transmitted, an end-to-end (station-to-station) circuit must be established .
2. **Data Transfer:** The data may be analog or digital, depending on the nature of the network
3. **Circuit Disconnect:**After some period of data transfer, the connection is terminated, usually by the action of one of the two stations



Examples: PSTN, PBX etc.

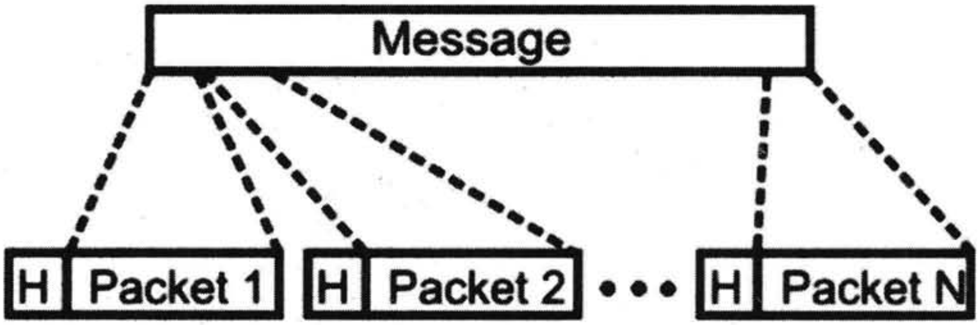
circuit switching telecommunication networks was originally designed to handle voice traffic, and the majority of the traffic on these networks continues to be voice. A key characteristics of the circuit switching is that resources within the network are dedicated to a particular call. For voice communication the resulting circuit will enjoy the high percentage of utilization because most of the time one party or the other is talking.

However, as the circuit-switching network began to be used increasingly for data connections, two shortcomings became apparent:

1. In a typical userlhost data connection (e.g., personal computer user logged on to a database server), much of the time the line is idle. Thus, with data connections, a circuit-switching approach is inefficient.
2. In a circuit-switching network, the connection provides for transmission at constant data rate. Thus, each of the two devices that are connected must transmit and receive at the same data rate as the other; this limits the utility of the network in interconnecting a variety of host computers and terminals.

Packet Switching:

Messages are divided into subsets of equal length called packets. In packet switching approach, data are transmitted in short packets (few Kbytes). A long message is broken up into a series of packets as shown in Fig Every packet contains some control information in its header, which is required for routing and other purposes.



A message is divided into a number of equal length short packets

Main difference between Packet switching and Circuit Switching is that the communication lines are not dedicated to passing messages from the source to the destination. In Packet Switching, different messages (and even different packets) can pass through different routes, and when there is a "dead time" in the communication between the source and the destination, the lines can be used by other sources.

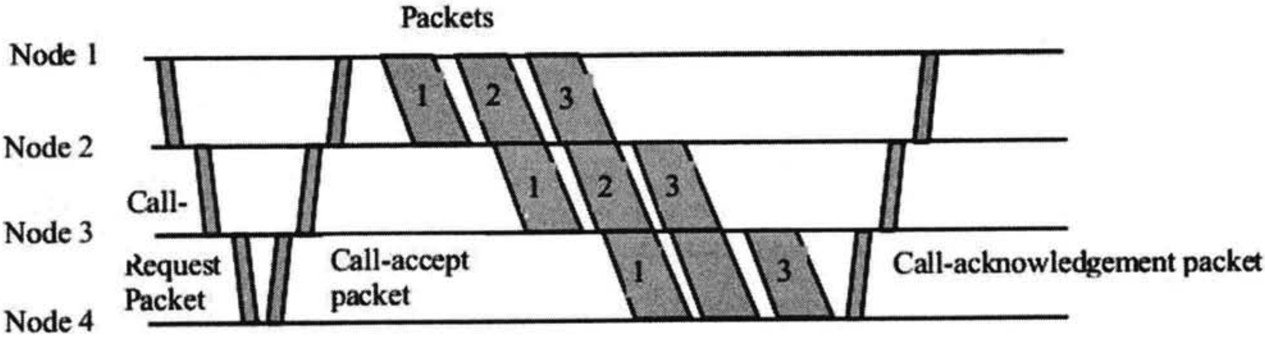
There are two basic approaches commonly used to packet Switching: **virtual circuit packet switching and datagram packet switching**. In virtual-circuit packet switching a virtual circuit is made before actual data is transmitted, but it is different from circuit switching in a sense that in circuit switching the call accept signal comes only from the final destination to the source while in case of virtual-packet switching this call accept signal is transmitted between each adjacent intermediate node as shown in Fig. Other features of virtual circuit packet switching are discussed in the following subsection.

Virtual Circuit:

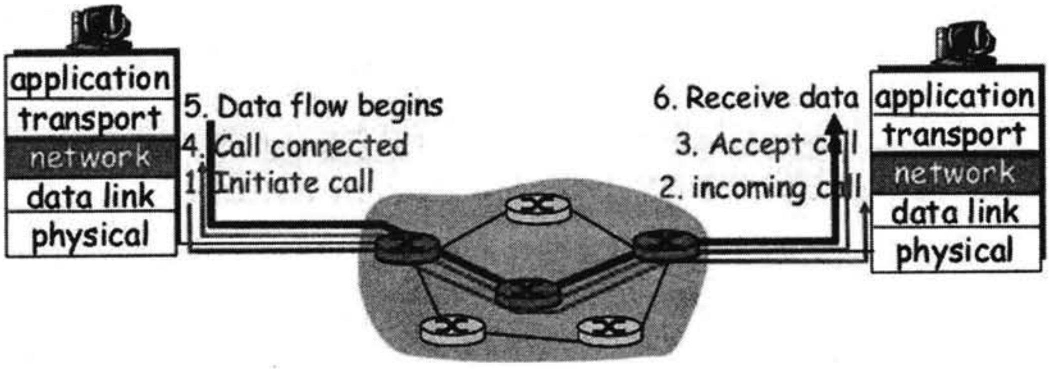
An initial setup phase is used to set up a route between the intermediate nodes for all the packets passed during the session between the two end nodes. In each intermediate node, an entry is registered in a table to indicate the route for the connection that has been set up. Thus, packets passed through this route, can have short headers, containing only a **virtual circuit identifier (VCI)**, and not their destination.

Each intermediate node passes the packets according to the information that was stored in it, in the setup phase. In this way, packets arrive at the destination in the correct sequence, and it is guaranteed that essentially there will not be errors. This approach is slower than Circuit Switching, since different virtual circuits may compete over the same resources, and an initial setup phase is needed to initiate the circuit. As in Circuit Switching, if an intermediate node fails, all virtual circuits that pass through it are lost.

The most common forms of Virtual Circuit networks are X.25 and Frame Relay, which are commonly used for public data networks (PDN).



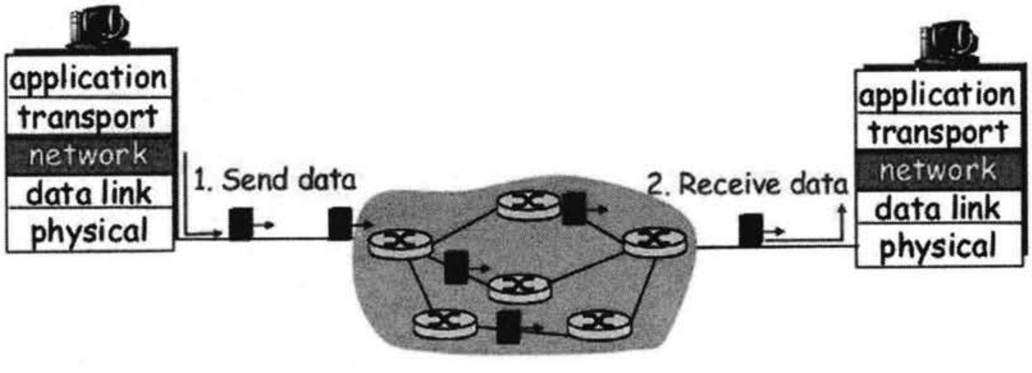
Virtual circuit Packet Switching techniques



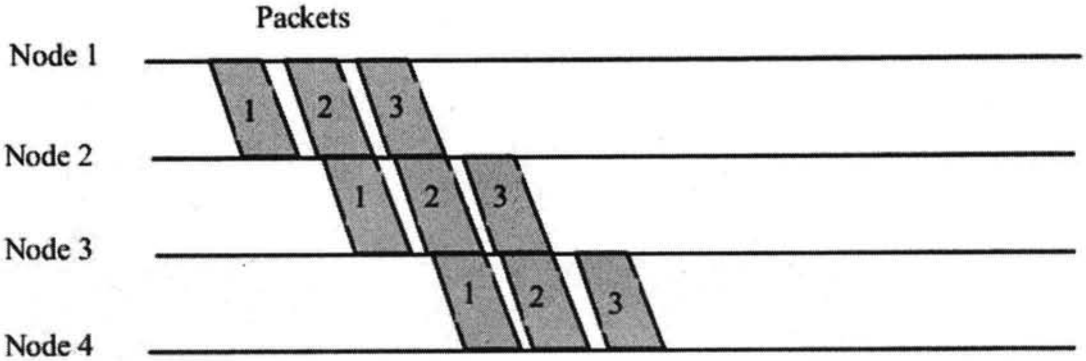
Virtual Circuit

Datagram:

This approach uses a different, more dynamic scheme, to determine the route through the network links. Each packet is treated as an independent entity, and its header contains full information about the destination of the packet. The intermediate nodes examine the header of the packet, and decide to which node to send the packet so that it will reach its destination.



in this method, the packets don't follow a pre-established route, and the intermediate nodes (the routers) don't have pre-defined knowledge of the routes that the packets should be passed through. Packets can follow different routes to the destination, and delivery is not guaranteed . Due to the nature of this method, the packets can reach the destination in a different order than they were sent, thus they must be sorted at the destination to form the original message. This approach is time consuming since every router has to decide where to send each packet. The main implementation of Datagram Switching network is the Internet, which uses the IP network protocol.



Datagram Packet Switching

Datagram Packet Switching Vs Virtual-circuit Packet Switching:

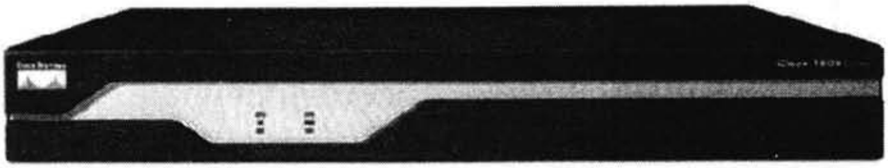
sno	Datagram Packet Switching	Virtual-circuit Packet Switching
1	Two packets of the same user pair can travel along different routes	All packets of the same virtual circuit travel along the same path.
2	The packets can arrive out of sequence.	Packet sequencing is guaranteed.
3	Packets contain full Src, Dst addresses	Packets contain short VC Id. (VCI).
4	Each host occupies routine table entries.	Each VC occupies routing table entries.
5	Requires no connection setup.	Requires VC setup. First packet has large delay
6	Also called Connection less	Also called connection oriented.
7	Examples: X.25 and Frame Relay	Eg. Internet which uses IP Network protocol

2.9 Routing Algorithms

2.9.1 Router

A Router is a computer, just like any other computer including a PC. Routers have many of the same hardware and software components that are found in other computers including:

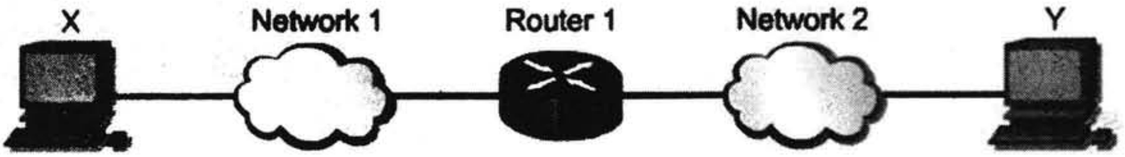
- CPU
- RAM
- ROM
- Operating System



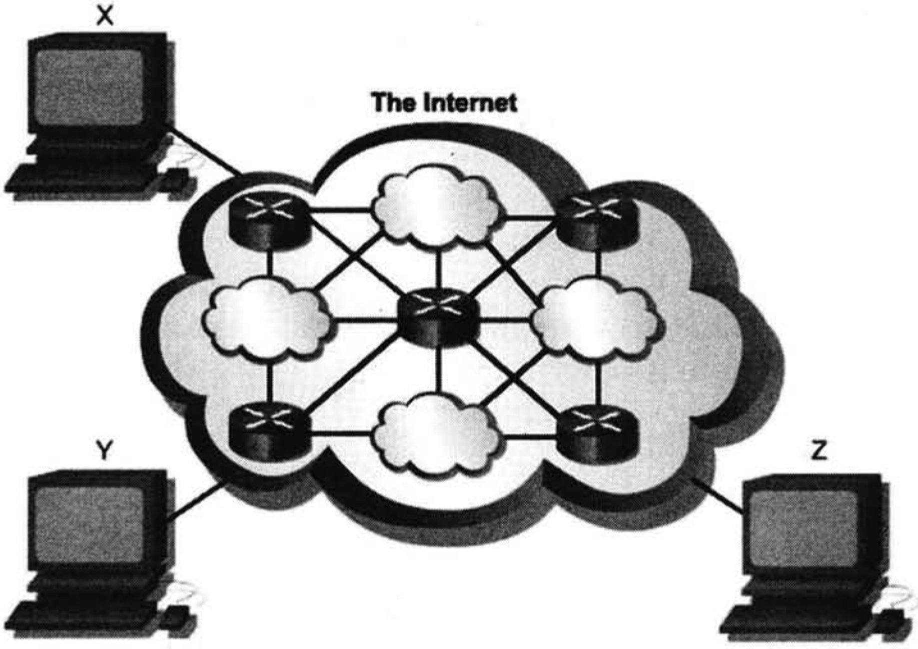
4er 1841 Integrated Services Router

Router is the basic backbone for the Internet. The main function of the router is to connect two or more than two network and forwards the packet from one network to another. A router connects multiple networks. This means that it has multiple interfaces that each belong to a different IP network.

When a router receives an IP packet on one interface, it determines which interface to use to forward the packet onto its destination. The interface that the router uses to forward the packet may be the network of the final destination of the packet (the network with the destination IP address of this packet), or it may be a network connected to another router that is used to reach the destination network.



Router connects two network



Internet Architecture

· A router uses IP to forward packets from the source network to the destination network. The packets must include an identifier for both the source and destination networks. A router uses the IP address of the destination network to deliver a packet to the correct network. When the packet arrives at a router connected to the destination network, the router uses the IP address to locate the specific computer on the network.

2.9.2 Routing and Routing Protocols:

The primary responsibility of a router is to direct packets destined for local and remote networks by:

- Determining the best path to send packets
- Forwarding packets toward their destination

The router uses its routing table to determine the best path to forward the packet. When the router receives a packet, it examines its destination IP address and searches for the best match with a network address in the router's routing table. The routing table also includes the interface to be used to forward the packet. Once a match is found, the router encapsulates the IP packet into the data link frame of the outgoing or exit interface, and the packet is then forwarded toward its destination.

2.9.2 Static Routes:

Static routes are configured manually, network administrators must add and delete static routes to reflect any network topology changes. In a large network, the manual maintenance of routing tables could require a lot of administrative time. On small networks with few possible changes, static routes require very little maintenance. Static routing is not as scalable as dynamic routing because of the extra administrative requirements. Even in large networks, static routes that are intended to accomplish a specific purpose are often configured in conjunction with a dynamic routing protocol.

When to use static Routing:

- **A network consists of only a few routers.** Using a dynamic routing protocol in such a case does not present any substantial benefit. On the contrary, dynamic routing may add more administrative overhead.
- **A network is connected to the Internet only through a single ISP.** There is no need to use a dynamic routing protocol across this link because the ISP represents the only exit point to the Internet.

- **A large network is configured in a hub-and-spoke topology.** A hub-and-spoke topology consists of a central location (the hub) and multiple branch locations (spokes), with each spoke having only one connection to the hub. Using dynamic routing would be unnecessary because each branch has only one path to a given destination-through the central location.

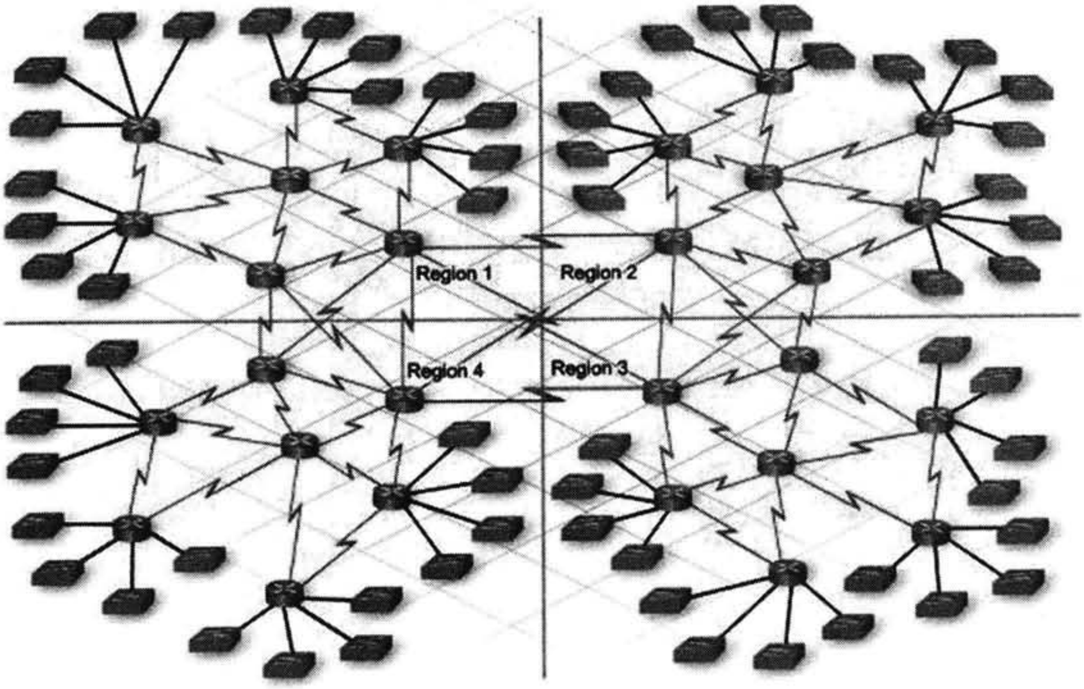
2.9.3 Connected Routes:

Those network that are directly connected to the Router are called connected routes and are not needed to configure on the router for routing. They are automatically routed by the Router.

2.9.4 Dynamic Routes:

Dynamic routing protocol uses a route that a routing protocol adjusts automatically for topology or traffic changes.

Imagine maintaining static routing configurations for THIS network!



2.9.5 Routing Protocol:

A routing protocol is the communication used between routers. A routing protocol allows routers to share information about networks and their proximity to each other. Routers use this information to build and maintain routing tables.

Autonomous System:

An AS is a collection of networks under a common administration that share a common routing strategy. To the outside world, an AS is viewed as a single entity. The AS may be run by one or more operators while it presents a consistent view of routing to the external world.

The American Registry of Internet Numbers (ARIN), a service provider, or an administrator assigns a 16-bit identification number to each AS.

Dynamic Routing Protocol:

1. Interior Gateway protocol (IGP) I). Distance Vector Protocol II). Link·State Protocol
2. Exterior Gateway Protocol (EGP)

Interior gateway protocol (IGP): Within one Autonomous System.

Exterior Routing Protocol(EGP): Between the Autonomous System. Example BGP (Boarder gateway protocol)

Metric:

There are cases when a routing protocol learns of more than one route to the same destination. To select the best path, the routing protocol must be able to evaluate and differentiate between the available paths. For this purpose a metric is used. A metric is a value used by routing protocols to assign costs to reach remote networks. The metric is used to determine which path is most preferable when there are multiple paths to the same remote network.

Each routing protocol uses its own metric. For example, RIP uses hop count, EIGRP uses a combination of bandwidth and delay, and Cisco's implementation of OSPF uses bandwidth.

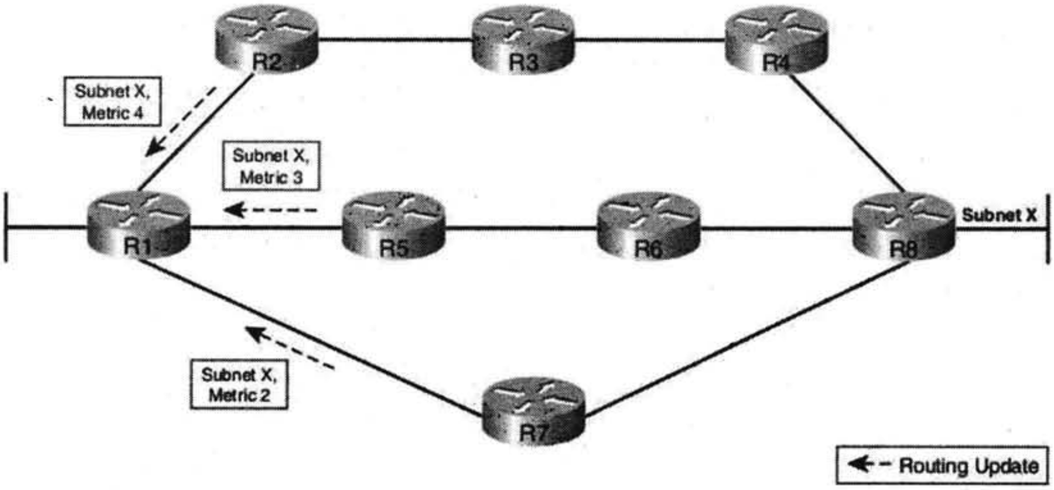
2.9.6 Distance Vector Routing Algorithm:

As the name implies, distance vector means that routes are advertised as vectors of distance and direction. Distance is defined in terms of a metric such as hop count and direction is simply the next-hop router or exit interface. A router using a distance vector routing protocol does not have the knowledge of the entire path to a destination network. Instead the router knows only:

The direction or interface in which packets should be forwarded and The distance or how far it is to the destination network.

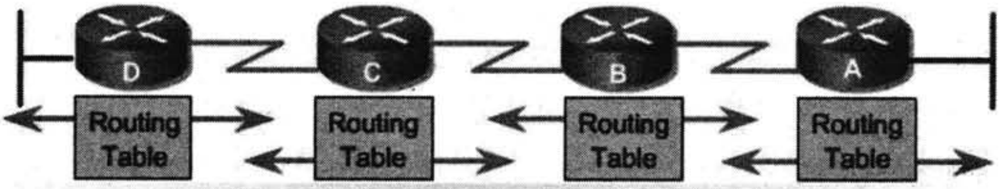
To show you more exactly what a distance vector protocol does, Figure shows a view of what a router learns with a distance vector routing protocol. The figure shows an internetwork in which R1 learns about three routes to reach subnet X:

- The four-hop route through R2
- The three-hop route through R5
- The two-hop route through R7

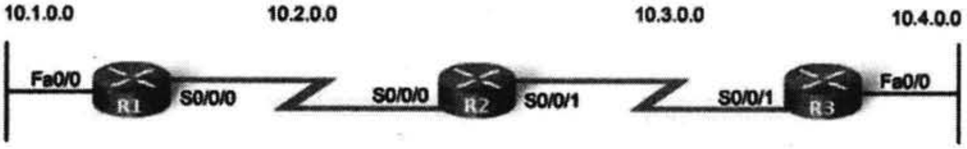


R1 learns about the subnet, and a metric associated with that subnet, and nothing more. R1 must then pick the best route to reach subnet X. In this case, it picks the two-hop route through R7, because that route has the lowest metric.

Distance vector protocols typically use the **Bellman-Ford algorithm** for the best path route determination.



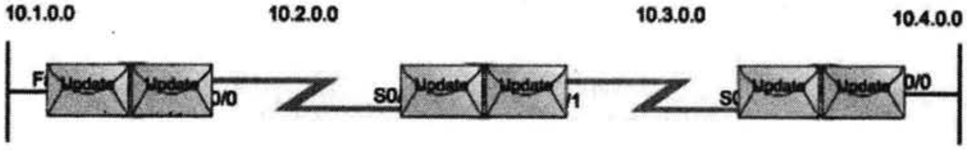
Pass periodic copies of a routing table to neighbor routers and accumulate distance vectors.



Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0

Network	Interface	Hop
10.3.0.0	S0/0/0	0
10.4.0.0	Fa0/0	0



Initial Update:

R1

- Sends an update about network 10.1.0.0 out the Serial0/0/0 interface
- Sends an update about network 10.2.0.0 out the FastEthernet0/0 interface
- Receives update from R2 about network 10.3.0.0 with a metric of 1
- Stores network 10.3.0.0 in the routing table with a metric of 1

R2

- Sends an update about network 10.3.0.0 out the Serial 0/0/0 interface
- Sends an update about network 10.2.0.0 out the Serial 0/0/1 interface
- Receives an update from R1 about network 10.1.0.0 with a metric of 1
- Stores network 10.1.0.0 in the routing table with a metric of 1
- Receives an update from R3 about network 10.4.0.0 with a metric of 1
- Stores network 10.4.0.0 in the routing table with a metric of 1

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/0	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

R3

- Sends an update about network 10.4.0.0 out the Serial 0/0/0 interface
- Sends an update about network 10.3.0.0 out the FastEthernet0/0
- Receives an update from R2 about network 10.2.0.0 with a metric of 1
- Stores network 10.2.0.0 in the routing table with a metric of 1

After this first round of update exchanges, each router knows about the connected networks of their directly connected neighbors. However, did you notice that R1 does not yet know about 10.4.0.0 and that R3 does not yet know about 10.1.0.0? Full knowledge and a converged network will not take place until there is another exchange of routing information.

Next Update:

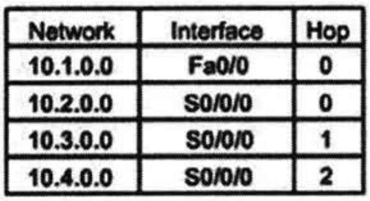
R1

- Sends an update about network 10.1.0.0 out the Serial 0/0/0 interface.
- Sends an update about networks 10.2.0.0 and 10.3.0.0 out the FastEthernet0/0 interface.
- Receives an update from R2 about network 10.4.0.0 with a metric of 2.
- Stores network 10.4.0.0 in the routing table with a metric of 2.

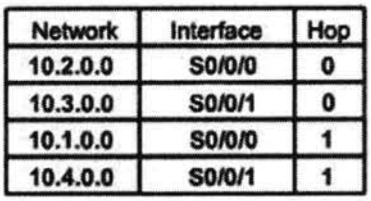
Same update from R2 contains information about network 10.3.0.0 with a metric of 1. There is no change; therefore, the routing information remains the same.

R2

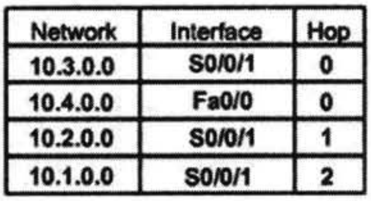
- Sends an update about networks 10.3.0.0 and 10.4.0.0 out of Serial 0/0/0 interface.
- Sends an update about networks 10.1.0.0 and 10.2.0.0 out of Serial 0/0/1 interface.
- Receives an update from R1 about network 10.1.0.0. There is no change; therefore, the routing information remains the same.
- Receives an update from R3 about network 10.4.0.0. There is no change; therefore, the routing information remains the same.



Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2



Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1



Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

R3

- Sends an update about network 10.4.0.0 out the Serial 0/0/0 interface.
- Sends an update about networks 10.2.0.0 and 10.3.0.0 out the FastEthernet0/0 interface.
- Receives an update from R2 about network 10.1.0.0 with a metric of 2.

- Stores network 10.1.0.0 in the routing table with a metric of 2.
- Same update from R2 contains information about network 10.2.0.0 with a metric of 1. There is no change; therefore, the routing information remains the same.

Note: Distance vector routing protocols typically implement a technique known as split horizon. Split horizon prevents information from being sent out the same interface from which it was received. For example, R2 would not send an update out Serial 0/0/0 containing the network 10.1.0.0 because R2 learned about that network through Serial 0/0/0.

2.9.7 Link State Routing Algorithm:

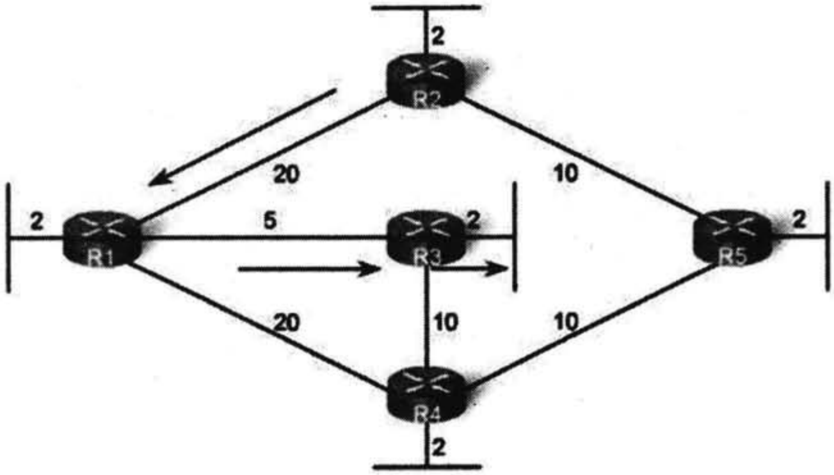
Also known as Shortest path Routing algorithm.

Link states:

Information about the state of (Router interfaces) links is known as link-states. As you can see in the figure,

this information includes:

- The interface's IP address and subnet mask.
- The type of network, such as Ethernet (broadcast) or Serial point-to-point link.
- The cost of that link.
- Any neighbor routers on that link.



Shortest Path for host on R2 LAN to reach host on R3 LAN:
R2 to R1 (20) + R1 to R3 (5) + R3 to LAN (2) = 27

Dijkstra's Shortest Path first algorithm

All routers will complete the following generic link-state routing process to reach a state of convergence:

1. **Each router learns about its own links, its own directly connected networks.** This is done by detecting that an interface is in the up state.

2. **Each router is responsible for meeting its neighbors on directly connected networks.** link state routers do this by exchanging Hello packets with other link-state routers on directly connected networks.

3. **Each router builds a Link-State Packet (LSP) containing the state of each directly connected link.** This is done by recording all the pertinent information about each neighbor, including neighbor ID, link type, and bandwidth.

4. **Each router floods the LSP to all neighbors, who then store all LSPs received in a database.** Neighbors then flood the LSPs to their neighbors until all routers in the area have received the LSPs. Each router stores a copy of each LSP received from its neighbors in a local database.

5. **Each router uses the database to construct a complete map of the topology and computes the best path to each destination network**. Like having a road map, the router now has a complete map of all destinations in the topology and the routes to reach them. The SPF algorithm is used to construct the map of the topology and to determine the best path to each network.

Advantages of Link state Routing protocol:

Build the topological map:

Link-state routing protocols create a topological map, or SPF tree of the network topology. Distance vector routing protocols do not have a topological map of the network.

Faster Convergence:

When receiving a Link- state Packet (LSP), link-state routing protocols immediately flood the LSP out all interfaces except for the interface from which the LSP was received. This way, it achieve the faster convergence. With distance vector routing algorithm, router needs to process each routing update and update its routing table before flooding them out other interfaces.

Event Driven Updates:

After the initial flooding of LSPs, link-state routing protocols only send out an LSP when there is a change in the topology. The LSP contains only the information regarding the affected link. Unlike some distance vector routing protocols, link-state routing protocols do not send periodic updates.

2.9.8 Flow based routing:

A flooding algorithm is an algorithm for distributing material to every part of a connected network. The name derives from the concept of inundation by a flood. Its implemented by the ospf:

Advantages of Flooding

The main advantage of flooding the increased reliability provided by this routing method. Since the message will be sent at least once to every host it is almost guaranteed to reach its destination. In addition, the message will reach the host through the shortest possible path.

Disadvantages of Flooding

There are several disadvantages with this approach to routing. It is very wasteful in terms of the networks total bandwidth. While a message may only have one destination it has to be sent to every host. This increases the maximum load placed upon the network.

Messages can also become duplicated in the network further increasing the load on the networks bandwidth as well as requiring an increase in processing complexity to disregard duplicate messages.

A variant of flooding called *selective flooding* partially addresses these issues by only sending packets to routers in the same direction.

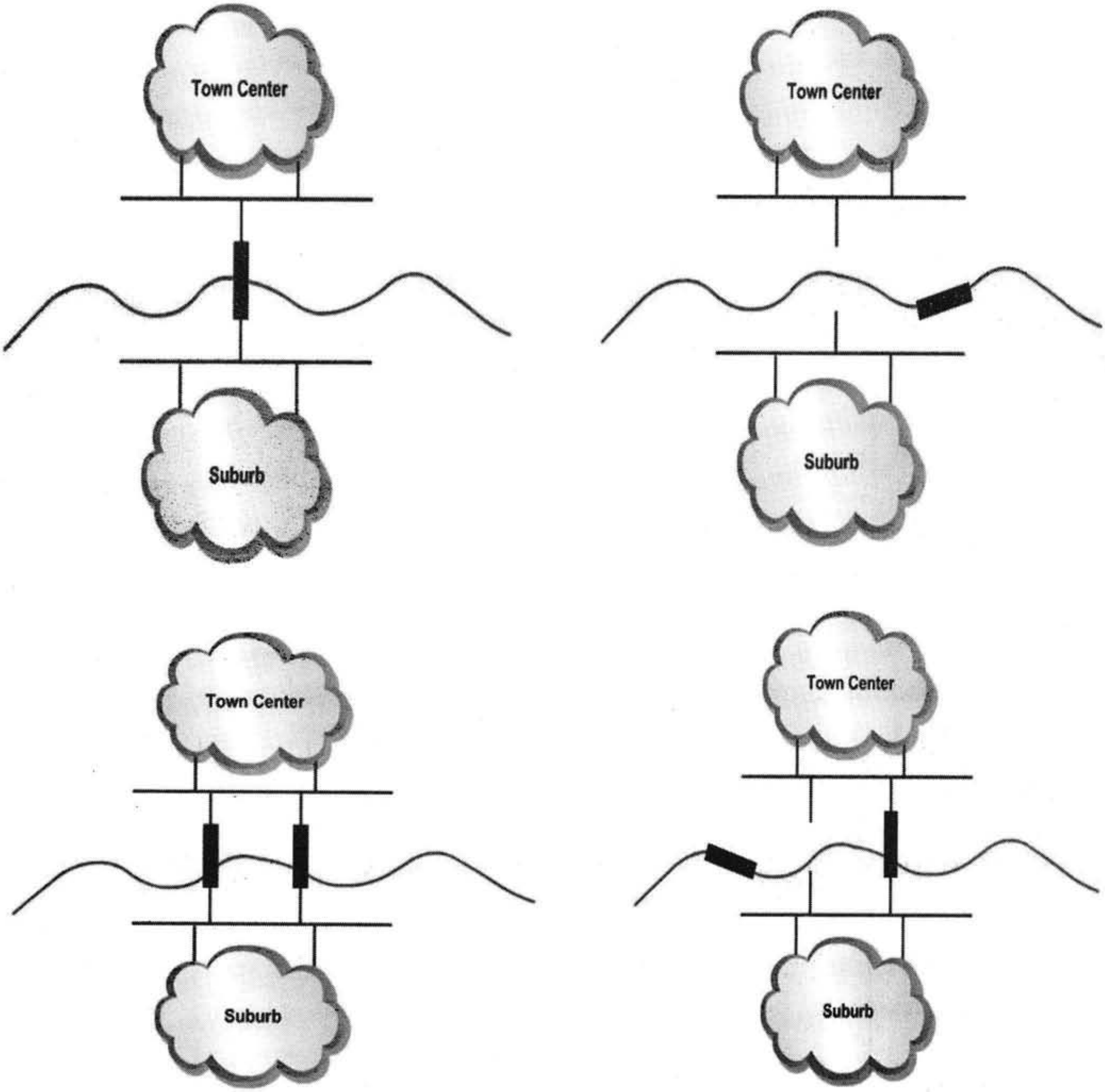
2.9.9 Spanning Tree Protocol(STP)

Need for Redundant Topology:

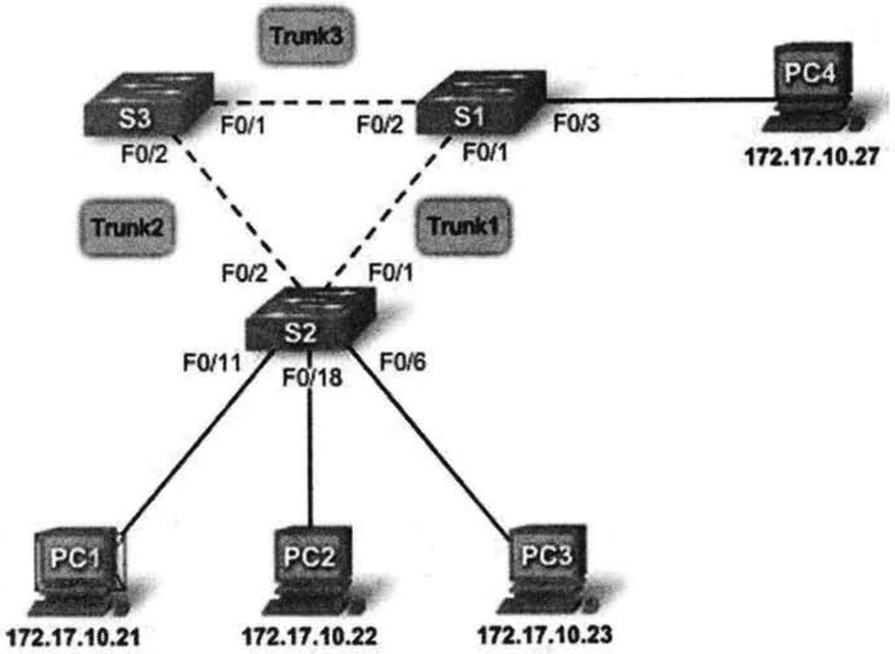
The goal of redundant topologies is to eliminate network outages caused by a single point of failure.

All networks need redundancy for enhanced reliability.

A network of roads is a global example of a redundant topology. If one road is closed for repair, there is likely an alternate route to the destination. Consider a community separated by a river from the town center. If there is only one bridge across the river, there is only one way into town. The topology has no redundancy. If the bridge is flooded or damaged by an accident, travel to the town center across the bridge is impossible. A second bridge across the river creates a redundant topology. The suburb is not cut off from the town center if one bridge is impassable.



Issues with Redundancy:



Layer 2 loops

Ethernet frames do not have a time to live (TTL) like IP packets traversing routers. As a result, if they are not terminated properly on a switched network, they continue to bounce from switch to switch endlessly or until a link is disrupted and breaks the loop.

Broadcast stroms

A broadcast storm occurs when there are so many broadcast frames caught in a Layer 2 loop that all available bandwidth is consumed. Consequently, no bandwidth is available bandwidth for legitimate traffic, and the network becomes unavailable for data communication.

Duplicate unicast frame:

Broadcast frames are not the only type of frames that are affected by loops. Unicast frames sent onto a looped network can result in duplicate frames arriving at the destination device.

Spanning Tree Protocol(STP)

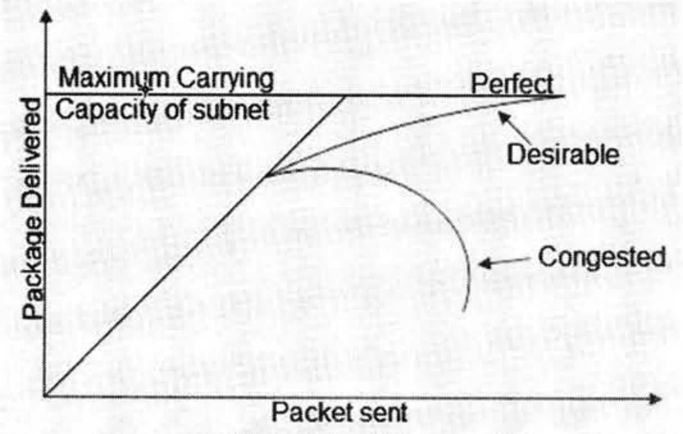
Redundancy increases the availability of the network topology by protecting the network from a single point of failure, such as a failed network cable or switch. When redundancy is introduced into a Layer 2 design, loops and duplicate frames can occur. Loops and duplicate frames can have severe consequences on a network. The **Spanning Tree Protocol (STP)** was developed to address these issues.

STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop. A port is considered blocked when network traffic is prevented from entering or leaving that port. This does not include bridge protocol data unit (BPDU) frames that are used by STP to prevent loops.

Blocking the redundant paths is critical to preventing loops on the network. The physical paths still exist to provide redundancy, but these paths are disabled to prevent the loops from occurring. If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

2.10 Congestion Control Algorithms.

Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network *(i.e.* the number of packets sent to the network) is greater than the capacity of the network *(i.e.* the number of packets a network can handle.)

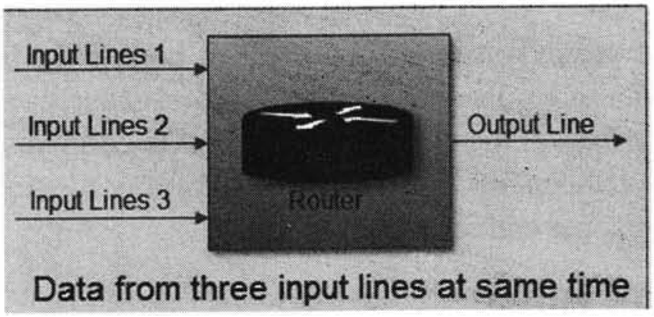


Concept of Congestion

2.10.1 Causing of Congestion:

The various causes of congestion in a subnet are:

- The input traffic rate exceeds the capacity of the output lines. If suddenly, a stream of packet start arriving on three or four input lines and all need the same output line. In this case, a queue will be built up. If there is insufficient memory to hold all the packets, the packet will be lost. Increasing the memory to unlimited size does not solve the problem. This is because, by the time packets reach front of the queue, they have already timed out (as they waited the queue). When timer goes off source transmits duplicate packet that are also added to the queue. Thus same packets are added again and again, increasing the load all the way to the destination

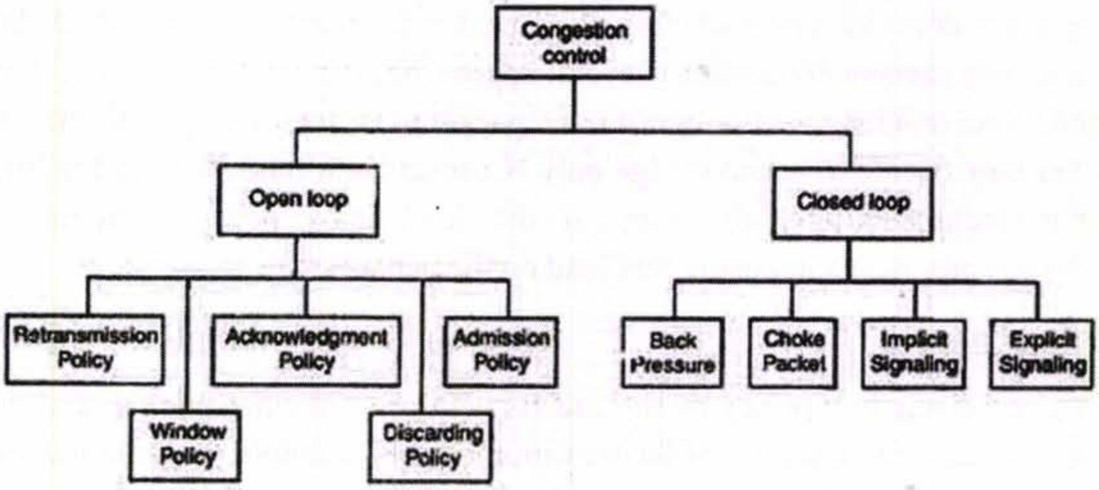


- The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).
- The routers' buffer is too limited.
- Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table etc slowly. As a result of this, queues are built up even though there is excess line capacity.
- Congestion is also caused by slow links. This problem will be solved when high speed links are used. But it is not always the case. Sometimes increase in link bandwidth can further deteriorate the congestion problem as higher speed links may make the network more unbalanced.Congestion can make itself worse. If a route!" does not have free buffers, it start ignoring/discarding the newly arriving packets. When these packets are discarded, the sender may retransmit them after the timer goes off. Such packets are transmitted by the sender again and again until the source gets the acknowledgement of these packets. Therefore multiple transmissions of packets will force the congestion to take place at the sending end.

2.10.2 How to correct the Congestion Problem:

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories:

open-loop congestion control (prevention) and closed-loop congestion control (removal) as shown in Figure.



Types of Congestion Control Methods

2.10.3 Open-Loop Congestion Control

In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. We give a brief list of policies that can prevent congestion.

Retransmission Policy

Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion. The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion. For example, the retransmission policy used by TCP (explained later) is designed to prevent or alleviate congestion.

Window Policy

The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-Nwindow for congestion control. In the Go-Back-N window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver. This duplication may make the congestion worse. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

Acknowledgment Policy

The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. Several approaches are used in this case. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires. A receiver may decide to acknowledge only N packets at a time. We need to know that the acknowledgments are also part of the load in a network. Sending fewer acknowledgments means imposing less load on the network.

Discarding Policy

A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission. For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.

Admission Policy

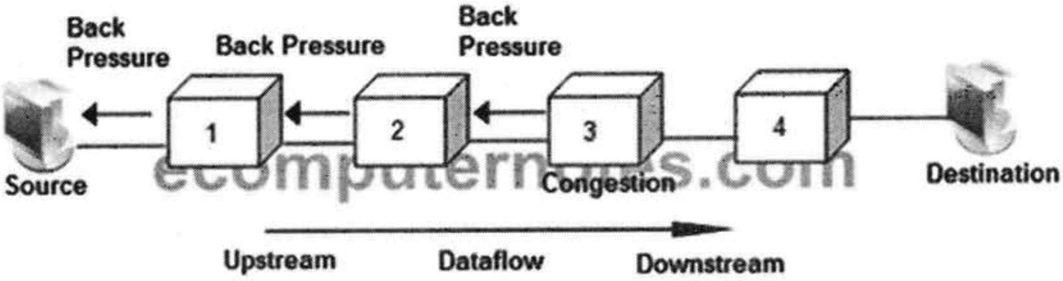
An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtualcircuit connection ifthere is congestion in the network or ifthere is a possibility offuture congestion.

2.10.4 Closed-Loop Congestion Control

Closed-loop congestion control mechanisms try to alleviate congestion after it happens. Several mechanisms have been used by different protocols. We describe a few of them here.

Backpressure

The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes. And so on. Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source. The backpressure technique can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is corning.



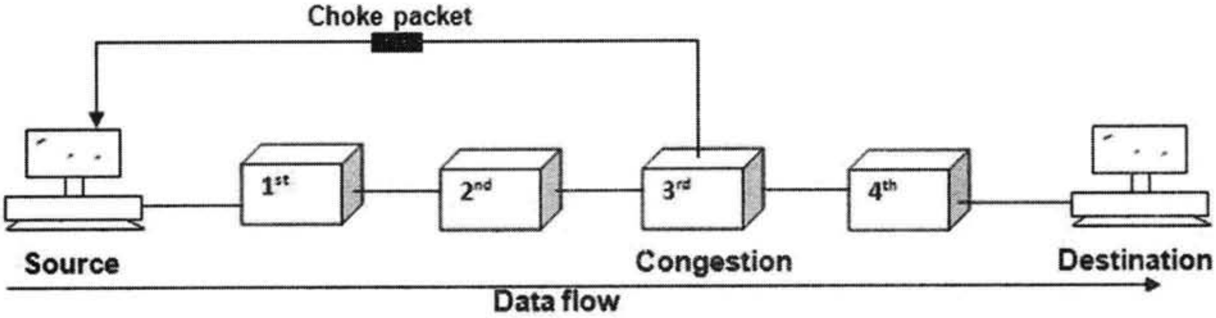
Backpressure Method

Node III in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node II to slow down. Node II, in turn, may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which in turn may create congestion.

If so, node I informs the source of data to slow down. This, in time, alleviates the congestion. Note that the pressure on node III is moved backward to the source to remove the congestion. None of the virtual-circuit networks we studied in this book use backpressure. It was, however, implemented in the first virtual-circuit network, X.25. The technique cannot be implemented in a datagram network because in this type of network, a node (router) does not have the slightest knowledge of the upstream router.

Choke Packet

A choke packet is a packet sent by a node to the source to inform it of congestion. Note the difference between the backpressure and choke packet methods. In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has travelled are not warned.



We have seen an example of this type of control in ICMP. When a router in the Internet is overwhelmed with IP datagram, it may discard some of them; but it informs the source host, using a source quench ICMP message. The warning message goes directly to the source station; the intermediate routers, and does not take any action.

Implicit Signaling

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down. We will see this type of signaling when we discuss TCP congestion control later in the chapter.

Explicit Signaling

The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signaling method, the signal is included in the packets that carry data. Explicit signaling, as we will see in Frame Relay congestion control, can occur in either the forward or the backward direction.

- Backward Signaling: A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.
- Forward Signaling: A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the i congestion.

2.10.5 Congestion control algorithms

Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network. Two techniques can shape traffic: leaky bucket and token bucket.

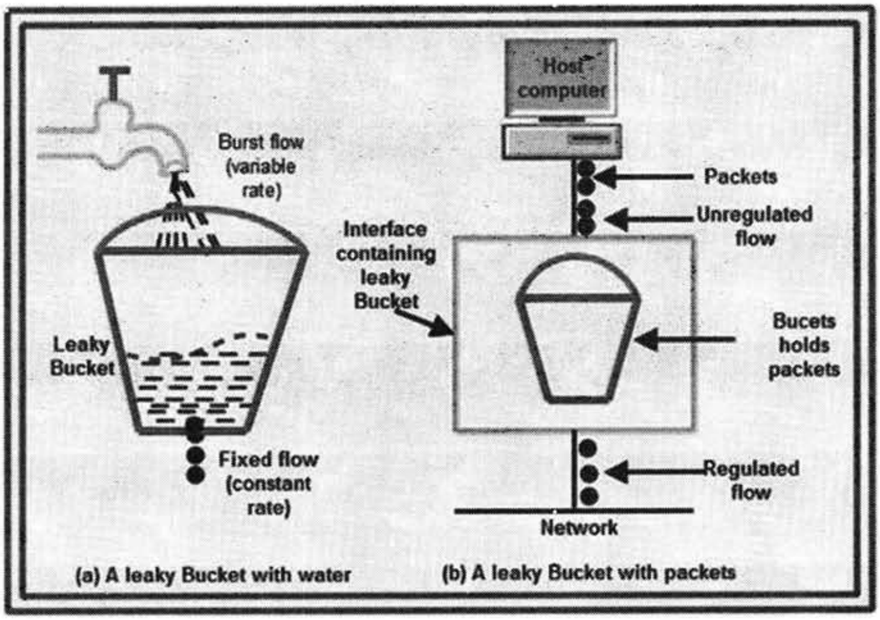
1. Leaky Bucket Algorithm

- It is a traffic shaping mechanism that controls the amount and the rate of the traffic sent to the network.

- A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate.

- Imagine a bucket with a small hole at the bottom.

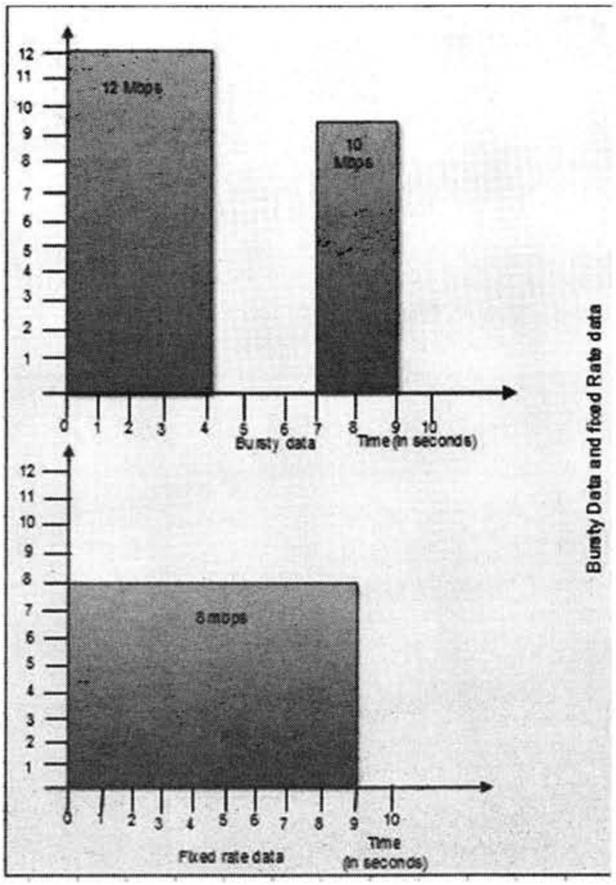
- The rate at which the water is poured into the bucket is not fixed and can vary but it leaks from the bucket at a constant rate. Thus (as long as water is present in bucket), the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.


Burst flow (variable rate)
Leaky Bucket
Fixed flow (constant rate)
Interface containing leaky Bucket
Host computer
Packets
Unregulated flow
Bucets holds packets
Regulated flow
Network
(a) A leaky Bucket with water
(b) A leaky Bucket with packets

- Also, when the bucket is full, any additional water that enters into the bucket spills over the sides and is lost.

- The same concept can be applied to packets in the network. Consider that data is coming from the source at variable speeds. Suppose that a source sends data at 12 Mbps for 4 seconds. Then there is no data for 3 seconds. The source again transmits data at a rate of 10 Mbps for 2 seconds. Thus, in a time span of 9 seconds, 68 Mb data has been transmitted.

If a leaky bucket algorithm is used, the data flow will be 8 Mbps for 9 seconds. Thus constant flow is maintained.



2. Token bucket Algorithm

- The leaky bucket algorithm allows only an average (constant) rate of data flow. Its major problem is that it cannot deal with bursty data.

- A leaky bucket algorithm does not consider the idle time of the host. For example, if the host was idle for 10 seconds and now it is willing to sent data at a very high speed for another 10 seconds, the total data transmission will be divided into 20 seconds and average data rate will be maintained. The host is having no advantage of sitting idle for 10 seconds.

- To overcome this problem, a token bucket algorithm is used. A token bucket algorithm allows bursty data transfers.

- A token bucket algorithm is a modification of leaky bucket in which leaky bucket contains tokens.

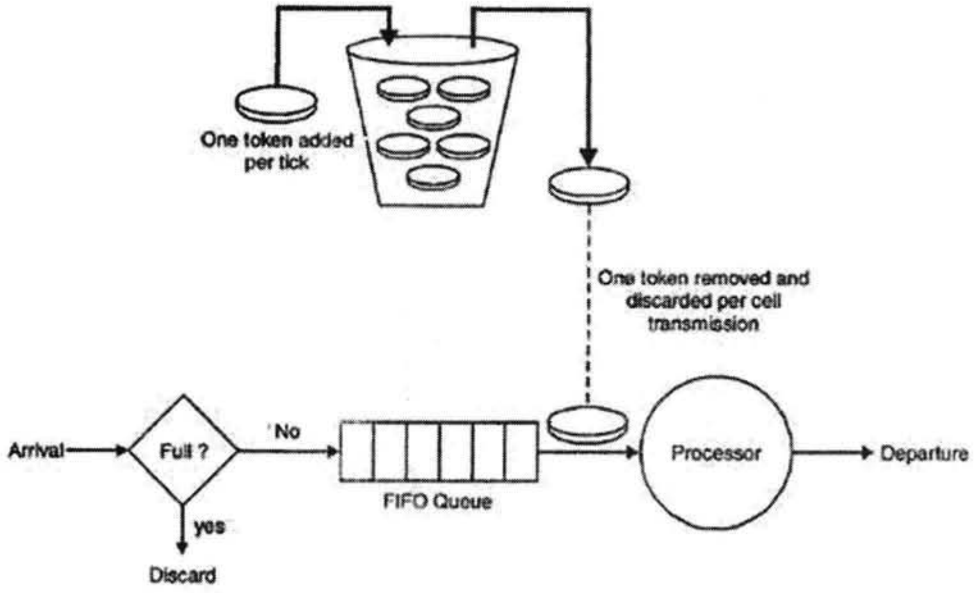
- In this algorithm, a token(s) are generated at every clock tick. For a packet to be transmitted, system must remove token(s) from the bucket.

- Thus, a token bucket algorithm allows idle hosts to accumulate credit for the future in form of tokens.

- For example, if a system generates 100 tokens in one clock tick and the host is idle for 100 ticks. The bucket will contain 10,000 tokens.

Now, if the host wants to send bursty data, it can consume all 10,000 tokens at once for sending 10,000 cells or bytes.

Thus a host can send bursty data as long as bucket is not empty.



Token bucket algorithm

Review questions

3. Explain the following error detecting / correcting mechanisms i. Parity bit ii. Check sum iii. Cyclic Redundancy check iv. Hamming code
4. Explain various multiple access techniques.
5. Explain how congestion control is achieved in TCP, discuss the various mechanism involved.
6. Explain in detail the sliding window protocol.
7. Discuss the various issues in the data link layer.
8. Describe leaky bucket algorithm with suitable example.
9. What are the various routing algorithm? Explain them.
10. Illustrate the dynamic channel allocation problem.
11. Mention the design issues in Network layer.
12. Differentiate datagram packet switching and virtual circuit packet switching.

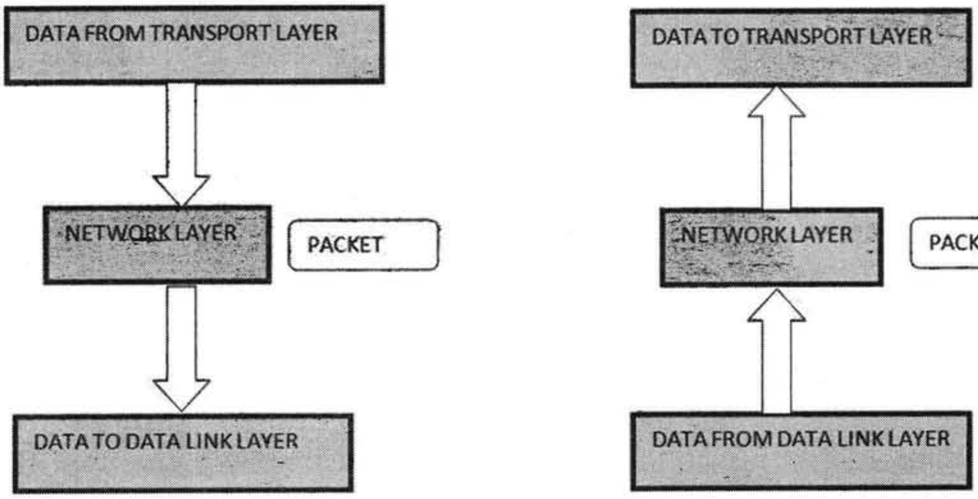
UNIT-III

NETWORK LAYER

3.1 Network Layer:

The main aim of this layer is to deliver packets from source to destination across multiple links (networks). If two computers (system) are connected on the same link then there is no need for a network layer. It routes the signal through different channels to the other end and acts as a network controller.

It also divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels.



FUNCTIONS OF NETWORK LAYER:

1. It translates logical network address into physical address. Concerned with circuit, message or packet switching.
2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
3. Connection services are provided including network layer flow control, network layer error control and packet sequence control.
4. Breaks larger packets into small packets.
5.

3.2 IP Protocol

Internet Protocol is connectionless and unreliable protocol. It ensures no guarantee of successfully transmission of data.

In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

Internet protocol transmits the data in form of a datagram as shown in the following diagram:

4 8 16 32 bits

<table>
<tr><td>VER</td><td>HLEN</td><td>D.S. type of service</td><td colspan="2">Total length of 16 bits</td></tr>
<tr><td colspan="3">Identification of 16 bits</td><td>Flags
3 bits</td><td>Fragmentation Offset (13 bits)</td></tr>
<tr><td colspan="2">Time to live</td><td>Protocol</td><td colspan="2">Header checksum (16 bits)</td></tr>
<tr><td colspan="5">Source IP address</td></tr>
<tr><td colspan="5">Destination IP address</td></tr>
<tr><td colspan="5">Option + Padding</td></tr>
</table>

Points to remember:

- The length of datagram is variable.
- The Datagram is divided into two parts: header and data.
- The length of header is 20 to 60 bytes.
- The header contains information for routing and delivery of the packet.

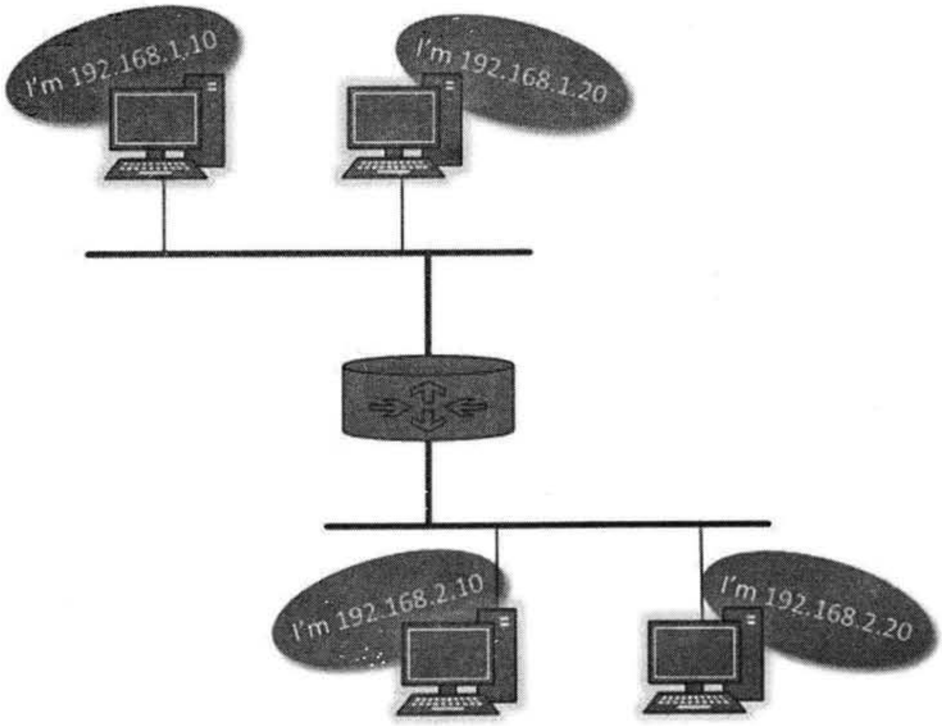
3.2 IP Address

Layer 3 network addressing is one of the major tasks of Network Layer. Network Addresses are always logical i.e. these are software based addresses which can be changed by appropriate configurations.

A network address always points to host / node / server or it can represent a whole network. Network address is always configured on network interface card and is generally mapped by system with the MAC address (hardware address or layer-2 address) of the machine for Layer-2 communication.

There are different kinds of network addresses in existence:

- IP
- IPX
- AppleTalk



IP addressing provides mechanism to differentiate between hosts and network. Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network. The host which needs to communicate outside its subnet, needs to know destination network address, where the packet/data is to be sent.

Hosts in different subnet need a mechanism to locate each other. This task can be done by DNS. DNS is a server which provides Layer-3 address of remote host mapped with its domain name or FQDN. When a host acquires the Layer-3 Address (IP Address) of the remote host, it forwards all its packet to its gateway. A gateway is a router equipped with all the information which leads to route packets to the destination host.

Routers take help of routing tables, which has the following information:

- Address of destination network
- Method to reach the network

Routers upon receiving a forwarding request, forwards packet to its next hop (adjacent router) towards the destination.

The next router on the path follows the same thing and eventually the data packet reaches its destination.

Network address can be of one of the following:

- Unicast (destined to one host)
- Multicast (destined to group)
- Broadcast (destined to all)
- Anycast (destined to nearest one)

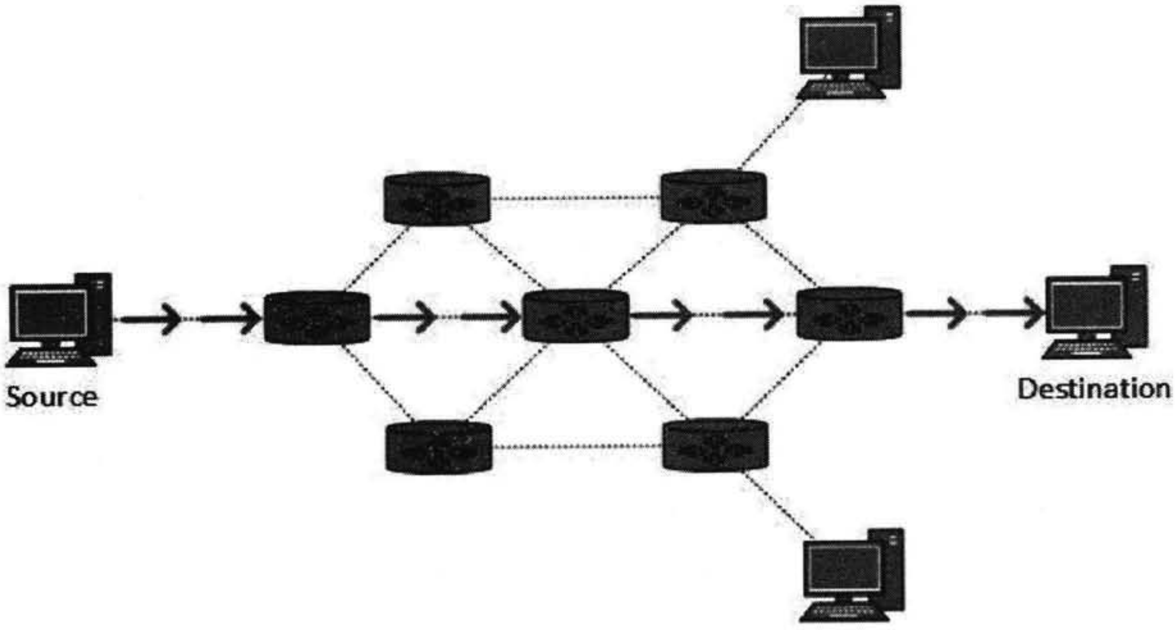
A router never forwards broadcast traffic by default. Multicast traffic uses special treatment as it is most a video stream or audio with highest priority. Anycast is just similar to unicast, except that the packets are delivered to the nearest destination when multiple destinations are available.

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes. The software based routers have limited functionality and limited scope.

3.3.1 Unicast routing

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing.

It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.

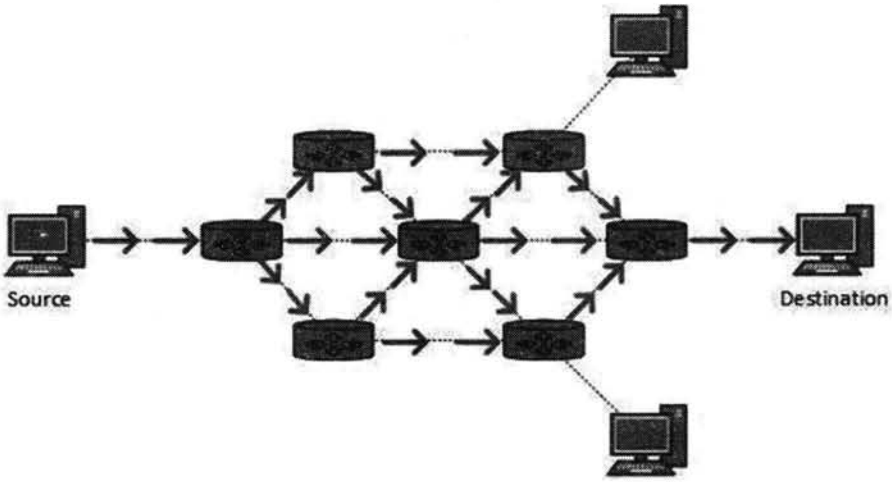


3.3.2 Broadcast routing

By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

Broadcast routing can be done in two ways (algorithm):

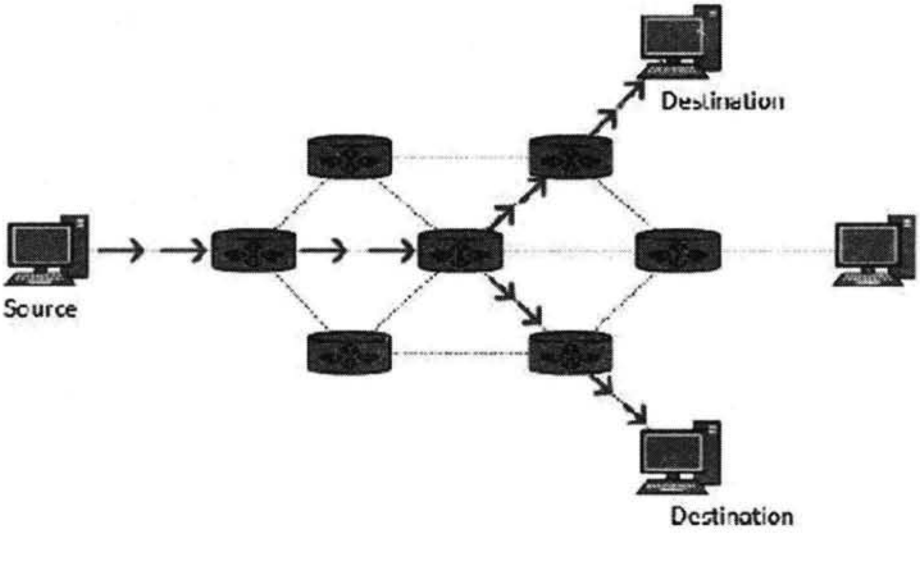
- A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting.
- This method consumes lots of bandwidth and router must destination address of each node.
- Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.



- This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers.
- Reverse path forwarding is a technique, in which router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect and discard duplicates.

3.3.3 Multicast Routing

Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.



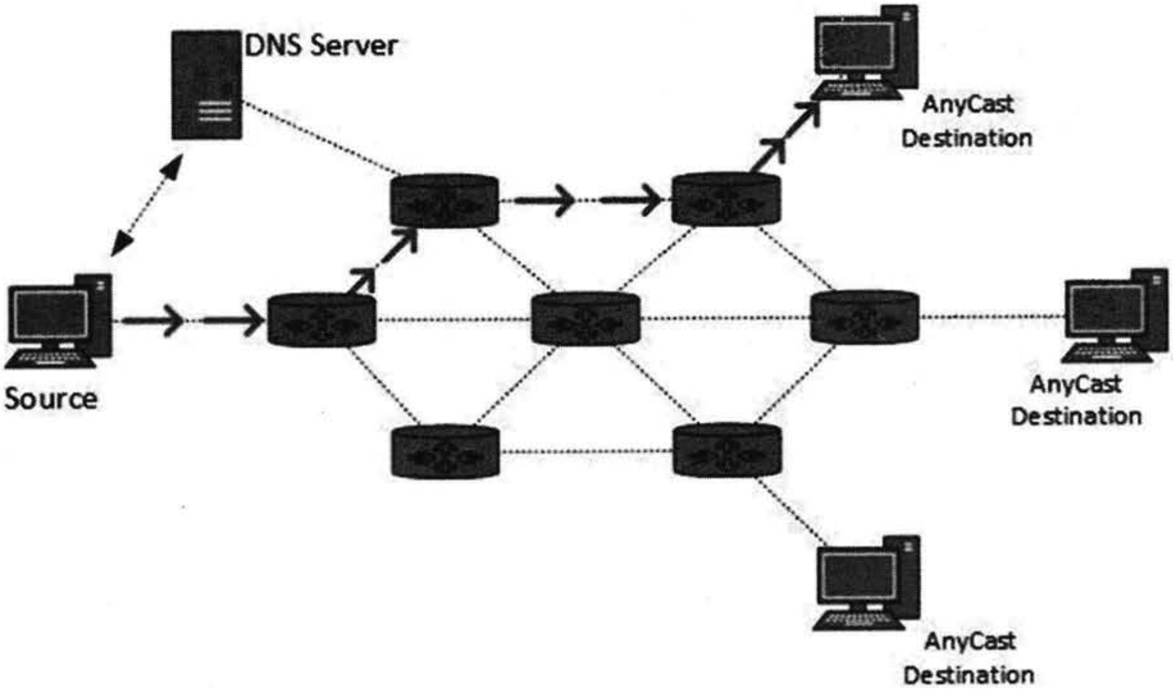
The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.

Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops.

3.3.4 Anycast Routing

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in routing topology.

Anycast routing is done with help of DNS server. Whenever an Anycast packet is received it is enquired with DNS to where to send it. DNS provides the IP address which is the nearest IP configured on it.



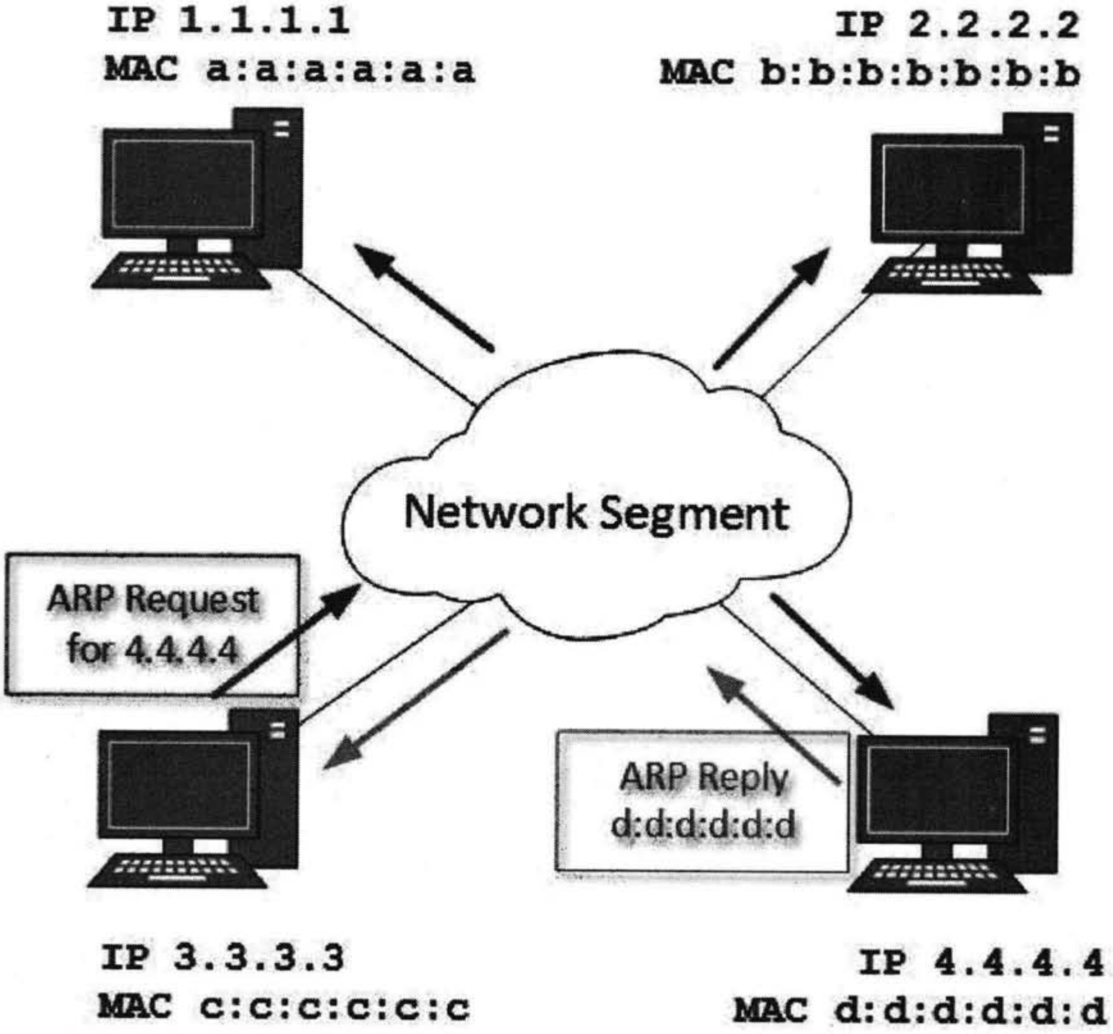
3.4Internet Control Protocol.

Every computer in a network has an IP address by which it can be uniquely identified and addressed. An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time and another IP at some different time.

3.4.1 Address Resolution Protocol (ARP)

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.



To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, "Who has this IP address?" Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

3.4.2 Internet Control Message Protocol (ICMP)

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP. ICMP contains dozens of diagnostic and error reporting messages.

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.

Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A:** It uses first octet for network addresses and last three octets for host addressing.
- **Class B:** It uses first two octets for network addresses and last two for host addressing.
- **Class C:** It uses first three octets for network addresses and last one for host addressing.

- **Class D:** It provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E:** It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.

Internet Protocol Version 6 (IPv6)

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6-equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6-enabled networks to speak and roam around different networks easily on IPv4. These are:

- Dual stack implementation
- Tunneling
- NAT-PT

3.3 Transport Layer

Next Layer in OSI Model is recognized as Transport Layer (Layer-4). All modules and procedures pertaining to transportation of data or data stream are categorized into this layer. As all other layers, this layer communicates with its peer Transport layer of the remote host.

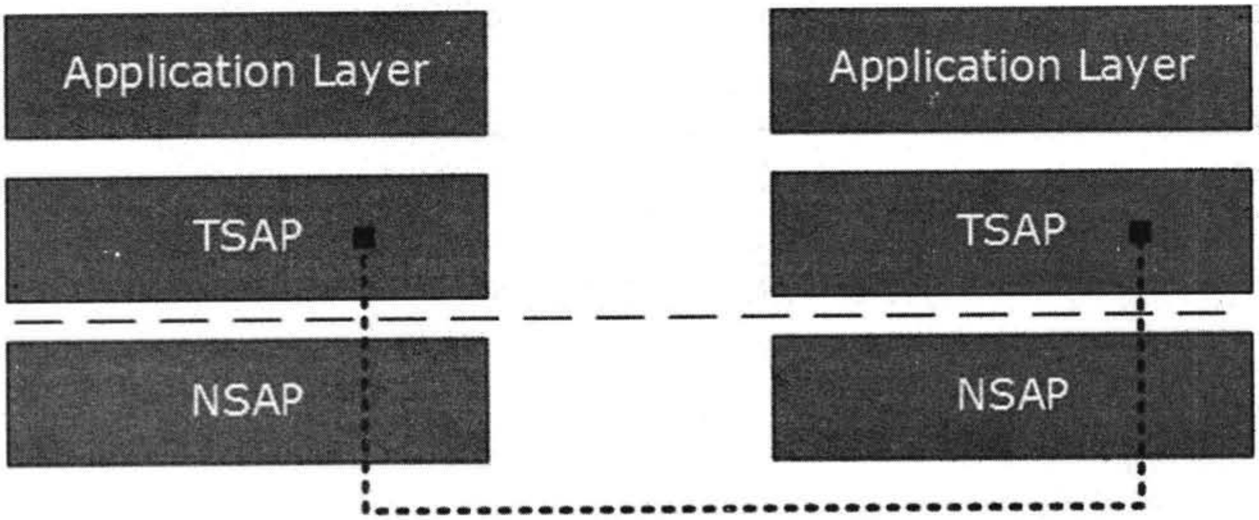
Transport layer offers peer-to-peer and end-to-end connection between two processes on remote hosts. Transport layer takes data from upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to lower layer (Network Layer) for delivery.

Functions

- ❖ This Layer is the first one which breaks the information data, supplied by Application layer in to smaller units called segments. It numbers every byte in the segment and maintains their accounting.
- ❖ This layer ensures that data must be received in the same sequence in which it was sent.
- ❖ This layer provides end-to-end delivery of data between hosts which may or may not belong to the same subnet.
- ❖ All server processes intend to communicate over the network are equipped with well-known Transport Service Access Points (TSAPs) also known as port numbers.

3.5.1 End-to-End Communication

A process on one host identifies its peer host on remote network by means of TSAPs, also known as Port numbers. TSAPs are very well defined and a process which is trying to communicate with its peer knows this in advance.



For example, when a DHCP client wants to communicate with remote DHCP server, it always requests on port number 67. When a DNS client wants to communicate with remote DNS server, it always requests on port number 53 (UDP).

3.4 Design Issues

The transport layer delivers the message from one process to another process running on two different hosts. Thus, it has to perform number of functions to ensure the accurate delivery of message.

The various functions of transport layer are:

- Establishing, Maintaining & Releasing Connection
- Addressing
- Data Transfer
- Flow Control
- Error Control
- Congestion Control

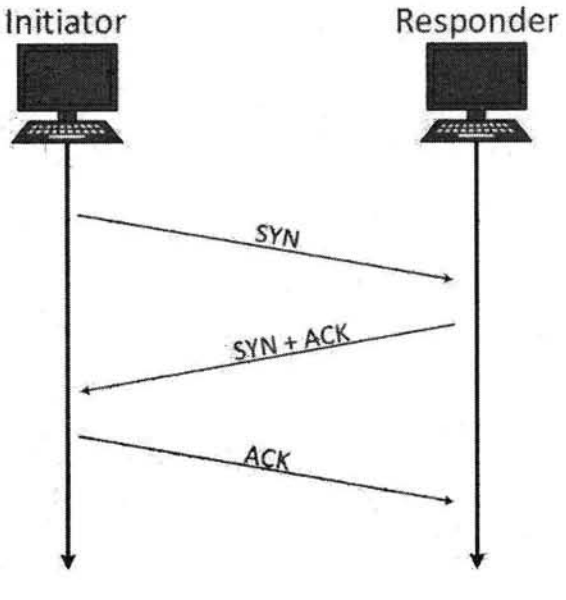
3.6.1 Addressing

TCP communication between two remote hosts is done by means of port numbers (TSAPs). Ports numbers can range from 0 – 65535 which are divided as:

- System Ports (0 – 1023)
- User Ports (1024 – 49151)
- Private/Dynamic Ports (49152 – 65535)

3.6.2 Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.



3.6.3 Establishment

Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

3.6.4 Release

Either of server and client can send TCP segment with FIN flag set to 1. When the receiving end responds it back by ACKnowledging FIN, that direction of TCP communication is closed and connection is released.

3.6.5 Bandwidth Management

TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each successful communication.

For example, the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received the windows size is doubled to 4 and next the segment sent will be 4 data bytes long. When the acknowledgement of 4-byte data segment is received, the client sets windows size to 8 and so on.

If an acknowledgement is missed, i.e. data lost in transit network or it received NACK, then the window size is reduced to half and slow start phase starts again.

3.6.6 Error Control and Flow Control

TCP uses port numbers to know what application process it needs to handover the data segment. Along with that, it uses sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.

If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the TCP timestamp value is compared to make a decision.

3.6.7 Multiplexing

The technique to combine two or more data streams in one session is called Multiplexing. When a TCP client initializes a connection with Server, it always refers to a well-defined port number which indicates the application process. The client itself uses a randomly generated port number from private port number pools.

Using TCP Multiplexing, a client can communicate with a number of different application process in a single session. For example, a client requests a web page which in turn contains different types of data (HTTP, SMTP, FTP etc.) the TCP session timeout is increased and the session is kept open for longer time so that the three-way handshake overhead can be avoided.

This enables the client system to receive multiple connection over single virtual connection. These virtual connections are not good for Servers if the timeout is too long.

3.6.8 Congestion Control

When large amount of data is fed to system which is not capable of handling it, congestion occurs. TCP controls congestion by means of Window mechanism. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:

- Additive increase, Multiplicative Decrease
- Slow Start
- Timeout React

3.6.9 Timer Management

TCP uses different types of timers to control and management various tasks:

Keep-alive timer:

- This timer is used to check the integrity and validity of a connection.
- When keep-alive time expires, the host sends a probe to check if the connection still exists.

Retransmission timer:

- This timer maintains stateful session of data sent.
- If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

Persist timer:

- TCP session can be paused by either host by sending Window Size 0.
- To resume the session a host needs to send Window Size with some larger value.

- If this segment never reaches the other end, both ends may wait for each other for infinite time.
- When the Persist timer expires, the host resends its window size to let the other end know.
- Persist Timer helps avoid deadlocks in communication.

Timed-Wait:

- After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.
- This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
- Timed-out can be a maximum of 240 seconds (4 minutes).

3.6.10 Crash Recovery

TCP is very reliable protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e. when a host receives a packet, it is bound to ACK that packet having the next sequence number expected (if it is not the last segment).

When a TCP Server crashes mid-way communication and re-starts its process, it sends TPDU broadcast to all its hosts. The hosts can then send the last data segment which was never unacknowledged and carry onwards.

3.5 Internet Transport Protocol (TCP).

3.7.1 Transmission Control Protocol (TCP)

TCP is a connection oriented protocol and offers end-to-end packet delivery. It acts as back bone for connection.It exhibits the following key features:

- Transmission Control Protocol (TCP) corresponds to the Transport Layer of OSI Model.
- TCP is a reliable and connection oriented protocol.
- TCP offers:
    - Stream Data Transfer.
    - Reliability.

    - Efficient Flow Control
    - Full-duplex operation.
    - Multiplexing.
- TCP offers connection oriented end-to-end packet delivery.
- TCP ensures reliability by sequencing bytes with a forwarding acknowledgement number that indicates to the destination the next byte the source expect to receive.
- It retransmits the bytes not acknowledged with in specified time period.

TCP Services

TCP offers following services to the processes at the application layer:

- Stream Delivery Service
- Sending and Receiving Buffers
- Bytes and Segments
- Full Duplex Service
- Connection Oriented Service
- Reliable Service

STREAM DELIVER SERVICE

TCP protocol is stream oriented because it allows the sending process to send data as stream of bytes and the receiving process to obtain data as stream of bytes.

SENDING AND RECEIVING BUFFERS

It may not be possible for sending and receiving process to produce and obtain data at same speed, therefore, TCP needs buffers for storage at sending and receiving ends.

BYTES AND SEGMENTS

The Transmission Control Protocol (TCP), at transport layer groups the bytes into a packet. This packet is called segment. Before transmission of these packets, these segments are encapsulated into an IP datagram.

FULL DUPLEX SERVICE

Transmitting the data in duplex mode means flow of data in both the directions at the same time.

CONNECTION ORIENTED SERVICE

TCP offers connection oriented service in the following manner:

1. TCP of process-1 informs TCP of process – 2 and gets its approval.
2. TCP of process – 1 and TCP of process – 2 and exchange data in both the two directions.
3. After completing the data exchange, when buffers on both sides are empty, the two TCP's destroy their buffers.

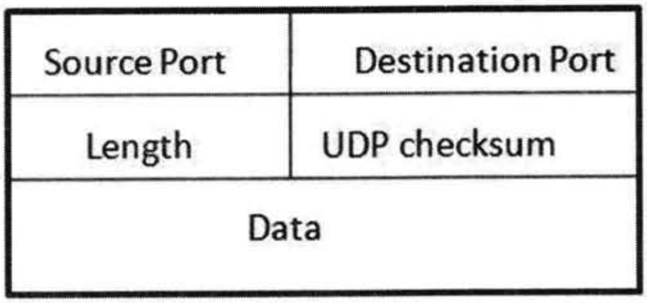
RELIABLE SERVICE

For sake of reliability, TCP uses acknowledgement mechanism.

3.7.2 User Datagram Protocol (UDP)

Like IP, UDP is connectionless and unreliable protocol. It doesn't require making a connection with the host to exchange data. Since UDP is unreliable protocol, there is no mechanism for ensuring that data sent is received.

UDP transmits the data in form of a datagram. The UDP datagram consists of five parts as shown in the following diagram:



<table>
<tr><td>Source Port</td><td>Destination Port</td></tr>
<tr><td>Length</td><td>UDP checksum</td></tr>
<tr><td colspan="2">Data</td></tr>
</table>

Points

- UDP is used by the application that typically transmit small amount of data at one time.

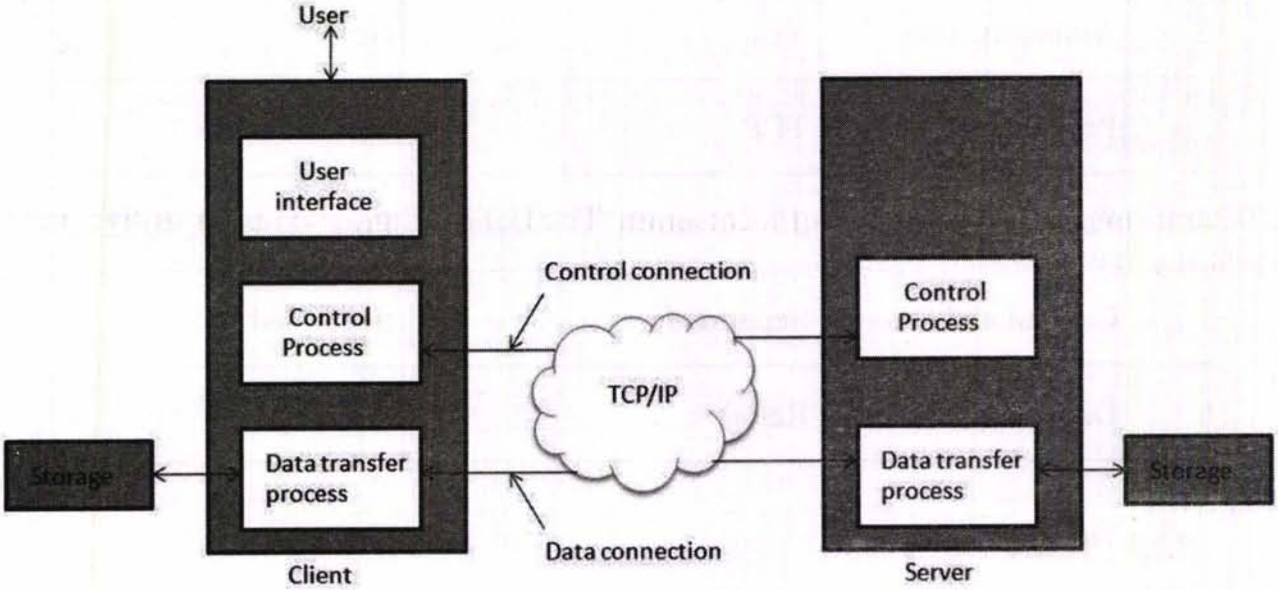
- UDP provides protocol port used i.e. UDP message contains both source and destination port number, that makes it possible for UDP software at the destination to deliver the message to correct application program.

3.7.3 File Transfer Protocol (FTP)

FTP is used to copy files from one host to another. FTP offers the mechanism for the same in following manner:

- FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.
- FTP establishes two different connections: one is for data transfer and other is for control information.
- **Control connection** is made between **control processes** while**Data Connection** is made between<="" b="" style="box-sizing: border-box;">

FTP uses **port 21** for the control connection and **Port 20** for the data connection.



3.7.3 Trivial File Transfer Protocol (TFTP)

Trivial File Transfer Protocol is also used to transfer the files but it transfers the files without authentication. Unlike FTP, TFTP does not separate control and data information. Since there is no authentication exists, TFTP lacks in security features therefore it is not recommended to use TFTP.

Key points

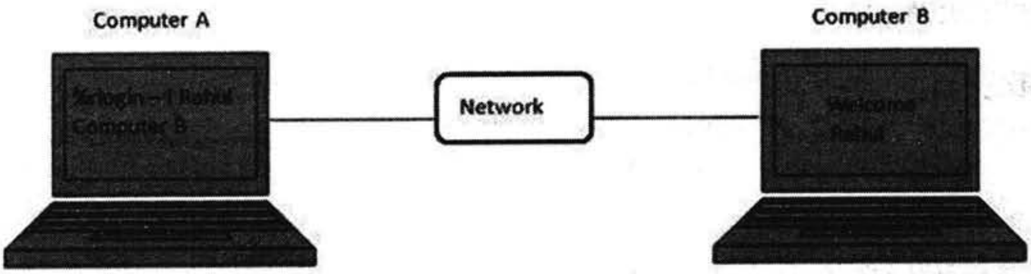
- TFTP makes use of UDP for data transport. Each TFTP message is carried in separate UDP datagram.
- The first two bytes of a TFTP message specify the type of message.
- The TFTP session is initiated when a TFTP client sends a request to upload or download a file.
- The request is sent from an ephemeral UDP port to the **UDP port 69**of an TFTP server.

3.7.4 Difference between FTP and TFTP

S.N.	Parameter	FTP	TFTP
1	Operation	Transferring Files	Transferring Files
2	Authentication	Yes	No
3	Protocol	TCP	UDP
4	Ports	21 – Control, 20 – Data	Port 3214, 69, 4012
5	Control and Data	Separated	Separated
6	Data Transfer	Reliable	Unreliable

3.7.5 Telnet

Telnet is a protocol used to log in to remote computer on the internet. There are a number of Telnet clients having user friendly user interface. The following diagram shows a person is logged in to computer A, and from there, he remote logged into computer B.



3.7.6 Hyper Text Transfer Protocol (HTTP)

HTTP is a communication protocol. It defines mechanism for communication between browser and the web server. It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.

HTTP Request

HTTP request comprises of lines which contains:

- Request line
- Header Fields
- Message body

Key Points

- The first line i.e. the **Request line** specifies the request method i.e.**Get** or **Post.**
- The second line specifies the header which indicates the domain name of the server from where index.htm is retrieved.

HTTP Response

Like HTTP request, HTTP response also has certain structure. HTTP response contains:

- Status line
- Headers
- Message body

Review questions:

1. List the classes in classful addressing and define the application of each class (unicast, multicast, broadcast, or reserve).
2. How can we distinguish a multicast address in IPv4 addressing? How can we do so in IPv6 addressing?
3. What is the difference between connectionless and connection-oriented services? Which type of service is provided byIPv4? Which type of service is provided by IPv6?
4. Explain: (a) ALOHA, (b) CSMA/CD.
5. Compare the TCP header and the UDP header. List the fields in the TCP header that are missing from UDP header. Give the reason for their absence.
6. How are options negotiated in TELNET?
7. Differentiate FTP and TFTP.
8. Describe the Services of TCP.
9. Explain Connection management of the Transport layer in detail.
10. Discuss the Address Resolution Protocol (ARP)

UNIT-IV

NETWORK SECURITY

4.1 Network Security Overview

In this modern era, organizations greatly rely on computer networks to share information throughout the organization in an efficient and productive manner. Organizational computer networks are now becoming large and ubiquitous. Assuming that each staff member has a dedicated workstation, a large scale company would have few thousands workstations and many server on the network.

It is likely that these workstations may not be centrally managed, nor would they have perimeter protection. They may have a variety of operating systems, hardware, software, and protocols, with different level of cyber awareness among users. Now imagine, these thousands of workstations on company network are directly connected to the Internet. This sort of unsecured network becomes a target for an attack which holds valuable information and displays vulnerabilities.

4.1.1 Physical Network

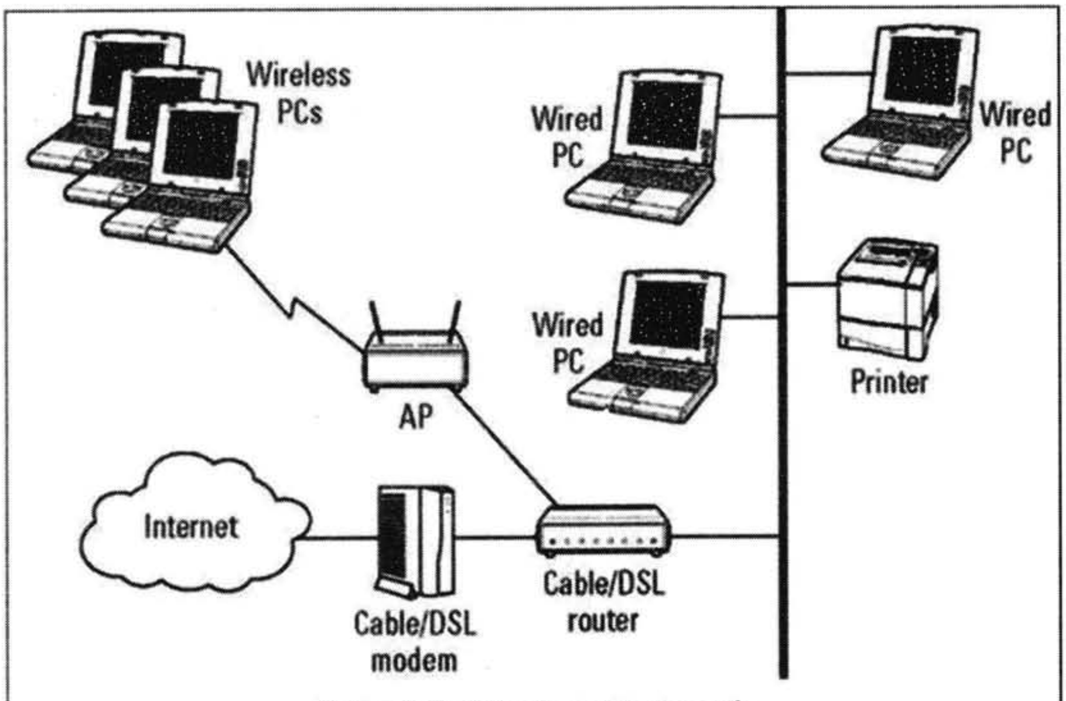
A network is defined as two or more computing devices connected together for sharing resources efficiently. Further, connecting two or more networks together is known as **internetworking**. Thus, the Internet is just an internetwork – a collection of interconnected networks.

For setting up its internal network, an organization has various options. It can use a wired network or a wireless network to connect all workstations. Nowadays, organizations are mostly using a combination of both wired and wireless networks.

Wired & Wireless Networks

In a wired network, devices are connected to each other using cables. Typically, wired networks are based on Ethernet protocol where devices are connected using the Unshielded Twisted Pair (UTP) cables to the different switches. These switches are further connected to the network router for accessing the Internet.

In wireless network, the device is connected to an access point through radio transmissions. The access points are further connected through cables to switch/router for external network access.



Wired & Wireless Network

Wireless networks have gained popularity due to the mobility offered by them. Mobile devices need not be tied to a cable and can roam freely within the wireless network range. This ensures efficient information sharing and boosts productivity.

Vulnerabilities & Attacks

The common vulnerability that exists in both wired and wireless networks is an "unauthorized access" to a network. An attacker can connect his device to a network though unsecure hub/switch port. In this regard, wireless network are considered less secure than wired network, because wireless network can be easily accessed without any physical connection.

After accessing, an attacker can exploit this vulnerability to launch attacks such as

- Sniffing the packet data to steal valuable information.
- Denial of service to legitimate users on a network by flooding the network medium with spurious packets.
- Spoofing physical identities (MAC) of legitimate hosts and then stealing data or further launching a 'man-in-the-middle' attack.

4.1.2 Network Protocol

Network Protocol is a set of rules that govern communications between devices connected on a network. They include mechanisms for making connections, as well as formatting rules for data packaging for messages sent and received.

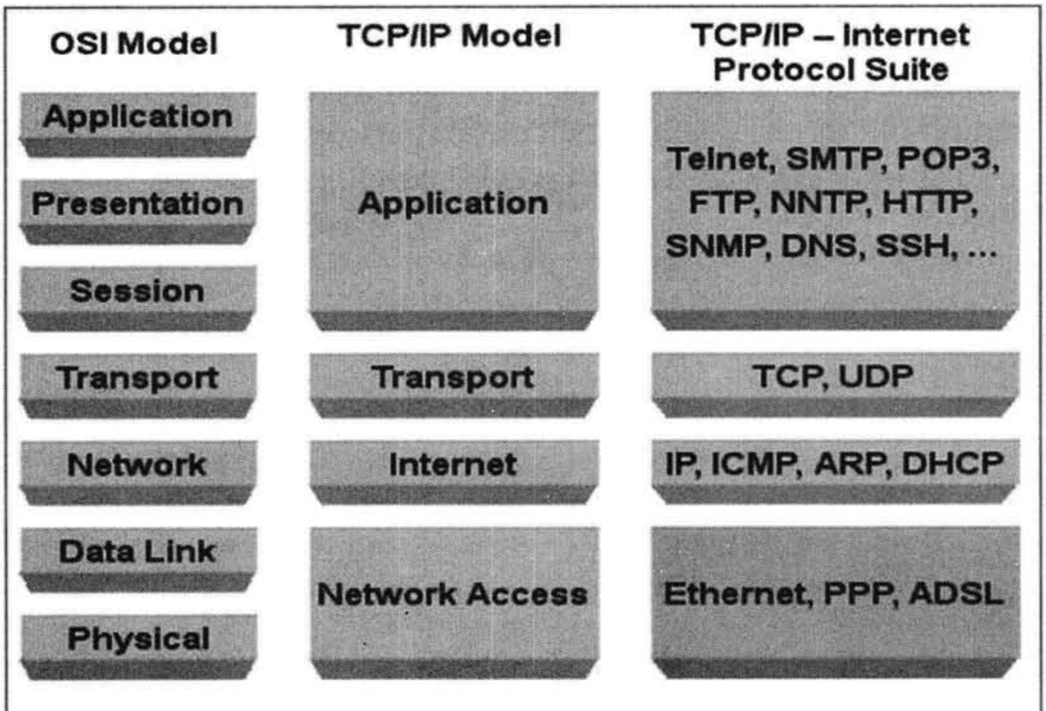
Several computer network protocols have been developed each designed for specific purposes. The popular and widely used protocols are TCP/IP with associated higher- and lower-level protocols.

TCP/IP Protocol

Transmission Control Protocol (TCP) and **Internet Protocol** (IP) are two distinct computer network protocols mostly used together. Due to their popularity and wide adoption, they are built in all operating systems of networked devices.

IP corresponds to the Network layer (Layer 3) whereas TCP corresponds to the Transport layer (Layer 4) in OSI. TCP/IP applies to network communications where the TCP transport is used to deliver data across IP networks.

TCP/IP protocols are commonly used with other protocols such as HTTP, FTP, SSH at application layer and Ethernet at the data link/physical layer.



OSI Model	TCP/IP Model	TCP/IP – Internet Protocol Suite
Application	Application	Telnet, SMTP, POP3, FTP, NNTP, HTTP, SNMP, DNS, SSH, ...
Presentation		
Session		
Transport	Transport	TCP, UDP
Network	Internet	IP, ICMP, ARP, DHCP
Data Link	Network Access	Ethernet, PPP, ADSL
Physical		

TCP/IP Protocol Suite

TCP/IP protocol suite was created in 1980 as an internetworking solution with very little concern for security aspects.

It was developed for a communication in the limited trusted network. However, over a period, this protocol became the de-facto standard for the unsecured Internet communication.

Some of the common security vulnerabilities of TCP/IP protocol suits are –

- HTTP is an application layer protocol in TCP/IP suite used for transfer files that make up the web pages from the web servers. These transfers are done in plain text and an intruder can easily read the data packets exchanged between the server and a client.

- Another HTTP vulnerability is a weak authentication between the client and the web server during the initializing of the session. This vulnerability can lead to a session hijacking attack where the attacker steals an HTTP session of the legitimate user.

- TCP protocol vulnerability is three-way handshake for connection establishment. An attacker can launch a denial of service attack "SYN-flooding" to exploit this vulnerability. He establishes lot of half-opened sessions by not completing handshake. This leads to server overloading and eventually a crash.

- IP layer is susceptible to many vulnerabilities. Through an IP protocol header modification, an attacker can launch an IP spoofing attack.

Apart from the above-mentioned, many other security vulnerabilities exist in the TCP/IP Protocol family in design as well in its implementation.

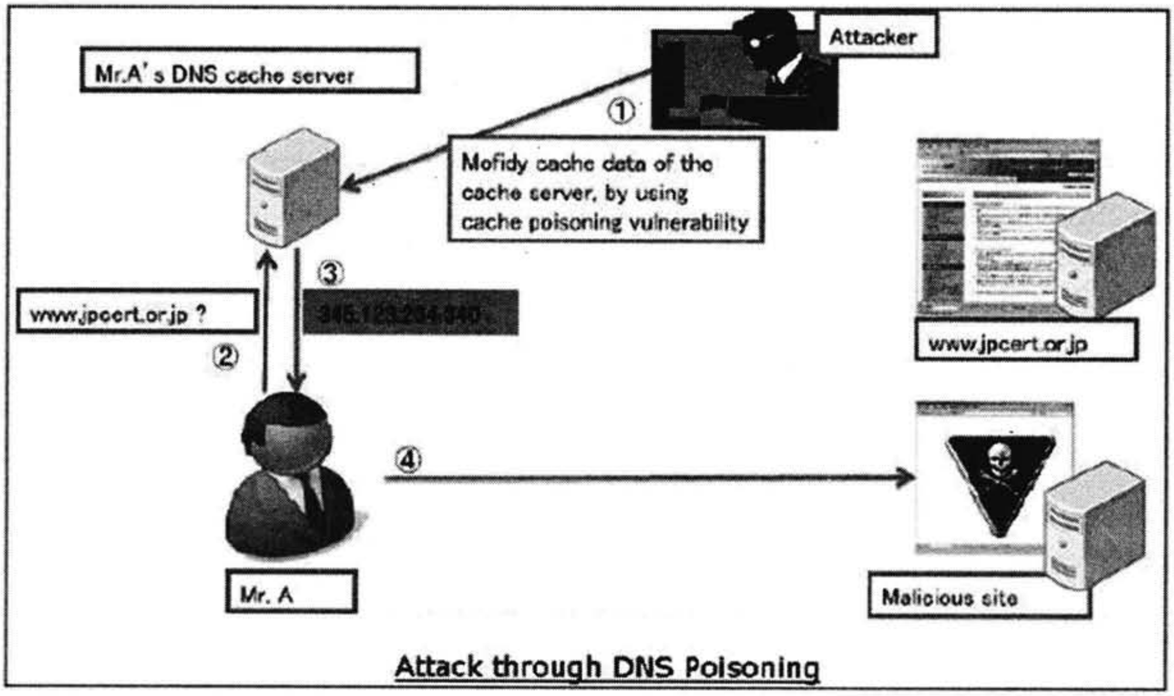
Incidentally, in TCP/IP based network communication, if one layer is hacked, the other layers do not become aware of the hack and the entire communication gets compromised. Hence, there is need to employ security controls at each layer to ensure foolproof security.

4.1.3 DNS Protocol

Domain Name System (DNS) is used to resolve host domain names to IP addresses. Network users depend on DNS functionality mainly during browsing the Internet by typing a URL in the web browser.

In an attack on DNS, an attacker's aim is to modify a legitimate DNS record so that it gets resolved to an incorrect IP address. It can direct all traffic for that IP to the wrong computer. An attacker can either exploit DNS protocol vulnerability or compromise the DNS server for materializing an attack.

DNS cache poisoning is an attack exploiting a vulnerability found in the DNS protocol. An attacker may poison the cache by forging a response to a recursive DNS query sent by a resolver to an authoritative server. Once, the cache of DNS resolver is poisoned, the host will get directed to a malicious website and may compromise credential information by communication to this site.



Attack through DNS Poisoning

4.1.4 ICMP Protocol

Internet Control Management Protocol (ICMP) is a basic network management protocol of the TCP/IP networks. It is used to send error and control messages regarding the status of networked devices.

ICMP is an integral part of the IP network implementation and thus is present in very network setup. ICMP has its own vulnerabilities and can be abused to launch an attack on a network.

The common attacks that can occur on a network due to ICMP vulnerabilities are –

- ICMP allows an attacker to carry out network reconnaissance to determine network topology and paths into the network. ICMP sweep involves discovering all host IP addresses which are alive in the entire target's network.

- Trace route is a popular ICMP utility that is used to map target networking by describing the path in real-time from the client to the remote host.

- An attacker can launch a denial of service attack using the ICMP vulnerability. This attack involves sending IPMP ping packets that exceeds 65,535 bytes to the target device. The target computer fails to handle this packet properly and can cause the operating system to crush.

Other protocols such as ARP, DHCP, SMTP, etc. also have their vulnerabilities that can be exploited by the attacker to compromise the network security. We will discuss some of these vulnerabilities in later chapters.

The least concern for the security aspect during design and implementation of protocols has turned into a main cause of threats to the network security.

4.1.5 Goals of Network Security

During transmission, data is highly vulnerable to attacks. An attacker can target the communication channel, obtain the data, and read the same or re-insert a false message to achieve his nefarious aims.

Network security is not only concerned about the security of the computers at each end of the communication chain; however, it aims to ensure that the entire network is secure.

Network security entails protecting the usability, reliability, integrity, and safety of network and data. Effective network security defeats a variety of threats from entering or spreading on a network.

The primary goal of network security are Confidentiality, Integrity, and Availability. These three pillars of Network Security are often represented as **CIA triangle**.

- **Confidentiality** – The function of confidentiality is to protect precious business data from unauthorized persons. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons.

- **Integrity** – This goal means maintaining and assuring the accuracy and consistency of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.
- **Availability** – The function of availability in Network Security is to make sure that the data, network resources/services are continuously available to the legitimate users, whenever they require it.

Achieving Network Security

Ensuring network security may appear to be very simple. The goals to be achieved seems to be straightforward. But in reality, the mechanisms used to achieve these goals are highly complex, and understanding them involves sound reasoning.

International Telecommunication Union (ITU), in its recommendation on security architecture X.800, has defined certain mechanisms to bring the standardization in methods to achieve network security. Some of these mechanisms are –

- **En-cipherment** – This mechanism provides data confidentiality services by transforming data into not-readable forms for the unauthorized persons. This mechanism uses encryption-decryption algorithm with secret keys.
- **Digital signatures** – This mechanism is the electronic equivalent of ordinary signatures in electronic data. It provides authenticity of the data.
- **Access control** – This mechanism is used to provide access control services. These mechanisms may use the identification and authentication of an entity to determine and enforce the access rights of the entity.

Having developed and identified various security mechanisms for achieving network security, it is essential to decide where to apply them; both physically (at what location) and logically (at what layer of an architecture such as TCP/IP).

Security Mechanisms at Networking Layers

Several security mechanisms have been developed in such a way that they can be developed at a specific layer of the OSI network layer model.

- **Security at Application Layer** – Security measures used at this layer are application specific. Different types of application would need separate security measures. In order to ensure application layer security, the applications need to be modified.

It is considered that designing a cryptographically sound application protocol is very difficult and implementing it properly is even more challenging. Hence, application layer security mechanisms for protecting network communications are preferred to be only standards-based solutions that have been in use for some time.

An example of application layer security protocol is Secure Multipurpose Internet Mail Extensions (S/MIME), which is commonly used to encrypt e-mail messages. DNSSEC is another protocol at this layer used for secure exchange of DNS query messages.

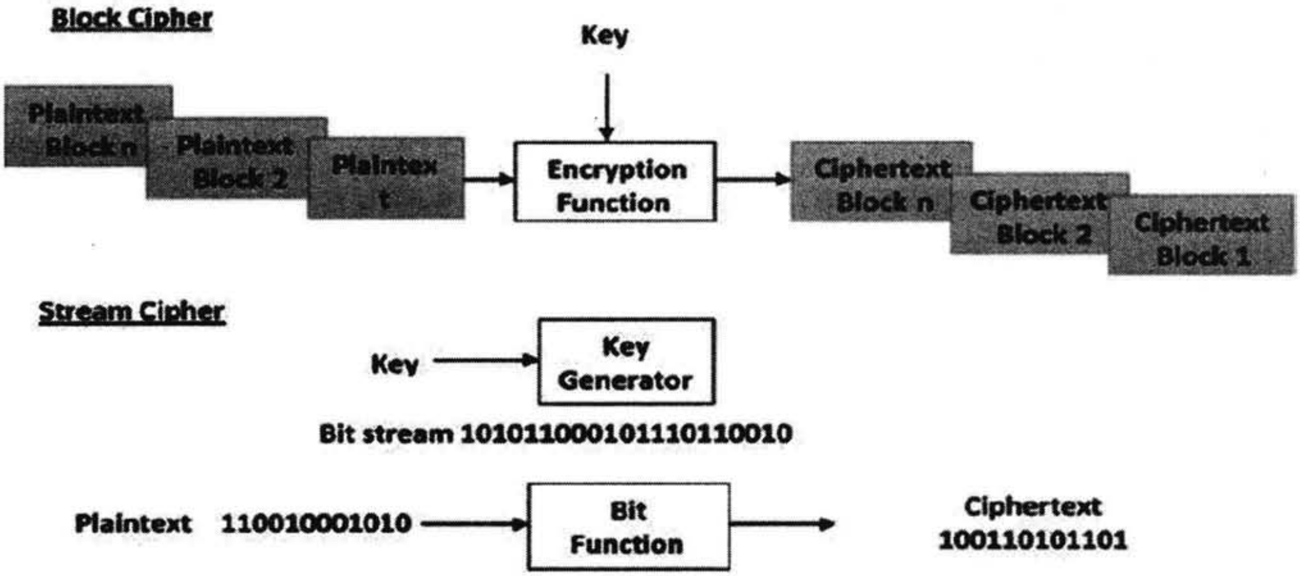
- **Security at Transport Layer** – Security measures at this layer can be used to protect the data in a single communication session between two hosts. The most common use for transport layer security protocols is protecting the HTTP and FTP session traffic. The Transport Layer Security (TLS) and Secure Socket Layer (SSL) are the most common protocols used for this purpose.
- **Network Layer** – Security measures at this layer can be applied to all applications; thus, they are not application-specific. All network communications between two hosts or networks can be protected at this layer without modifying any application. In some environments, network layer security protocol such as Internet Protocol Security (IPsec) provides a much better solution than transport or application layer controls because of the difficulties in adding controls to individual applications. However, security protocols at this layer provides less communication flexibility that may be required by some applications.

Incidentally, a security mechanism designed to operate at a higher layer cannot provide protection for data at lower layers, because the lower layers perform functions of which the higher layers are not aware. Hence, it may be necessary to deploy multiple security mechanisms for enhancing the network security.

4.2 Symmetric Ciphers

Digital data is represented in strings of binary digits (bits) unlike alphabets. Modern cryptosystems need to process this binary string to convert in to another binary string. Based on how these binary strings are processed, a symmetric encryption schemes can be classified in to –

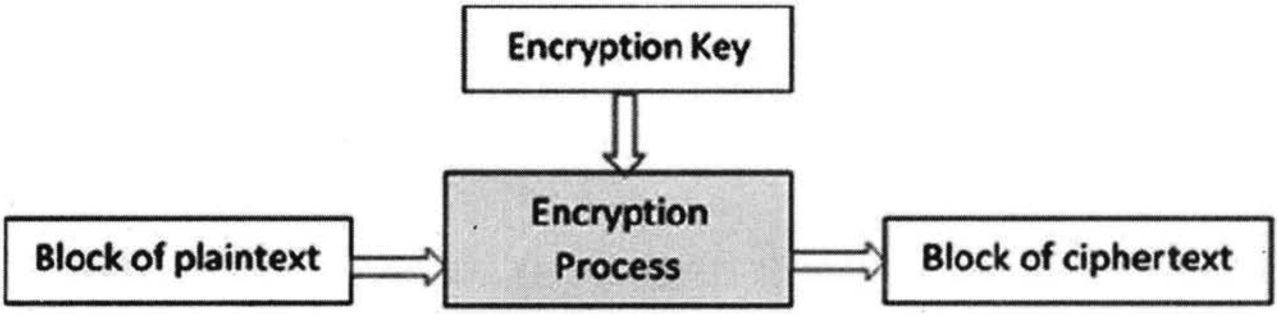
- Block Ciphers
- Stream Ciphers



4.2.1 Block Ciphers

In this scheme, the plain binary text is processed in blocks (groups) of bits at a time; i.e. a block of plaintext bits is selected, a series of operations is performed on this block to generate a block of ciphertext bits. The number of bits in a block is fixed. For example, the schemes DES and AES have block sizes of 64 and 128, respectively.

The basic scheme of a block cipher is depicted as follows –



A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size. The size of block is fixed in the given scheme. The choice of block size does not directly affect to the strength of encryption scheme. The strength of cipher depends up on the key length.

Block Size

Though any size of block is acceptable, following aspects are borne in mind while selecting a size of a block.

- **Avoid very small block size** – Say a block size is m bits. Then the possible plaintext bits combinations are then 2^m. If the attacker discovers the plain text blocks corresponding to some previously sent ciphertext blocks, then the attacker can launch a type of 'dictionary attack' by building up a dictionary of plaintext/ciphertext pairs sent using that encryption key. A larger block size makes attack harder as the dictionary needs to be larger.

- **Do not have very large block size** – With very large block size, the cipher becomes inefficient to operate. Such plaintexts will need to be padded before being encrypted.

- **Multiples of 8 bit** – A preferred block size is a multiple of 8 as it is easy for implementation as most computer processor handle data in multiple of 8 bits.

Padding in Block Cipher

Block ciphers process blocks of fixed sizes (say 64 bits). The length of plaintexts is mostly not a multiple of the block size. For example, a 150-bit plaintext provides two blocks of 64 bits each with third block of balance 22 bits.

The last block of bits needs to be padded up with redundant information so that the length of the final block equal to block size of the scheme. In our example, the remaining 22 bits need to have additional 42 redundant bits added to provide a complete block. The process of adding bits to the last block is referred to as **padding.**

Too much padding makes the system inefficient. Also, padding may render the system insecure at times, if the padding is done with same bits always.

Block Cipher Schemes

There is a vast number of block ciphers schemes that are in use. Many of them are publically known. Most popular and prominent block ciphers are listed below.

- **Digital Encryption Standard (DES)** – The popular block cipher of the 1990s. It is now considered as a 'broken' block cipher, due primarily to its small key size.

- **Triple DES** – It is a variant scheme based on repeated DES applications. It is still a respected block ciphers but inefficient compared to the new faster block ciphers available.

- **Advanced Encryption Standard (AES)** – It is a relatively new block cipher based on the encryption algorithm **Rijndael** that won the AES design competition.

- **IDEA** – It is a sufficiently strong block cipher with a block size of 64 and a key size of 128 bits. A number of applications use IDEA encryption, including early versions of Pretty Good Privacy (PGP) protocol. The use of IDEA scheme has a restricted adoption due to patent issues.

- **Twofish** – This scheme of block cipher uses block size of 128 bits and a key of variable length. It was one of the AES finalists. It is based on the earlier block cipher Blowfish with a block size of 64 bits.

- **Serpent** – A block cipher with a block size of 128 bits and key lengths of 128, 192, or 256 bits, which was also an AES competition finalist. It is a slower but has more secure design than other block cipher.

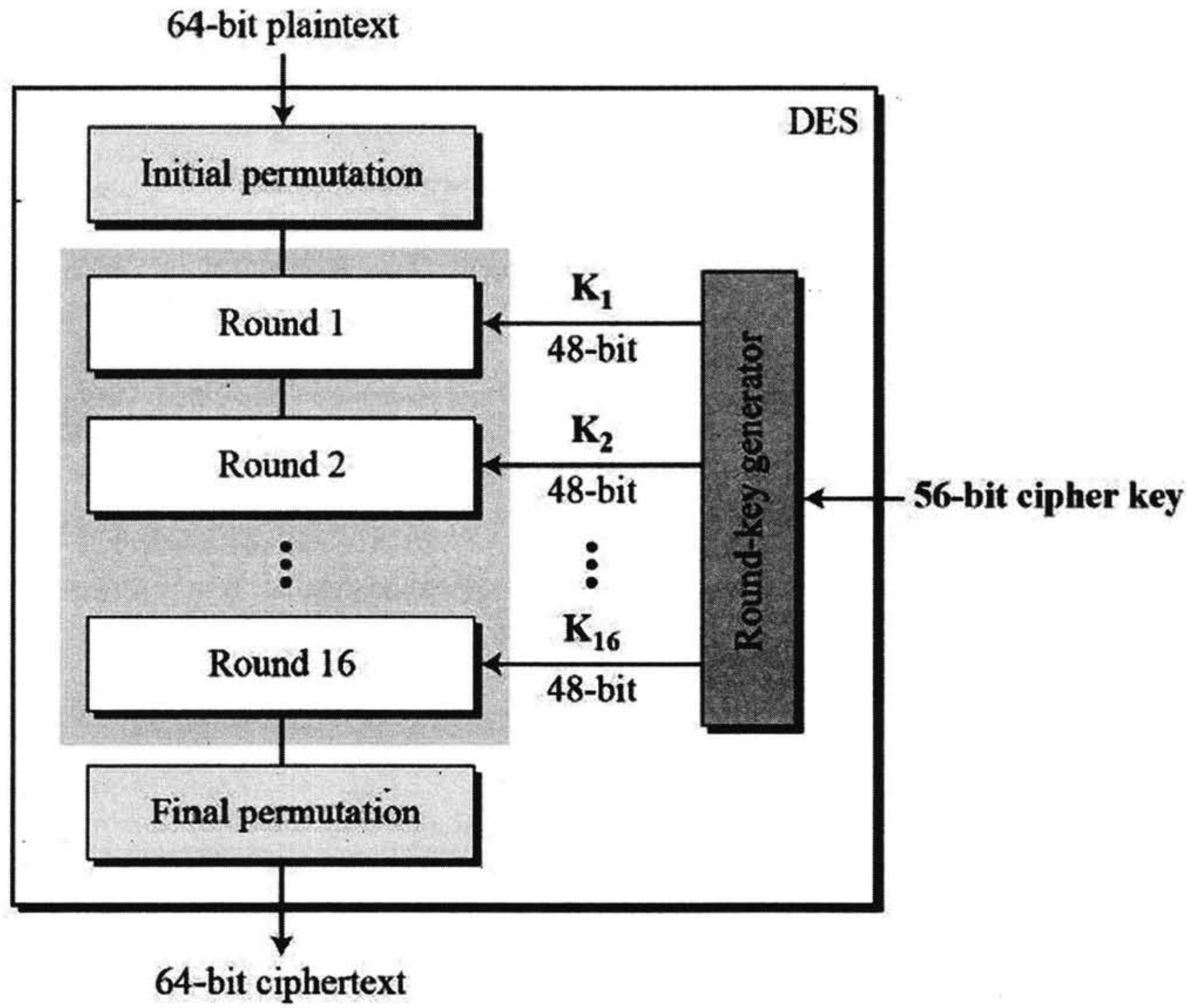
4.2.2 Stream Ciphers

In this scheme, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of ciphertext. Technically, stream ciphers are block ciphers with a block size of one bit.

4.3 Block and the Data Encryption Standards

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration –

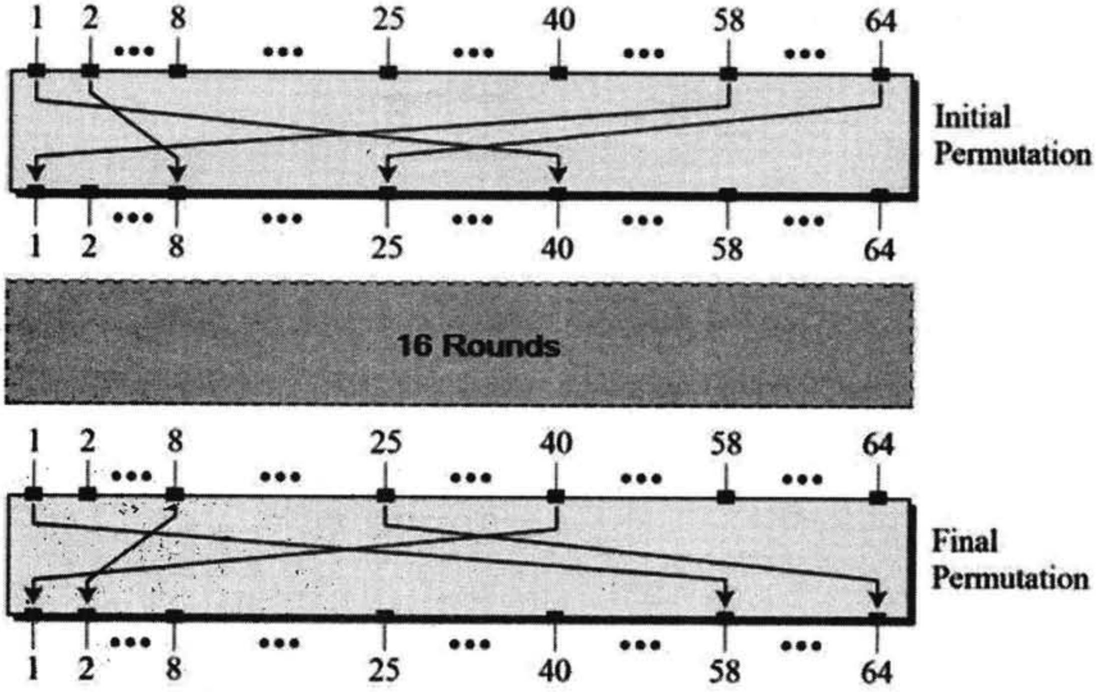


Since DES is based on the Feistel Cipher, all that is required to specify DES is –

- Round function
- Key schedule
- Any additional processing – Initial and final permutation

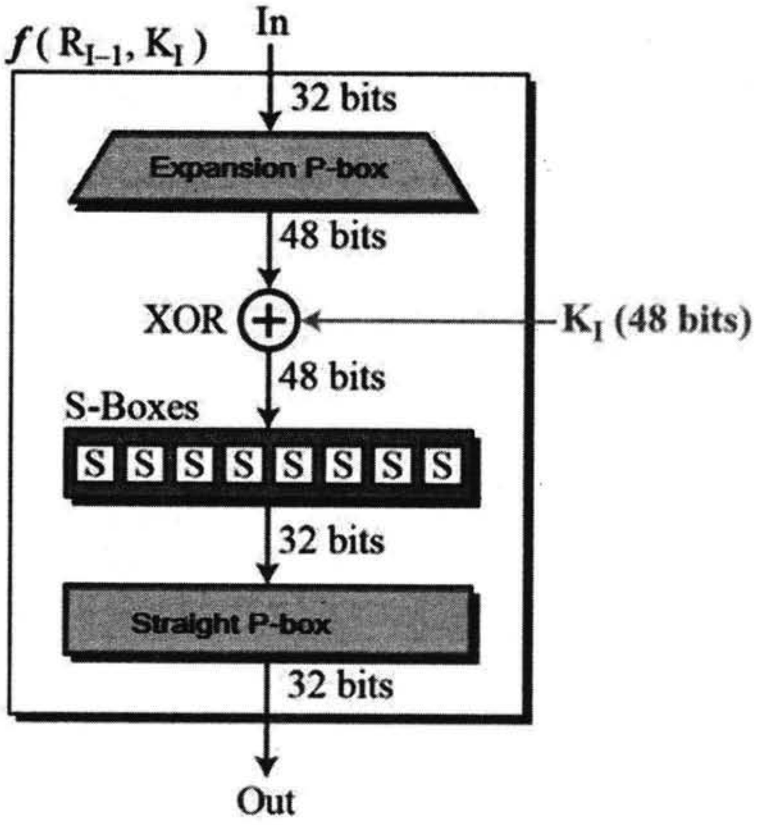
4.3.1 Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows –

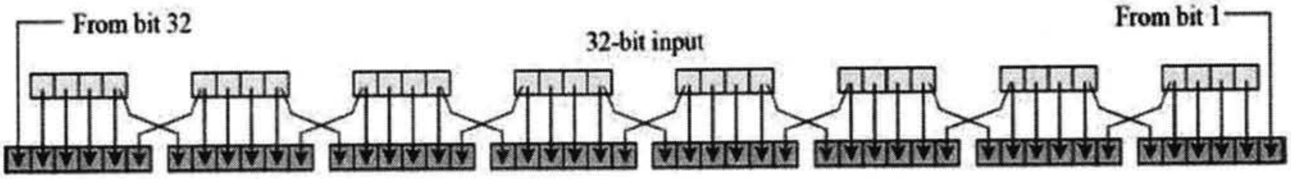


4.3.2 Round Fqnction

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



- **Expansion Permutation Box** – Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration –

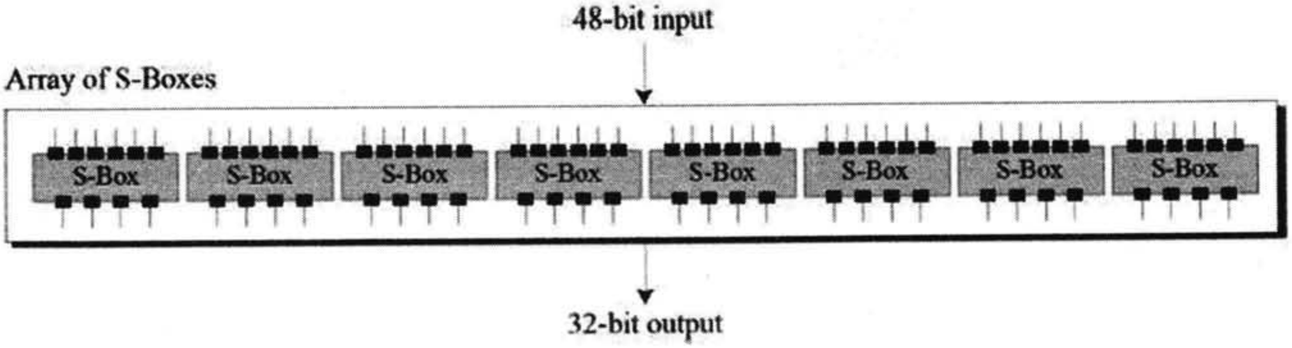


- The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown –

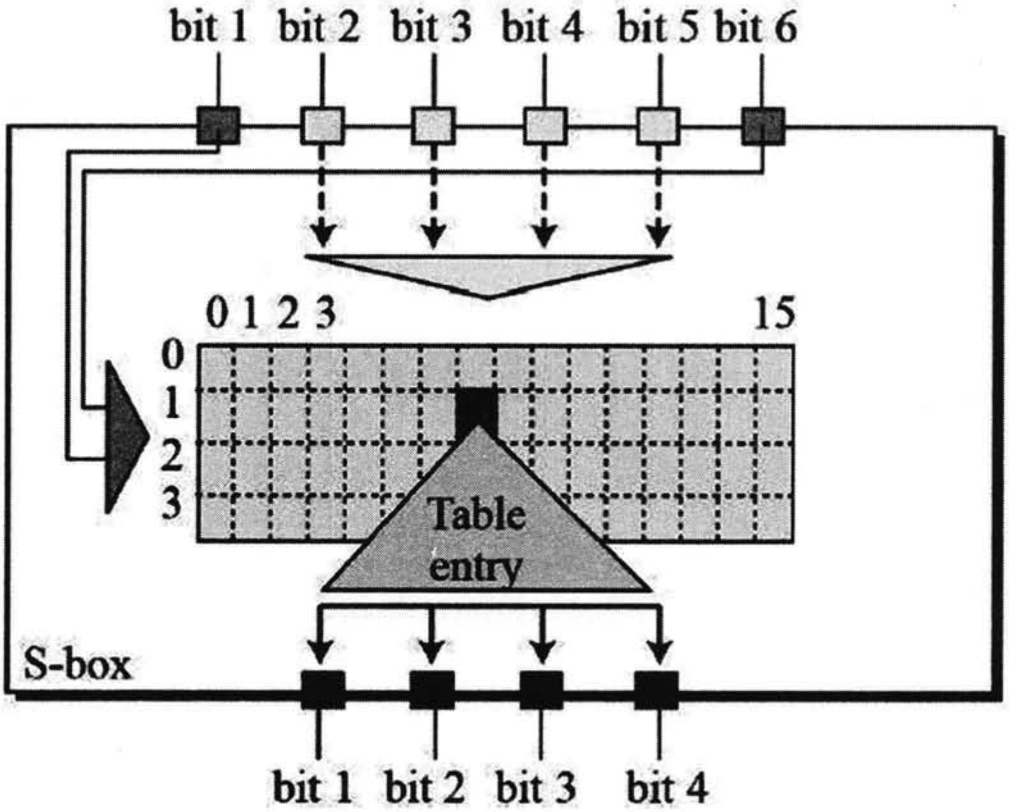
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

- **XOR (Whitener).** – After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

- **Substitution Boxes.** – The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration –



- The S-box rule is illustrated below –



- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

- **Straight Permutation** – The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:

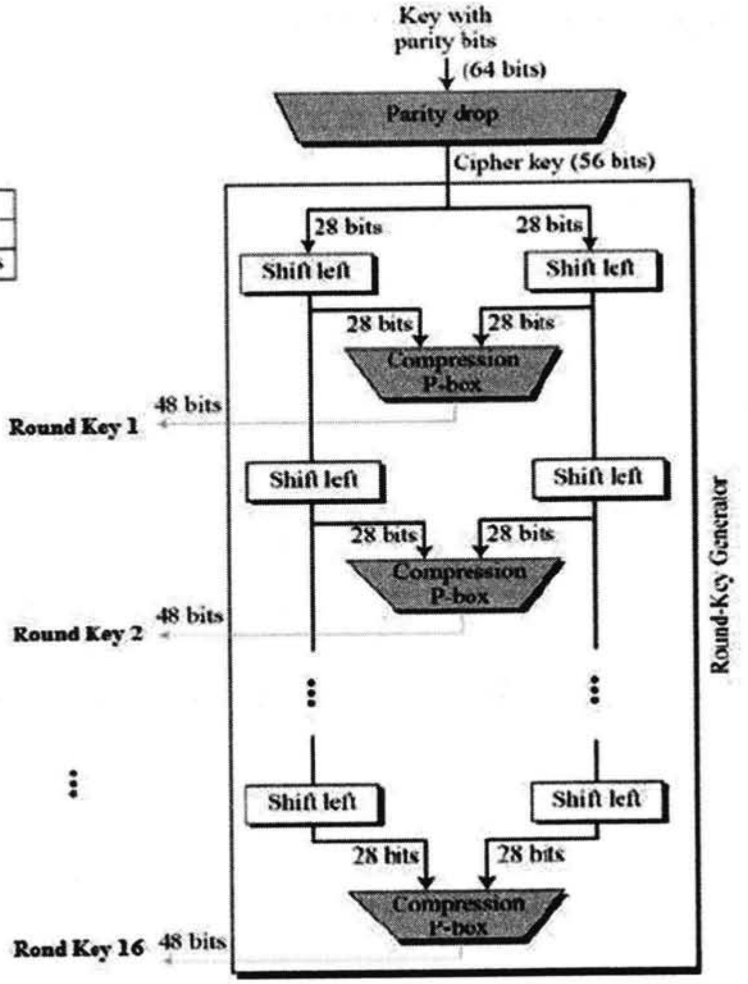
16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

4.3.4 Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration –

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits



The logic for Parity drop, shifting, and Compression P-box is given in the DES description.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** – A small change in plaintext results in the very grate change in the ciphertext.
- **Completeness** – Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

4.4Public key Encryption and Hash Functions

Encryption is a security method in which information is encoded in such a way that only authorized user can read it. It uses encryption algorithm to generate ciphertext that can only be read if decrypted.

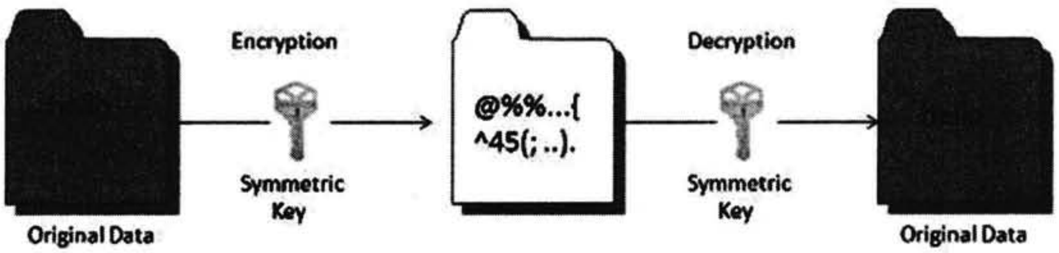
Types of Encryption

There are two types of encryptions schemes as listed below:

- Symmetric Key encryption
- Public Key encryption

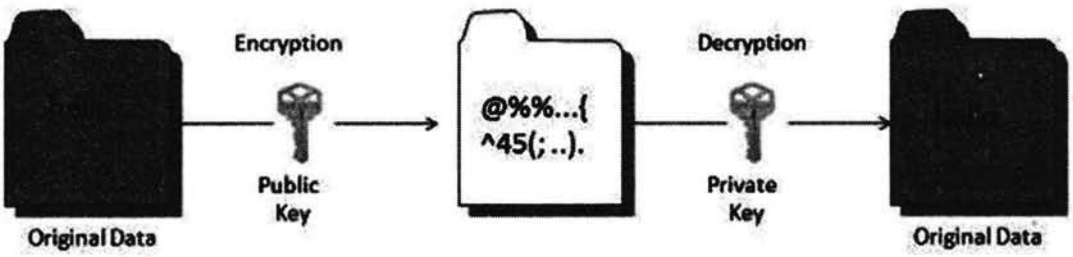
4.4.1 Symmetric key encryption

Symmetric key encryption algorithm uses same cryptographic keys for both encryption and decryption of cipher text.



4.4.2 Public key encryption

Public key encryption algorithm uses pair of keys, one of which is a secret key and one of which is public. These two keys are mathematically linked with each other.



4.4.3 Hashing

In terms of security, hashing is a technique used to encrypt data and generate unpredictable hash values. It is the hash function that generates the hash code, which helps to protect the security of transmission from unauthorized users.

Hash function algorithms

Hashing algorithm provides a way to verify that the message received is the same as the message sent. It can take a plain text message as input and then computes a value based on that message.

Key Points

- The length of computed value is much shorter than the original message.
- It is possible that different plain text messages could generate the same value.

Here we will discuss a sample hashing algorithm in which we will multiply the number of a's, e's and h's in the message and will then add the number of o's to this value.

For example, the message is " the combination to the safe is two, seven, thirty-five". The hash of this message, using our simple hashing algorithm is as follows:

2 x 6 x 3) + 4 = 40

The hash of this message is sent to John with cipher text. After he decrypts the message, he computes its hash value using the agreed upon hashing algorithm. If the hash value sent by Bob doesn't match the hash value of decrypted message, John will know that the message has been altered.

For example, John received a hash value of 17 and decrypted a message Bob has sent as "You are being followed, use backroads, hurry"

He could conclude the message had been altered, this is because the hash value of the message he received is:

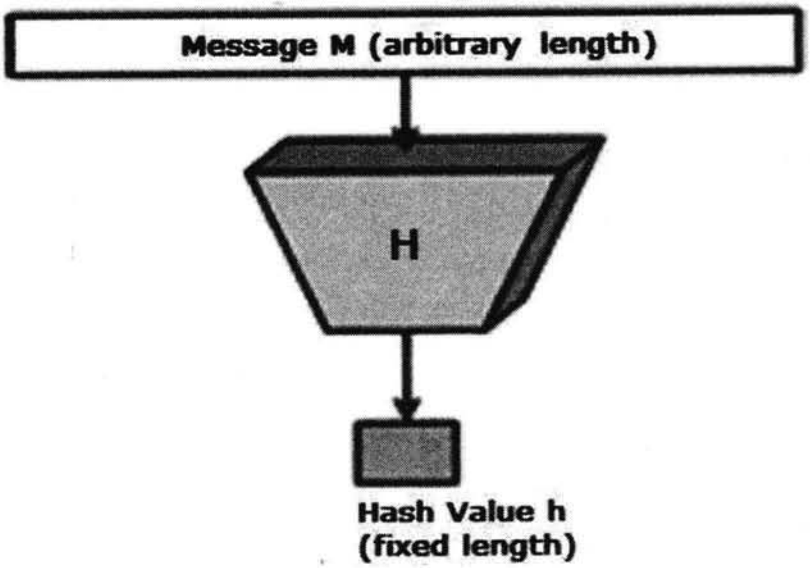
(3x4x1)+4 = 16

This is different from then value 17 that Bob sent.

Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called **message digest** or simply**hash values**. The following picture illustrated hash function –



Features of Hash Functions

The typical features of hash functions are –

- **Fixed Length Output (Hash Value)**
  - Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data**.
  - In general, the hash is much smaller than the input data, hence hash functions are sometimes called **compression functions**.
  - Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.
  - Hash function with n bit output is referred to as an **n-bit hash function**. Popular hash functions generate values between 160 and 512 bits.

- **Efficiency of Operation**
    - Generally for any hash function h with input x, computation of h(x) is a fast operation.
    - Computationally hash functions are much faster than a symmetric encryption.

Properties of Hash Functions

In order to be an effective cryptographic tool, the hash function is desired to possess following properties –

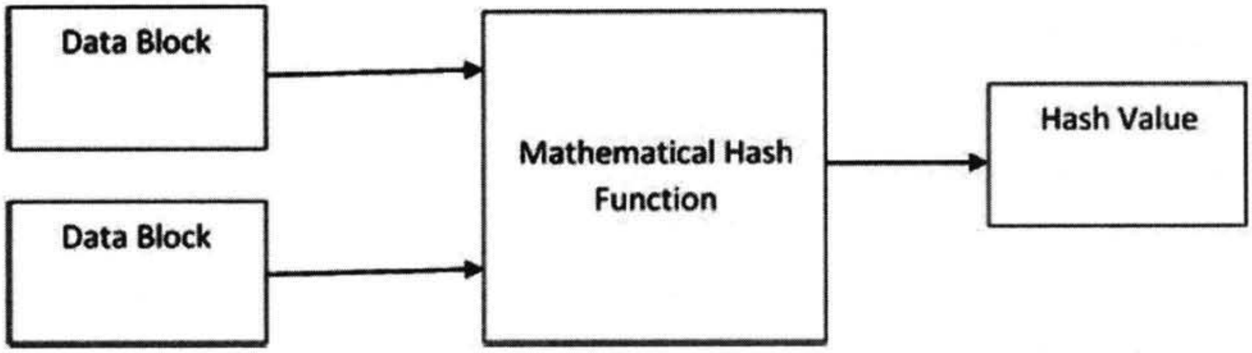
- **Pre-Image Resistance**
    - This property means that it should be computationally hard to reverse a hash function.
    - In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
    - This property protects against an attacker who only has a hash value and is trying to find the input.
- **Second Pre-Image Resistance**
    - This property means given an input and its hash, it should be hard to find a different input with the same hash.
    - In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).
    - This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.
- **Collision Resistance**
    - This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.

- In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).
- Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find.
- This property makes it very difficult for an attacker to find two input values with the same hash.
- Also, if a hash function is collision-resistant **then it is second pre-image resistant.**

Design of Hashing Algorithms

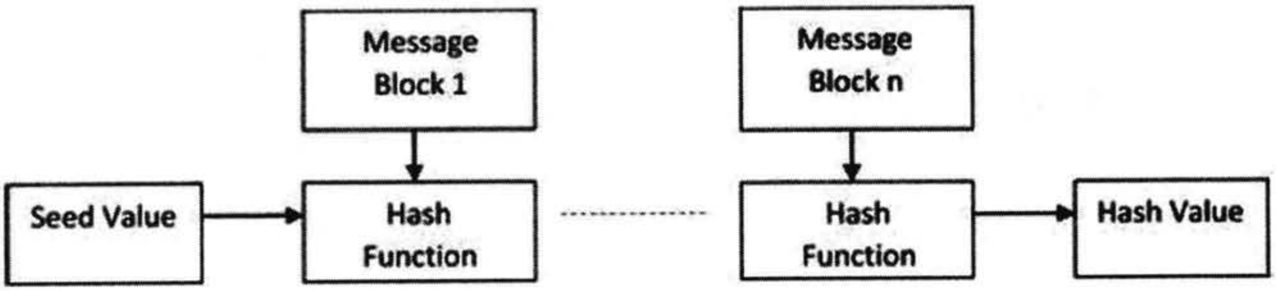
At the heart of a hashing is a mathematical function that operates on two fixed-size blocks of data to create a hash code. This hash function forms the part of the hashing algorithm.

The size of each data block varies depending on the algorithm. Typically the block sizes are from 128 bits to 512 bits. The following illustration demonstrates hash function –



Hashing algorithm involves rounds of above hash function like a block cipher. Each round takes an input of a fixed size, typically a combination of the most recent message block and the output of the last round.

This process is repeated for as many rounds as are required to hash the entire message. Schematic of hashing algorithm is depicted in the following illustration –



Since, the hash value of first message block becomes an input to the second hash operation, output of which alters the result of the third operation, and so on. This effect, known as an **avalanche** effect of hashing.

Avalanche effect results in substantially different hash values for two messages that differ by even a single bit of data.

Understand the difference between hash function and algorithm correctly. The hash function generates a hash code by operating on two blocks of fixed-length binary data.

Hashing algorithm is a process for using the hash function, specifying how the message will be broken up and how the results from previous message blocks are chained together.

Popular Hash Functions

Let us briefly see some popular hash functions –

1.Message Digest (MD)

MD5 was most popular and widely used hash function for quite some years.

- The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321. It is a 128-bit hash function.
- MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file. For example, file servers often provide a pre-computed MD5 checksum for the files, so that a user can compare the checksum of the downloaded file to it.
- In 2004, collisions were found in MD5. An analytical attack was reported to be successful only in an hour by using computer cluster. This collision attack resulted in compromised MD5 and hence it is no longer recommended for use.

2.Secure Hash Function (SHA)

Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, there are structurally different.

- The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993. It had few weaknesses and did not become very popular. Later in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0.
- SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security.
- In 2005, a method was found for uncovering collisions for SHA-1 within practical time frame making long-term employability of SHA-1 doubtful.
- SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash value. No successful attacks have yet been reported on SHA-2 hash function.
- Though SHA-2 is a strong hash function. Though significantly different, its basic design is still follows design of SHA-1. Hence, NIST called for new competitive hash function designs.
- In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard. Keccak offers many benefits, such as efficient performance and good resistance for attacks.

3.RIPEMD

The RIPEND is an acronym for RACE Integrity Primitives Evaluation Message Digest. This set of hash functions was designed by open research community and generally known as a family of European hash functions.

- The set includes RIPEND, RIPEMD-128, and RIPEMD-160. There also exist 256, and 320-bit versions of this algorithm.
- Original RIPEMD (128 bit) is based upon the design principles used in MD4 and found to provide questionable security. RIPEMD 128-bit version came as a quick fix replacement to overcome vulnerabilities on the original RIPEMD.

- RIPEMD-160 is an improved version and the most widely used version in the family. The 256 and 320-bit versions reduce the chance of accidental collision, but do not have higher levels of security as compared to RIPEMD-128 and RIPEMD-160 respectively.

1. Whirlpool

This is a 512-bit hash function.

- It is derived from the modified version of Advanced Encryption Standard (AES). One of the designer was Vincent Rijmen, a co-creator of the AES.
- Three versions of Whirlpool have been released; namely WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.

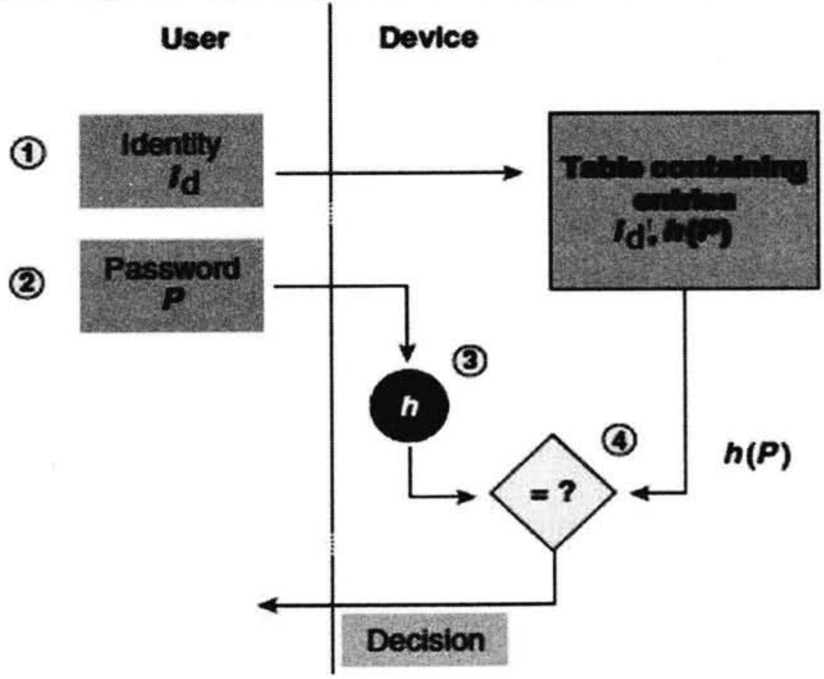
2. Applications of Hash Functions

There are two direct applications of hash function based on its cryptographic properties.

1. Password Storage

Hash functions provide protection to password storage.

- Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.
- The Password file consists of a table of pairs which are in the form (user id, h(P)).
- The process of logon is depicted in the following illustration –

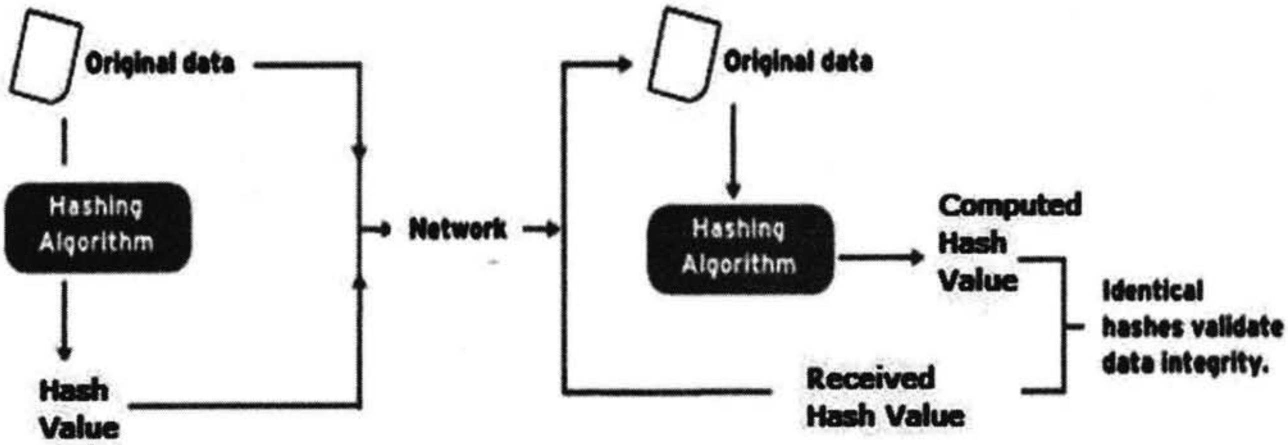


- An intruder can only see the hashes of passwords, even if he accessed the password. He can neither logon using hash nor can he derive the password from hash value since hash function possesses the property of pre-image resistance.

2. ***Data Integrity Check***

Data integrity check is a most common application of the hash functions. It is used to generate the checksums on data files. This application provides assurance to the user about correctness of the data.

The process is depicted in the following illustration –



The integrity check helps the user to detect any changes made to original file. It however, does not provide any assurance about originality. The attacker, instead of modifying file data, can change the entire file and compute all together new hash and send to the receiver. This integrity check application is useful only if the user is sure about the originality of file.

4.5 Public Key Cryptography and RSA

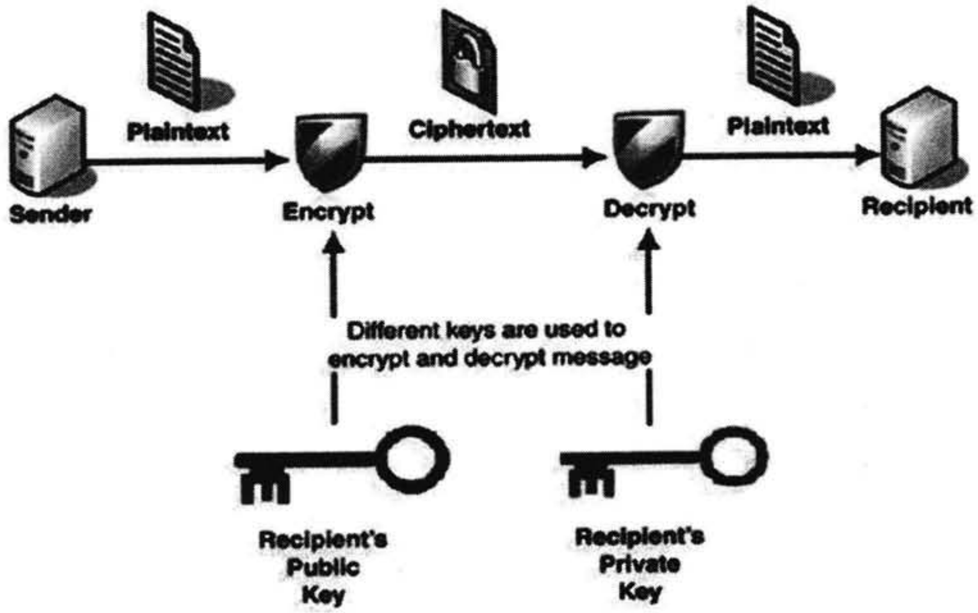
4.5.1 Public Key Cryptography

Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

The process of encryption and decryption is depicted in the following illustration –



The most important properties of public key encryption scheme are –

- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- Each receiver possesses a unique decryption key, generally referred to as his private key.
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

There are three types of Public Key Encryption schemes.

4.5.2 RSA Cryptosystem

This cryptosystem is one the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars **Ron Rivest, Adi Shamir,** and **Len Adleman** and hence, it is termed as RSA cryptosystem.

We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

Generation of RSA Key Pair

Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below –

- **Generate the RSA modulus (n)**
  - Select two large primes, p and q.
  - Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.

- **Find Derived Number (e)**
  - Number **e** must be greater than 1 and less than (p – 1)(q – 1).
  - There must be no common factor for e and (p – 1)(q – 1) except for 1. In other words two numbers e and (p – 1)(q – 1) are co prime.

- **Form the public key**
  - The pair of numbers (n, e) form the RSA public key and is made public.
  - Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.

- **Generate the private key**
  - Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
  - Number d is the inverse of e modulo (p - 1)(q – 1). This means that d is the number less than (p - 1)(q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1)(q - 1).
  - This relationship is written mathematically as follows –

$$ed = 1 \bmod (p - 1)(q - 1)$$

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example

An example of generating RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are very high).

- Let two primes be $p = 7$ and $q = 13$. Thus, modulus $n = pq = 7 \text{ x } 13 = 91$.
- Select $e = 5$, which is a valid choice since there is no number that is common factor of 5 and $(p - 1)(q - 1) = 6 \times 12 = 72$, except for 1.
- The pair of numbers $(n, e) = (91, 5)$ forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
- Input $p = 7$, $q = 13$, and $e = 5$ to the Extended Euclidean Algorithm. The output will be $d = 29$.
- Check that the d calculated is correct by computing –

$$de = 29 \times 5 = 145 = 1 \bmod 72$$

- Hence, public key is (91, 5) and private keys is (91, 29).

Encryption and Decryption

Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.

Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as –

$C = P^e \bmod n$

- In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.

- Returning to our Key Generation example with plaintext P = 10, we get ciphertext C –

$C = 10^5 \bmod 91$

RSA Decryption

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a ciphertext C.

- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

$\text{Plaintext} = C^d \bmod n$

- Returning again to our numerical example, the ciphertext C = 82 would get decrypted to number 10 using private key 29 –

$\text{Plaintext} = 82^{29} \bmod 91 = 10$

RSA Analysis

The security of RSA depends on the strengths of two separate functions. The RSA cryptosystem is most popular public-key cryptosystem strength of which is based on the practical difficulty of factoring the very large numbers.

- **Encryption Function** – It is considered as a one-way function of converting plaintext into ciphertext and it can be reversed only with the knowledge of private key d.

- **Key Generation** – The difficulty of determining a private key from an RSA public key is equivalent to factoring the modulus n. An attacker thus cannot use knowledge of an RSA public key to determine an RSA private key unless he can factor n. It is also a one way function, going from p & q values to modulus n is easy but reverse is not possible.

If either of these two functions are proved non one-way, then RSA will be broken. In fact, if a technique for factoring efficiently is developed then RSA will no longer be safe.

The strength of RSA encryption drastically goes down against attacks if the number p and q are not large primes and/ or chosen public key e is a small number.

Review questions

1. Explain in detail why network security is important.

2. Mention the protocols used by IPsec to provide security.

3. Analyze the characteristic of two keys in Public-Key algorithms.

4. Illustrate the properties of Hash Function.

5. Discuss the security mechanisms in the network layer.

6. Compare stream cipher with block cipher with example.

7. Explain the RSA Encryption Algorithm.

8. Differentiate public key and conventional encryption? Conventional Encryption Public key Encryption

9. Identify the possible threats for RSA algorithm.

10. List the most popular and prominent block ciphers and explain.

UNIT-V

SECURITY PRACTICES

5.1 Network Security Practices

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Information: is defined as "knowledge obtained from investigation, Study or Instruction, Intelligence, news, facts, data, a Signature or Character representing data".

Security: is defined as "freedom from Danger", or Safety: "Freedom from Fear or Anxiety".

Information Security: "Measures adopted to prevent the unauthorized use, misuse, modification, Denial of use of knowledge, Facts, data or Capabilities**".** From the above definition, Information Security does guarantees protection.

Computer security: With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, and the need is even more acute for systems that can be accessed over a public telephone network, data network, or the Internet. The generic name for the collection of tools designed to protect data and to thwart hackers is **computer security.**

Internet security: Security is affected with the introduction of distributed systems and the use of networks and communications for carrying data between terminal user and computer and between computer and computer. Network security measures are needed to protect data during their transmission. In fact, the term **network security** is somewhat misleading, because virtually all business, government, and academic organizations interconnect their data processing equipment with a collection of interconnected networks. Such a collection is often referred to as an internet, and the term **internet security** is used.

There are no clear boundaries between the above said forms of security.

5.1.1 The OSI Security Architecture:

The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) Recommends X.800, *Security Architecture for OSI*, defines a systematic approach. The OSI security architecture provides overview of many of the concepts and it focuses on security attacks, mechanisms, and services.

Security attack: Any action that compromises the security of information owned by an organization.

Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

The terms *threat* and *attack* are commonly used to mean more or less the same thing and the actual definitions are

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Attack: An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

5.1.2 Security Attacks:

Security attacks, used both in X.800 and RFC 2828, are classified as pa*ssive attacks* and *active attacks*.

A passive attack attempts to learn or make use of information from the system but does not affect system resources.

An active attack attempts to alter system resources or affect their operation.

Passive Attacks:

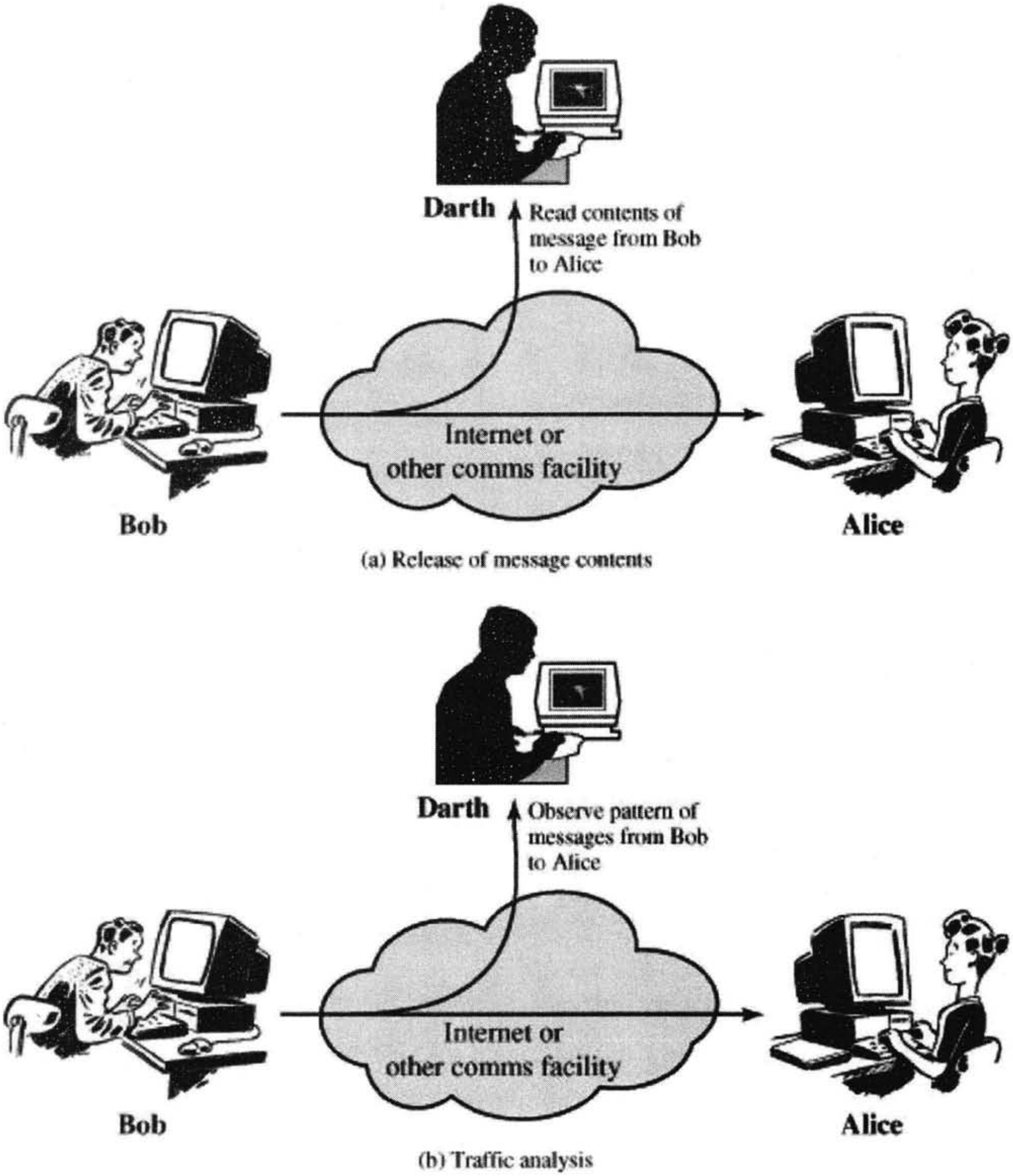
Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

The **release of message contents** is easily understood (Figure 1.3a). A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. To prevent an opponent from learning the contents of these transmissions.

A second type of passive attack, **traffic analysis**, is subtler (Figure 1.3b). Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice
Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

(b) Traffic analysis

Figure 1.3. Passive Attacks

Active Attacks:

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: Masquerade, Replay, Modification of messages, and Denial of service.

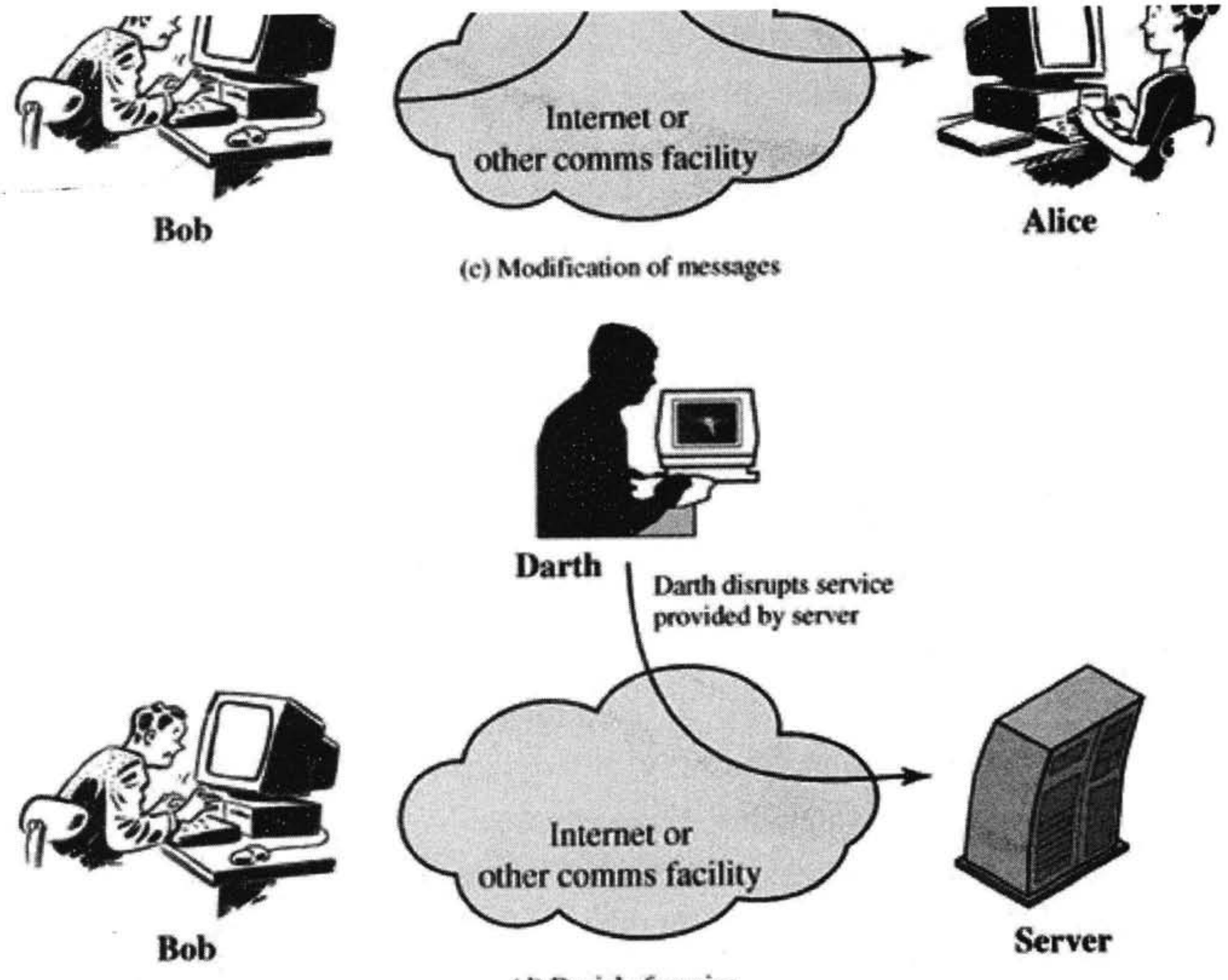
A **masquerade** takes place when one entity pretends to be a different entity (Figure 1.4a). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure 1.4b).

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure 1.4c). For example, a message meaning "Allow John Smith to read confidential file *accounts*" is modified to mean "Allow Fred Brown to read confidential file *accounts.*"

The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure 1.4d). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).

Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.



(c) Modification of messages

(d) Denial of service

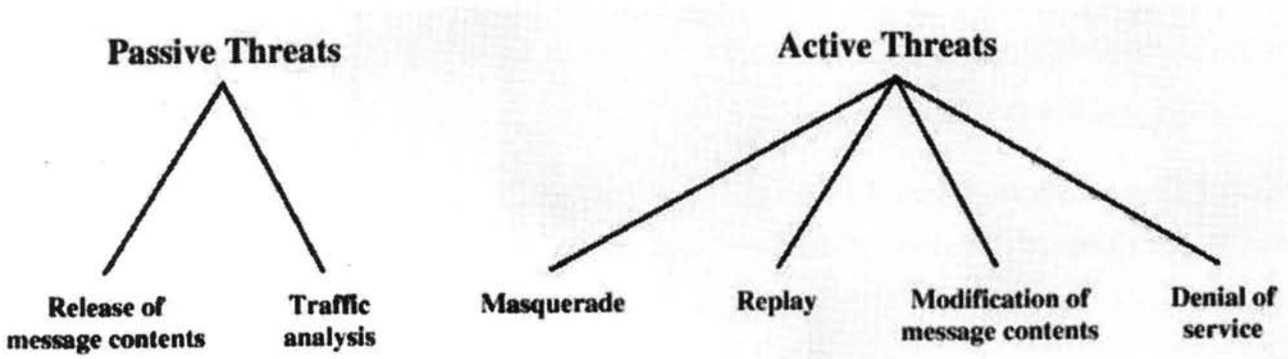


Figure 1.2 Active and Passive Security Threats

5.1.3 Types of Network Security Devices

Active Devices

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

5.2 Authentication Applications

Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Verifying the identity of a remote process in the face of a malicious, active intruder is surprisingly difficult and requires complex protocols based on cryptography. In this section, we will study some of the many authentication protocols that are used on insecure computer networks. As an aside, some people confuse authorization with authentication.

Authentication: The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication: Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data Origin Authentication: In a connectionless transfer, provides assurance that the source of received data is as claimed.

Access control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

Data confidentiality: The protection of data from unauthorized disclosure.

1. **Connection Confidentiality:**The protection of all user data on a connection.
2. **Connectionless Confidentiality:** The protection of all user data in a single data block
3. **Selective-Field Confidentiality:** The confidentiality of selected fields within the user Data on a connection or in a single data block.
4. **Traffic Flow Confidentiality:** The protection of the information that might be Derived from observation of traffic flows.

Data integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

- **Connection Integrity with Recovery:** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
- **Connection Integrity without Recovery:** As above, but provides only detection without recovery.
- **Selective-Field Connection Integrity:** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- **Connectionless Integrity:** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
- **Selective-Field Connectionless Integrity:** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

Nonrepudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

- **Nonrepudiation, Origin:** Proof that the message was sent by the specified party.

- **Nonrepudiation, Destination:** Proof that the message was received by the specified party.

5.2.1 Specific security mechanisms

Incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

- **Encipherment:** The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
- **Digital Signature:** Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.
- **Access Control:** A variety of mechanisms that enforce access rights to resources.
- **Data Integrity:** A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- **Authentication Exchange:** A mechanism intended to ensure the identity of an entity by means of information exchange.
- **Traffic Padding:** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- **Routing Control:** Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- **Notarization:** The use of a trusted third party to assure certain properties of a data exchange.

5.2.2 Pervasive security mechanisms

Mechanisms that are not specific to any particular OSI security service or protocol layer.

- **Trusted Functionality:** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

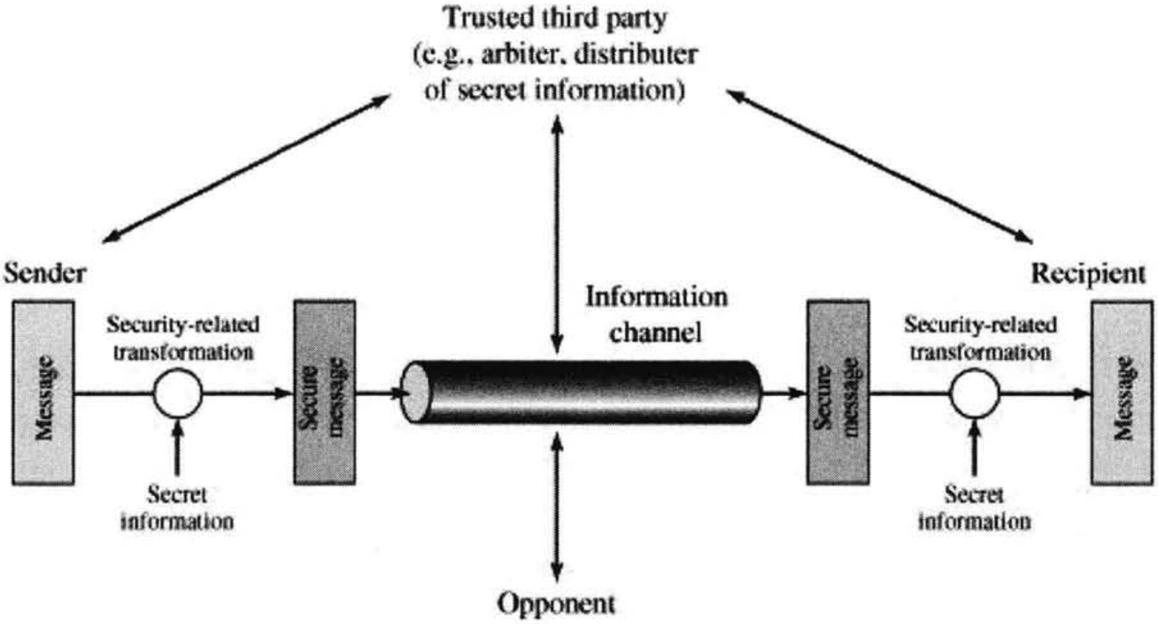
- **Security Label:** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

- **Event Detection:** Detection of security-relevant events.

- **Security Audit Trail:** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

- **Security Recovery:** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

5.2.3 A Model for Network Security:



A message is to be transferred from one party to another across some sort of internet. The two parties, who are the *principals* in this transaction, must cooperate for the exchange to take place.

A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.

All the techniques for providing security have two components:

- ***A security-related transformation on the information to be sent.*** Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender
- ***Some secret information shared by the two principals and, it is hoped, unknown to the opponent.*** An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

The general model shows that there are four basic tasks in designing a particular security service:

- Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
- Generate the secret information to be used with the algorithm.
- Develop methods for the distribution and sharing of the secret information.
- Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

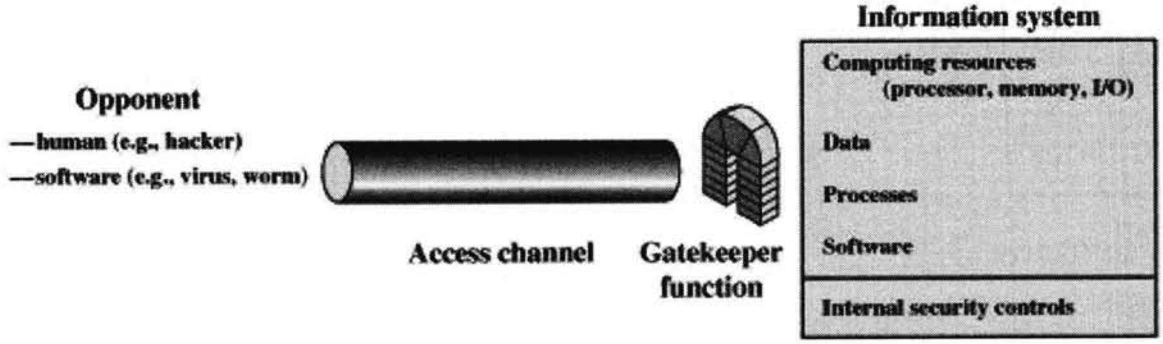


Figure: Network Access Security Model

A general model is illustrated by the above Figure, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. Or, the intruder can be a disgruntled employee who wishes to do damage, or a criminal who seeks to exploit computer assets for financial gain.

Internet Standards and the Internet Society:

Many of the protocols that make up the TCP/IP protocol suite have been standardized or are in the process of standardization. By universal agreement, an organization known as the Internet Society is responsible for the development and publication of these standards.

The Internet Society is a professional membership organization that oversees a number of boards and task forces involved in Internet development and standardization.

The Internet Organizations and RFC Publication:

The Internet Society is the coordinating committee for Internet design, engineering, and management. Areas covered include the operation of the Internet itself and the standardization of protocols used by end systems on the Internet for interoperability.

Three organizations under the Internet Society are responsible for the actual work of standards development and publication:

Internet Architecture Board (IAB): Responsible for defining the overall architecture of the Internet, providing guidance and broad direction to the IETF

Internet Engineering Task Force (IETF): The protocol engineering and development arm of the Internet

Internet Engineering Steering Group (IESG): Responsible for technical management of IETF activities and the Internet standards process

Working groups chartered by the IETF carry out the actual development of new standards and protocols for the Internet. Membership in a working group is voluntary; any interested party may participate. During the development of a specification, a working group will make a draft version of the document available as an Internet Draft, which is placed in the IETF's "Internet Drafts" online directory.

The document may remain as an Internet Draft for up to six months, and interested parties may review and comment on the draft. During that time, the IESG may approve publication of the draft as an RFC (Request for Comment). If the draft has not progressed to the status of an RFC during the six-month period, it is withdrawn from the directory. The working group may subsequently publish a revised version of the draft.

The IETF is responsible for publishing the RFCs, with approval of the IESG. The RFCs are the working notes of the Internet research and development community.

A document in this series may be on essentially any topic related to computer communications and may be anything from a meeting report to the specification of a standard. The work of the IETF is divided into eight areas, each with an area director and each composed of numerous working groups.

The Standardization Process:

The decision of which RFCs become Internet standards is made by the IESG, on the recommendation of the IETF. To become a standard, a specification must meet the following criteria:

- Be stable and well understood
- Be technically competent

- o Have multiple, independent, and interoperable implementations with substantial operational experience
- o Enjoy significant public support
- o Be recognizably useful in some or all parts of the Internet

The key difference between these criteria and those used for international standards from ITU is the emphasis here on operational experience.

The left-hand side of Figure1.1 shows the series of steps, called the *standards track*, that a specification goes through to become a standard; this process is defined in RFC 2026. The steps involve increasing amounts of scrutiny and testing.

At each step, the IETF must make a recommendation for advancement of the protocol, and the IESG must ratify it. The process begins when the IESG approves the publication of an Internet Draft document as an RFC with the status of Proposed Standard.

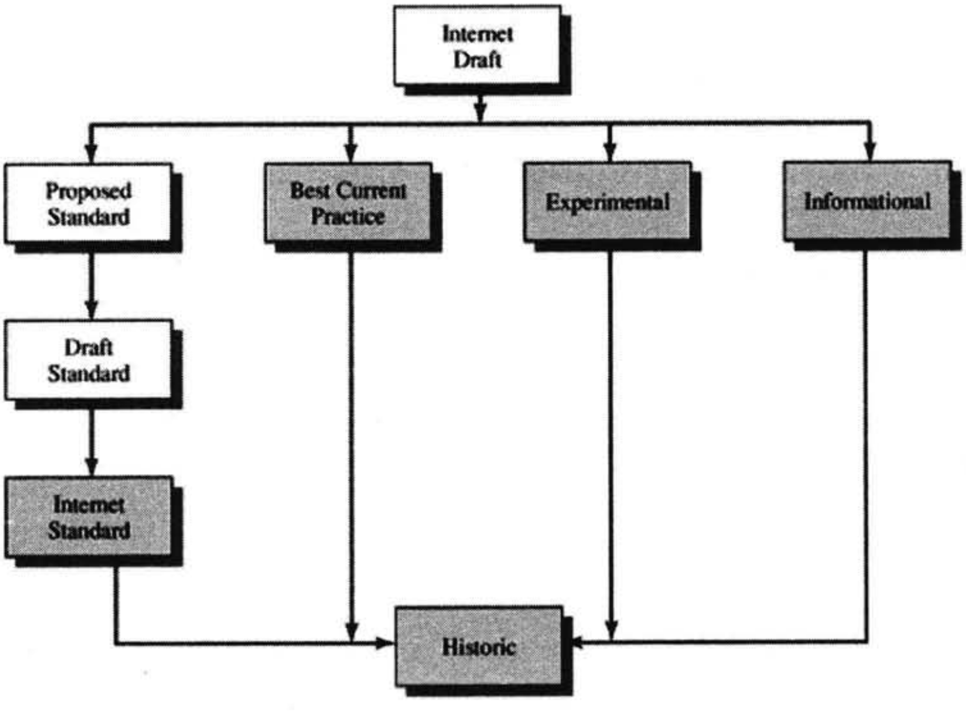


Figure 1.1 Internet RFC Publication Process

The white boxes in the diagram represent temporary states, which should be occupied for the minimum practical time. However, a document must remain a Proposed Standard for at least six months and a Draft Standard for at least four months to allow time for review and comment. The gray boxes represent long-term states that may be occupied for years.

For a specification to be advanced to Draft Standard status, there must be at least two independent and interoperable implementations from which adequate operational experience has been obtained. After significant implementation and operational experience has been obtained, a specification may be elevated to Internet Standard.

At this point, the Specification is assigned an STD number as well as an RFC number. Finally, when a protocol becomes obsolete, it is assigned to the Historic state.

Internet Standards Categories:

All Internet standards fall into one of two categories:

Technical specification (TS): A TS defines a protocol, service, procedure, convention, or format. The bulk of the Internet standards are TSs.

Applicability statement (AS): An AS specifies how, and under what circumstances, one or more TSs may be applied to support a particular Internet capability. An AS identifies one or more TSs that are relevant to the capability, and may specify values or ranges for particular parameters associated with a TS or functional subsets of a TS that are relevant for the capability.

Other RFC Types::

There are numerous RFCs that are not destined to become Internet standards. Some RFCs standardize the results of community deliberations about statements of principle or conclusions about what is the best way to perform some operations or IETF process function. Such RFCs are designated as Best Current Practice (BCP). Approval of BCPs follows essentially the same process for approval of Proposed Standards. Unlike standards-track documents, there is not a three-stage process for BCPs; a BCP goes from Internet draft status to approved BCP in one step.

A protocol or other specification that is not considered ready for standardization may be published as an Experimental RFC. After further work, the specification may be resubmitted. If the specification is generally stable, has resolved known design choices, is believed to be well understood, has received significant community review, and appears to enjoy enough community interest to be considered valuable, then the RFC will be designated a Proposed Standard. Finally, an Informational Specification is published for the general information of the Internet community.

5.2.3 Kerberos:

Kerberos is an authentication service developed by MIT. The problem that Kerberos addresses is this: Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network.

We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment, a workstation cannot be trusted to identify its users correctly to network services. In particular, the following three threats exist:

a. A user may gain access to a particular workstation and pretend to be another user operating from that workstation.

b. A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation.

c. A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.

In any of these cases, an unauthorized user may be able to gain access to services and data that he or she is not authorized to access.

Rather than building in elaborate authentication protocols at each server, Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. Unlike most other authentication schemes, Kerberos relies exclusively on symmetric encryption, making no use of public-key encryption.

Two versions of Kerberos are in common use. Version 4 implementations still exist. Version 5 corrects some of the security deficiencies of version 4 and has been issued as a proposed Internet Standard (RFC 1510).

Today the more commonly used architecture is a distributed architecture consisting of dedicated user workstations (clients) and distributed or centralized servers.

In this environment, three approaches to security can be envisioned:

- Rely on each individual client workstation to assure the identity of its user or users and rely on each server to enforce a security policy based on user identification (ID).
- Require that client systems authenticate themselves to servers, but trust the client system concerning the identity of its user.
- Require the user to prove his or her identity for each service invoked. Also require that servers prove their identity to clients.

In a small, closed environment, in which all systems are owned and operated by a single organization, the first or perhaps the second strategy may suffice. But in a more open environment, in which network connections to other machines are supported, the third approach is needed to protect user information and resources housed at the server. Kerberos supports this third approach.

Kerberos assumes distributed client/server architecture and employs one or more

A Kerberos server to provide an authentication service and Version 4 is the "original" **Kerberos.**

Kerberos Version 4:

Version 4 of Kerberos makes use of DES, to provide the authentication service. Viewing the protocol as a whole, it is difficult to see the need for the many elements contained therein. Therefore, we adopt a strategy used by Bill Bryant of Project Athena and build up to the full protocol by looking first at several hypothetical dialogues. Each successive dialogue adds additional complexity to counter security vulnerabilities revealed in the preceding dialogue.

A Simple Authentication Dialogue:

In any network environment, any client can apply to any server for service. The obvious security risk is that of impersonation. An opponent can pretend to be another client and obtain unauthorized privileges on server machines.

To counter this threat, servers must be able to confirm the identities of clients who request service.

Each server can be required to undertake this task for each client/server interaction, but in an open environment, this places a substantial burden on each server.

An alternative is to use an authentication server (AS) that knows the passwords of all users and stores these in a centralized database. In addition, the AS shares a unique secret key with each server. These keys have been distributed physically or in some other secure manner.

[The portion to the left of the colon indicates the sender and receiver; the portion to the right indicates the contents of the message, the symbol || indicates concatenation.]

(1) C →AS:	*IDC*||*PC*||*I* *DV*
(2) AS→ C:	*Ticket*
(3) C →V:	*IDC*||*Ticket*

Ticket = E(*Kv*, [*IDC*||*ADC*||*IDV]*)

Where C = client

AS = authentication server

V =server

IDC = identifier of user on C

IDV = identifier of V

PC = password of user on C

ADC = network address of C

Kv = secret encryption key shared by AS and V

In this scenario, the user logs on to a workstation and requests access to server V. The client module C in the user's workstation requests the user's password and then sends a message to the AS that includes the user's ID, the server's ID, and the user's password. The AS checks its database to see if the user has supplied the proper password for this user ID and whether this user is permitted access to server V.

If both tests are passed, the AS accepts the user as authentic and must now convince the server that this user is authentic. To do so, the AS creates a ticket that contains the user's ID and network address and the server's ID. This ticket is encrypted using the secret key shared by the AS and this server. This ticket is then sent back to C. Because the ticket is encrypted, it cannot be altered by C or by an opponent.

With this ticket, C can now apply to V for service. C sends a message to V containing C's ID and the ticket. V decrypts the ticket and verifies that the user ID in the ticket is the same as the unencrypted user ID in the message. If these two match, the server considers the user authenticated and grants the requested service

A More Secure Authentication Dialogue:

First, we would like to minimize the number of times that a user has to enter a password. Suppose each ticket can be used only once. If user C logs on to a workstation in the morning and wishes to check his or her mail at a mail server, C must supply a password to get a ticket for the mail server. If C wishes to check the mail several times during the day, each attempt requires reentering the password. We can improve matters by saying that tickets are reusable. For a single logon session, the workstation can store the mail server ticket after it is received and use it on behalf of the user for multiple accesses to the mail server

The second problem is that the earlier scenario involved a plaintext transmission of the password [message (1)]. An eavesdropper could capture the password and use any service accessible to the victim.

To solve these additional problems, we introduce a scheme for avoiding plaintext passwords and a new server, known as the ticket-granting server (TGS). The new but still hypothetical scenario is as follows:

Once per user logon session:

(1 **)** C→ AS	*IDC*||*IDtgs*
(2 **)** AS→ C:	E(*Kc, Tickettgs*)
Once per type of service:	
(3 **)** C →TGS	*IDC*||*IDV*||*Tickett* *gs*
(4 **)** TGS→ C	*Ticketv*
Once per service session:	
(5) C→ V	*IDC*||*Ticketv*

Tickettgs = E(*Ktgs,* [*IDC*||*ADC*||*IDtgs*||*TS*1||*Lifetime*1])

Ticketv = E(*Kv*, [*IDC*||*ADC*||*IDv*||*TS*2||*Lifetime*2])

The new service, TGS, issues tickets to users who have been authenticated to AS. Thus, the user first requests a ticket-granting ticket (Tickettgs) from the AS. The client module in the user workstation saves this ticket. Each time the user requires access to a new service, the client applies to the TGS, using the ticket to authenticate itself.

The TGS then grants a ticket for the particular service. The client saves each service-granting ticket and uses it to authenticate its user to a server each time a particular service is requested. Let us look at the details of this scheme.

1. The client requests a ticket-granting ticket on behalf of the user by sending its user's ID and password to the AS, together with the TGS ID, indicating a request to use the TGS service.
2. The AS responds with a ticket that is encrypted with a key that is derived from the user's password. When this response arrives at the client, the client prompts the user for his or her password, generates the key, and attempts to decrypt the incoming message. If the correct password is supplied, the ticket is successfully recovered.

The Version 4 Authentication Dialogue:

The first problem is the lifetime associated with the ticket-granting ticket. If this lifetime is very short (e.g., minutes), then the user will be repeatedly asked for a password. If the lifetime is long (e.g., hours), then an opponent has a greater opportunity for replay.

The second problem is that there may be a requirement for servers to authenticate themselves to users. Without such authentication, an opponent could sabotage the configuration so that messages to a server were directed to another location. The false server would then be in a position to act as a real server and capture any information from the user and deny the true service to the user.

The following Table which shows the actual Kerberos protocol

(1)C→ AS *IDc||IDtgs||TS*1
(2)AS →C E(*Kc*,[*Kc,tgs*||*IDtgs*||*TS*2||*Lifetime*2||*Tickettgs*])
Tickettgs = E(K*tgs*, [K*c,tgs*||IDc||ADc||IDtgs||TS2||Lifetime2])

(a) Authentication Service Exchange to obtain ticket-granting ticket

(1) **C →TGS** *IDv*||*Tickettgs*||*Authenticatorc*
(2) **TGS→ C** E(*Kc,tgs*, [*Kc,v*||*IDv*||*TS*4||*Ticketv*])
Tickettgs = E(K*tgs*, [K*c,tgs*||ID*C*||AD*C*||ID*tgs*||TS2||Lifetime2])

Ticketv = E(K*v*, [K*c,v*||ID*C*||AD*C*||ID*v*||TS4||Lifetime4])

Authenticatorc = E(K*c,tgs*, [ID*C*||AD*C*||TS3])

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(1) **C →V** *Ticketv*||*Authenticatorc*

(2) **V→ C** E(*Kc,v*, [*TS*5 + 1]) (for mutual authentication)

Ticketv = E(K*v*, [K*c,v*||ID*c*||AD*c*||ID*v*||TS4||Lifetime4])

Authenticatorc = E(K*c,v*,[ID*c*||AD*C*||TS5])

(c) Client/Server Authentication Exchange to obtain service

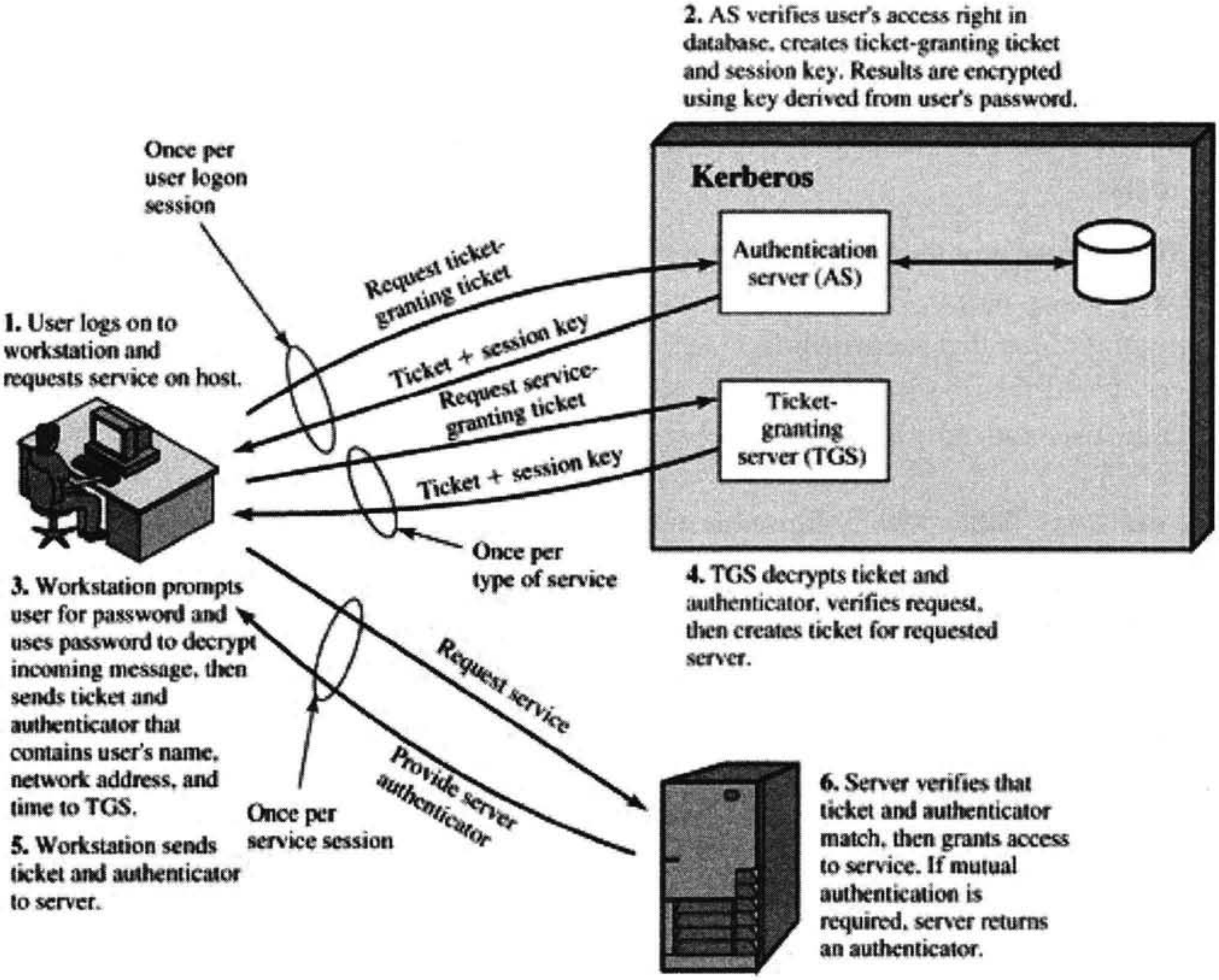

2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
Kerberos
Authentication server (AS)
Ticket-granting server (TGS)
Once per user logon session
Request ticket-granting ticket
Ticket + session key
Request service-granting ticket
Ticket + session key
1. User logs on to workstation and requests service on host.
Once per type of service
4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.
3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user's name, network address, and time to TGS.
Request service
Provide server authenticator
Once per service session
5. Workstation sends ticket and authenticator to server.
6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

Figure 1.1. Overview of Kerberos

Kerberos Realms and Multiple Kerberi:

A full-service Kerberos environment consisting of a Kerberos server, a number of clients,and a number of application servers requires the following:

1. The Kerberos server must have the user ID and hashed passwords of all participating users in its database. All users are registered with the Kerberos server.
2. The Kerberos server must share a secret key with each server. All servers are registered with the Kerberos server.
3. The Kerberos server in each interoperating realm shares a secret key with the server in the other realm. The two Kerberos servers are registered with each other.

Such an environment is referred to as a **Kerberos realm**. A Kerberos realm is a set of managed nodes that share the same Kerberos database.

Networks of clients and servers under different administrative organizations typically constitute different realms. The scheme requires that the Kerberos server in one realm trust the Kerberos server in the other realm to authenticate its users.

Furthermore, the participating servers in the second realm must also be willing to trust the Kerberos server in the first realm. With these ground rules in place, we can describe the mechanism as shown in the Figure.

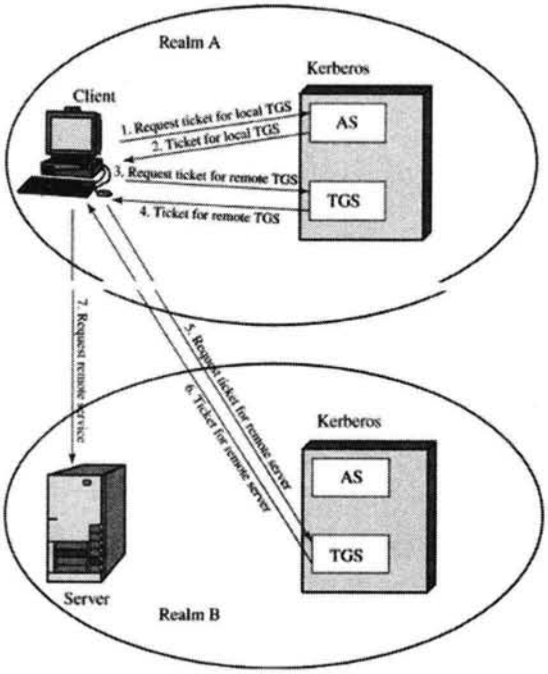

Realm A
Kerberos
Client
1. Request ticket for local TGS
2. Ticket for local TGS
AS
3. Request ticket for remote TGS
4. Ticket for remote TGS
TGS
7. Request remote service
5. Request ticket for remote server
6. Ticket for remote server
Kerberos
AS
TGS
Server
Realm B

Figure - Request for Service in Another Realm

The details of the exchanges are as follows

(1) C→ AS: *IDc*||*IDtgs*||*TS*1

(2)AS→ C:E(*Kc*, [*Kc,tgs*||*IDtgs*||*TS*2||*Lifetime*2||*Tickettgs*])

(3)C→ TGS:*IDtgsrem*||*Tickettgs*||*Authenticatorc*

(4)TGS→ C:E(*Kc,tgs*, [*Kc,tgsrem*||*IDtgsrem*||*TS*4||*Tickettgsrem*])

(5)C →TGSrem: *IDvrem*||*Tickettgsrem*||*Authenticatorc*

(6)TGSrem →C: E(*Kc,tgsrem*, [*Kc,vrem*||*IDvrem*||*TS*6||*Ticketvrem*])

(7)C→ Vrem:*Ticketvrem*||*Authenticatorc*

The ticket presented to the remote server (*Vrem*) indicates the realm in which the user was originally authenticated. The server chooses whether to honor the remote request.

Kerberos Version 5:

Kerberos Version 5 is specified in RFC 1510 and provides a number of improvements over version 4.

5.3 Electronic Mail Security

5.3.1 E-mail Hacking

Email hacking can be done in any of the following ways:

- Spam
- Virus
- Phishing

Spam

E-mail spamming is an act of sending **Unsolicited Bulk E-mails (UBI)**which one has not asked for. Email spams are the junk mails sent by commercial companies as an advertisement of their products and services.

Virus

Some emails may incorporate with files containing malicious script which when run on your computer may lead to destroy your important data.

Phishing

Email phishing is an activity of sending emails to a user claiming to be a legitimate enterprise. Its main purpose is to steal sensitive information such as usernames, passwords, and credit card details.

Such emails contains link to websites that are infected with malware and direct the user to enter details at a fake website whose look and feels are same to legitimate one.

5.3.2 ***E-mail Spamming and Junk Mails***

Email spamming is an act of sending Unsolicited Bulk E-mails (UBI) which one has not asked for. Email spams are the junk mails sent by commercial companies as an advertisement of their products and services.

Spams may cause the following problems:

- It floods your e-mail account with unwanted e-mails, which may result in loss of important e-mails if inbox is full.
- Time and energy is wasted in reviewing and deleting junk emails or spams.
- It consumes the bandwidth that slows the speed with which mails are delivered.
- Some unsolicited email may contain virus that can cause harm to your computer.

5.3.3 Blocking Spams

Following ways will help you to reduce spams:

- While posting letters to newsgroups or mailing list, use a separate e-mail address than the one you used for your personal e-mails.
- Don't give your email address on the websites as it can easily be spammed.
- Avoid replying to emails which you have received from unknown persons.
- Never buy anything in response to a spam that advertises a product.

5.3.4 E-mail Cleanup and Archiving

In order to have light weighted Inbox, it's good to archive your inbox from time to time. Here I will discuss the steps to clean up and archive your Outlook inbox.

- Select **File** tab on the mail pane.
- Select **Cleanup Tools** button on account information screen.
- Select **Archive** from cleanup tools drop down menu.
- Select **Archive this folder and all subfolders** option and then click on the folder that you want to archive. Select the date from the**Archive items older than:** list. Click **Browse** to create new **.pst** file name and location. Click **OK.**

5.4 IP Security

IPsec (IP security) as defined in RFC 2401 provides a security architecture for the Internet Protocol- not a security architecture for the Internet. The distinction is important: IPsec defines security services to be used at the IP layer, both for IPv4 and IPv6. It is often said that IPv6 is " more secure " than IPv4, but the difference is that IPsec is required for all IPv6, whereas it is optional for IPv4 nodes.

The IP Security Protocol (IPsec) provides an interoperable and open standard for building security into the network layer rather than at the application or transport layer. Although applications can benefit from network-layer security, the most important application IPsec enables is the creation of virtual private networks (VPNs) capable of securely carrying enterprise data across the open Internet.

IPsec is often used in conjunction with tunnel management protocols, including the Layer 2 Tunneling Protocol (L2TP), the Layer 2 Forwarding (L2F) protocol designed by Cisco Systems, and Microsoft's Point to Point Tunneling Protocol (PPTP). RFC 2661, " Layer Two Tunneling Protocol ' L2TP, ' " defines L2TP as a standards track specification for tunneling packets sent over a PPP link.

While the tunnel management protocols offer access security services, they don't provide authentication or privacy services, so they are often used in conjunction with IPsec-which does provide those services. However, saying that IPsec specifies protocols for encrypting and authenticating data sent within IP packets is an oversimplification and even obscures IPsec's full potential.

IPsec enables the following.

- **Encryption** of data passing between two nodes, using strong public and private key cryptographic algorithms
- **Authentication** of data and its source, using strong authentication mechanisms
- **Control over access** to sensitive data and private networks
- **Integrity verification** of data carried by a connectionless protocol (IP)
- **Protection against replay attacks,** in which an intruder intercepts packets sent between two IP nodes and resends them after decrypting or modifying them
- **Limitation of traffic analysis attacks,** in which an intruder intercepts protected data and analyzes source and destination information, size and type of packets, and other aspects of the data, including header contents that might not otherwise be protected by encryption
- **End-to-end security** for IP packets, providing assurance to users of endpoint nodes of the privacy and integrity of their transmissions
- **Secure tunneling** through insecure networks such as the global Internet and other public networks
- **Integration** of algorithms, protocols, and security infrastructures into an overarching security architecture.
- **Interoperable** As with all Internet protocols, interoperability is a fundamental goal.
- **High quality** The baseline for security through IPsec must be set high enough to guarantee a reasonable degree of actual security.

- **Cryptographically** based Cryptographers work with algorithms for encryption, secure hashing, and authentication.

Authentication Procedures:

X.509 also includes three alternative authentication procedures that are intended for use across a variety of applications. All these procedures make use of public-key signatures.

It is assumed that the two parties know each other's public key, either by obtaining each other's certificates from the directory or because the certificate is included in the initial message from each side.

Figure 14.6 illustrates the three procedures.

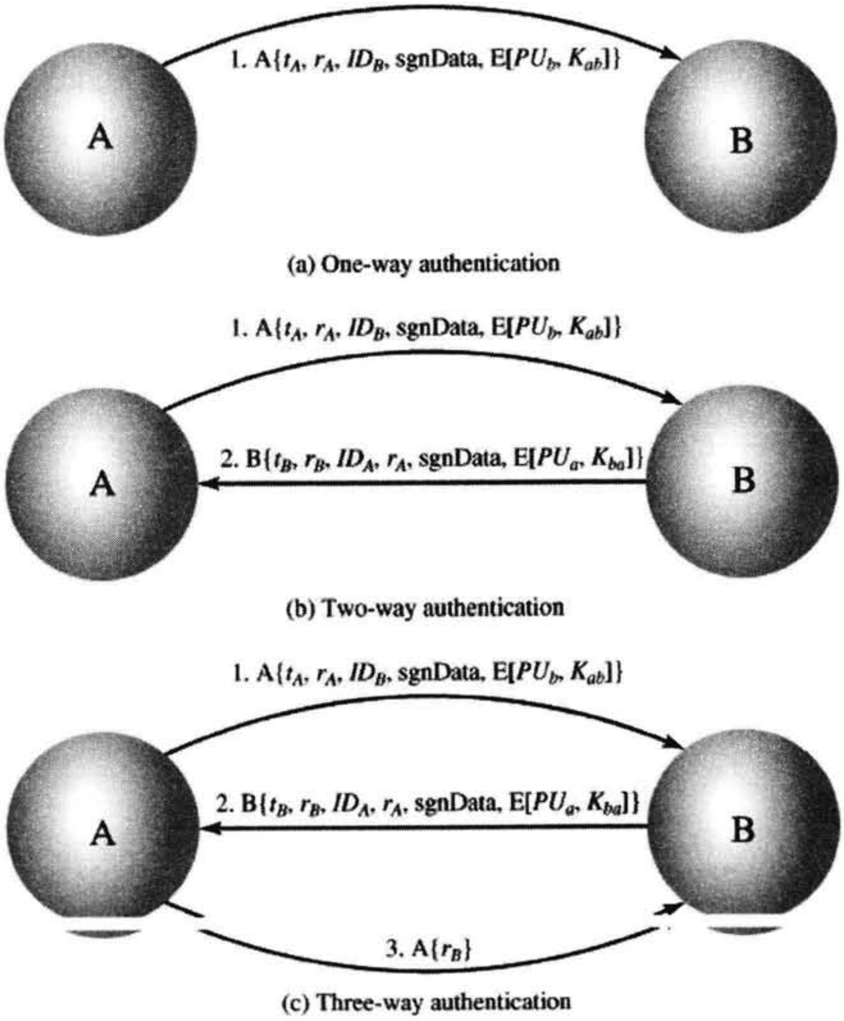

1. A{t_A, r_A, ID_B, sgnData, E[PU_b, K_{ab}]}
A
B
(a) One-way authentication
1. A{t_A, r_A, ID_B, sgnData, E[PU_b, K_{ab}]}
2. B{t_B, r_B, ID_A, r_A, sgnData, E[PU_a, K_{ba}]}
A
B
(b) Two-way authentication
1. A{t_A, r_A, ID_B, sgnData, E[PU_b, K_{ab}]}
2. B{t_B, r_B, ID_A, r_A, sgnData, E[PU_a, K_{ba}]}
A
B
3. A{r_B}
(c) Three-way authentication

Figure 1.6. X.509 Strong Authentication Procedures

One-Way Authentication:

One way authentication involves a single transfer of information from one user (A) to another (B), and establishes the following:

1. The identity of A and that the message was generated by A
2. That the message was intended for B
3. The integrity and originality (it has not been sent multiple times) of the message

Note that only the identity of the initiating entity is verified in this process, not that of the responding entity.

At a minimum, the message includes a timestamp *tA*, a nonce *rA* and the identity of B and is signed with A's private key. The timestamp consists of an optional generation time and an expiration time. This prevents delayed delivery of messages. The nonce can be used to detect replay attacks. The nonce value must be unique within the expiration time of the message. Thus, B can store the nonce until it expires and reject any new messages with the same nonce.

For pure authentication, the message is used simply to present credentials to B. The message may also include information to be conveyed. This information, signData, is included within the scope of the signature, guaranteeing its authenticity and integrity. The message may also be used to convey a session key to B, encrypted with B's public key.

Two-Way Authentication:

In addition to the three elements just listed, two-way authentication establishes the following elements:

1. The identity of B and that the reply message was generated by B
2. That the message was intended for A
3. The integrity and originality of the reply

Two-way authentication thus permits both parties in a communication to verify the identity of the other.

The reply message includes the nonce from A, to validate the reply. It also includes a timestamp and nonce generated by B. As before, the message may include signed additional information and a session key encrypted with A's public key

Three-Way Authentication:

In three-way authentication, a final message from A to B is included, which contains a signed copy of the nonce *rB*. The intent of this design is that timestamps need not be checked: Because both nonces are echoed back by the other side, each side can check the returned nonce to detect replay attacks. This approach is needed when synchronized clocks are not available.

X.509 Version 3:

The X.509 version 2 format does not convey all of the information that recent design and implementation experience has shown to be needed. The following requirements not satisfied by version 2:

1. The Subject field is inadequate to convey the identity of a key owner to a public-key user. X.509 names may be relatively short and lacking in obvious identification details that may be needed by the user.

2. The Subject field is also inadequate for many applications, which typically recognize entities by an Internet e-mail address, a URL, or some other Internet-related identification.
3. There is a need to indicate security policy information. This enables a security application or function, such as IPSec, to relate an X.509 certificate to a given policy.
4. There is a need to limit the damage that can result from a faulty or malicious CA by setting constraints on the applicability of a particular certificate.
5. It is important to be able to identify different keys used by the same owner at different times. This feature supports key life cycle management, in particular the ability to update key pairs for users and CAs on a regular basis or under exceptional circumstances.

- **Private-key usage period:** Indicates the period of use of the private key corresponding to the public key. Typically, the private key is used over a different period from the validity of the public key. For example, with digital signature keys, the usage period for the signing private key is typically shorter than that for the verifying public key.

- **Certificate policies:** Certificates may be used in environments where multiple policies apply. This extension lists policies that the certificate is recognized as supporting, together with optional qualifier information.

- **Policy mappings:** Used only in certificates for CAs issued by other CAs. Policy mappings allow an issuing CA to indicate that one or more of that issuer's policies can be considered equivalent to another policy used in the subject CA's domain.

5.5 Web Security

Security is critical to web services. However, neither XML-RPC nor SOAP specifications make any explicit security or authentication requirements.

There are three specific security issues with web services:

- Confidentiality
- Authentication
- Network Security

5.5.1 Confidentiality

If a client sends an XML request to a server, can we ensure that the communication remains confidential?

Answer lies here:

- XML-RPC and SOAP run primarily on top of HTTP.
- HTTP has support for Secure Socketes Layer (SSL).
- Communication can be encrypted via SSL.
- SSL is a proven technology and widely deployed.

A single web service may consist of a chain of applications. For example, one large service might tie together the services of three other applications. In this case, SSL is not adequate; the messages need to be encrypted at each node along the service path, and each node represents a potential weak link in the chain.

Currently, there is no agreed-upon solution to this issue, but one promising solution is the W3C XML Encryption Standard. This standard provides a framework for encrypting and decrypting entire XML documents or just portions of an XML document.

5.5.2 Authentication

If a client connects to a web service, how do we identify the user? Is the user authorized to use the service?

The following options can be considered but there is no clear consensus on a strong authentication scheme.

- HTTP includes built-in support for Basic and Digest authentication, and services can therefore be protected in much the same manner as HTML documents are currently protected.
- SOAP Digital Signature (SOAP-DSIG) leverages public key cryptography to digitally sign SOAP messages. It enables the client or server to validate the identity of the other party.
- The Organization for the Advancement of Structured Information Standards (OASIS) is working on the Security Assertion Markup Language (SAML).

5.5.3 Network Security

There is currently no easy answer to this problem, and it has been the subject of much debate. For now, if you are truly intent on filtering out SOAP or XML-RPC messages, one possibility is to filter out all HTTP POST requests that set their content type to text/xml.

Another alternative is to filter the SOAPAction HTTP header attribute. Firewall vendors are also currently developing tools explicitly designed to filter web service traffic.

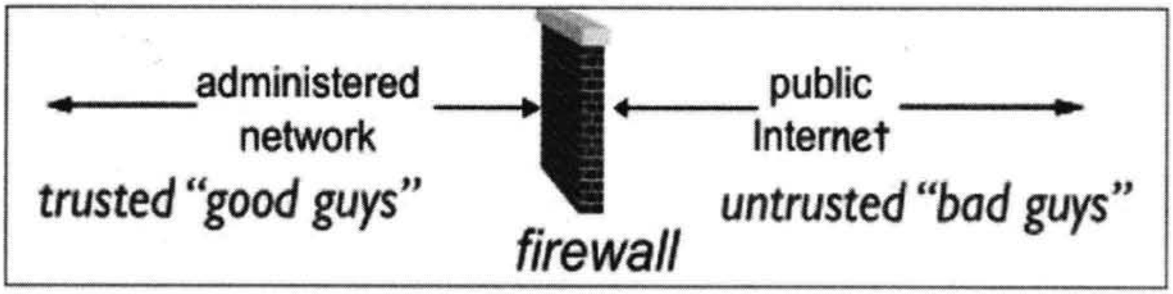
5.6 Firewall.

Almost every medium and large-scale organization has a presence on the Internet and has an organizational network connected to it. Network partitioning at the boundary between the outside Internet and the internal network is essential for network security. Sometimes the inside network (intranet) is referred to as the "trusted" side and the external Internet as the "un-trusted" side.

5.6.1 Types of Firewall

Firewall is a network device that isolates organization's internal network from larger outside network/Internet. It can be a hardware, software, or combined system that prevents unauthorized access to or from internal network.

All data packets entering or leaving the internal network pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.



Deploying firewall at network boundary is like aggregating the security at a single point. It is analogous to locking an apartment at the entrance and not necessarily at each door.

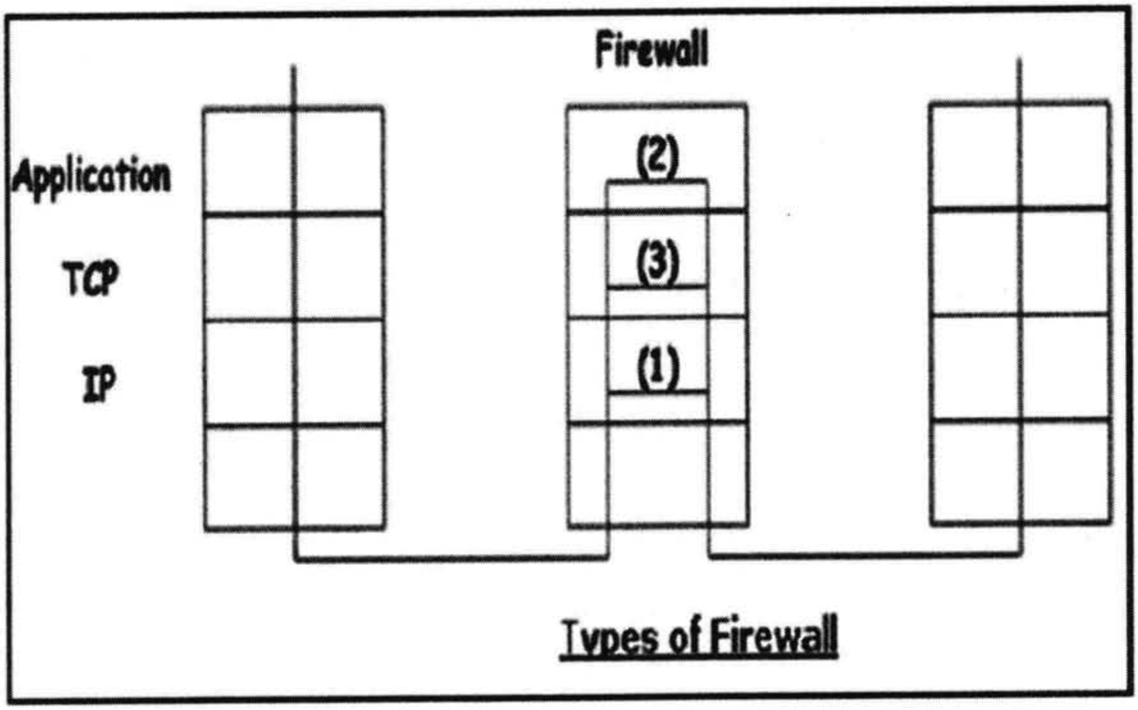
Firewall is considered as an essential element to achieve network security for the following reasons −

- Internal network and hosts are unlikely to be properly secured.
- Internet is a dangerous place with criminals, users from competing companies, disgruntled ex-employees, spies from unfriendly countries, vandals, etc.
- To prevent an attacker from launching denial of service attacks on network resource.
- To prevent illegal modification/access to internal data by an outsider attacker.

Firewall is categorized into three basic types –

- Packet filter (Stateless & Stateful)
- Application-level gateway
- Circuit-level gateway

These three categories, however, are not mutually exclusive. Modern firewalls have a mix of abilities that may place them in more than one of the three categories.



Types of Firewall

5.6.2 Stateless & Stateful Packet Filtering Firewall

In this type of firewall deployment, the internal network is connected to the external network/Internet via a router firewall. The firewall inspects and filters data packet-by-packet.

Packet-filtering firewalls allow or block the packets mostly based on criteria such as source and/or destination IP addresses, protocol, source and/or destination port numbers, and various other parameters within the IP header.

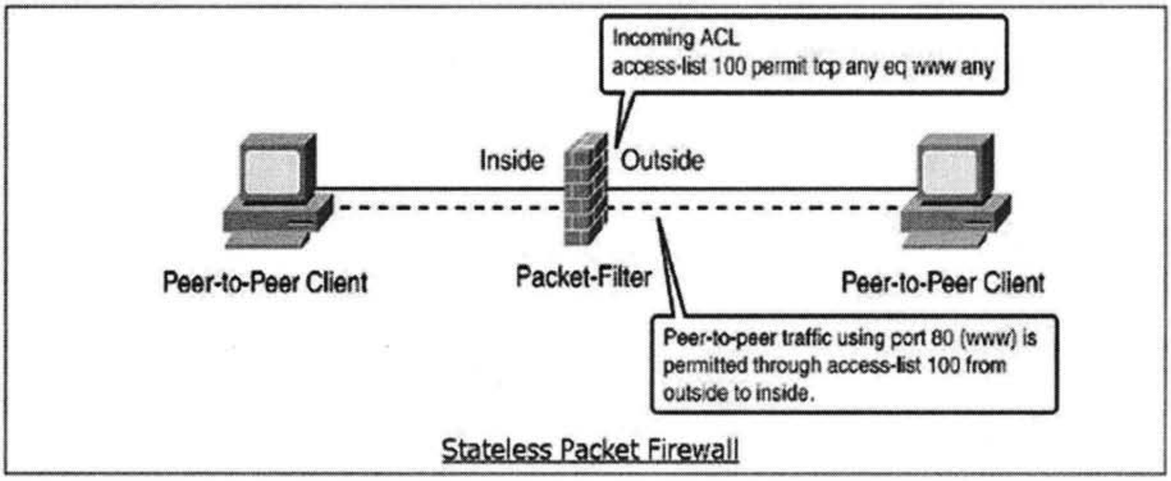
The decision can be based on factors other than IP header fields such as ICMP message type, TCP SYN and ACK bits, etc.

Packet filter rule has two parts –

- **Selection criteria** – It is a used as a condition and pattern matching for decision making.
- **Action field** – This part specifies action to be taken if an IP packet meets the selection criteria. The action could be either block (deny) or permit (allow) the packet across the firewall.

Packet filtering is generally accomplished by configuring Access Control Lists (ACL) on routers or switches. ACL is a table of packet filter rules.

As traffic enters or exits an interface, firewall applies ACLs from top to bottom to each incoming packet, finds matching criteria and either permits or denies the individual packets.


Incoming ACL
access-list 100 permit tcp any eq www any
Inside
Outside
Peer-to-Peer Client
Packet-Filter
Peer-to-Peer Client
Peer-to-peer traffic using port 80 (www) is permitted through access-list 100 from outside to inside.

Stateless Packet Firewall

Stateless firewall is a kind of a rigid tool. It looks at packet and allows it if its meets the criteria even if it is not part of any established ongoing communication.

Hence, such firewalls are replaced by **stateful firewalls** in modern networks. This type of firewalls offer a more in-depth inspection method over the only ACL based packet inspection methods of stateless firewalls.

Stateful firewall monitors the connection setup and teardown process to keep a check on connections at the TCP/IP level. This allows them to keep track of connections state and determine which hosts have open, authorized connections at any given point in time.

They reference the rule base only when a new connection is requested. Packets belonging to existing connections are compared to the firewall's state table of open connections, and decision to allow or block is taken. This process saves time and provides added security as well.

No packet is allowed to trespass the firewall unless it belongs to already established connection. It can timeout inactive connections at firewall after which it no longer admit packets for that connection.

Firewall provides network boundary protection by separating an internal network from the public Internet. Firewall can function at different layers of network protocol. IDS/IPS allows to monitor the anomalies in the network traffic to detect the attack and take preventive action against the same.

Review Questions:

1. Discuss the security mechanisms incorporated to provide some of the OSI security services.
2. Briefly explain the Kerberos version 4 messages exchanges and give the over view of Kerberos using a diagram
3. What is firewall? Explain the design goals of firewall.
4. Elucidate Email security in detail.
5. Discuss the encryption and decryption techniques in DES.
6. Illustrate one way authentication
7. Analyse Authentication Functions
8. Briefly explain about the IP Security
9. Describe 3 different approaches to Message Authentication
10. List four techniques used by firewalls to control access and enforce a security policy.

MODEL QUESTION PAPER

Subject Name: COMPUTER NETWORKS AND NETWORK SECURITY

Subject Code: HD5B/CHD5B

Section A (2 x 12 Marks = 24 Marks)

Answer any TWO Questions in about 500 words

1. Explain the layered architecture of OSI reference Model.
2. Describe Error detection and correction mechanisms
3. Elucidate the General Structure of DES

Section B (2 x 7 Marks = 14 Marks)

Answer any TWO Questions in about 300 words

4 . Explain Transmission Control Protocol in detail.

5. Email Security – Illustrate.
6. Discuss Hash functions of cryptography.

Section C (5 x 4 Marks = 20 Marks)

7. Answer FIVE of the following briefly:

a) What are the responsibilities of data link layer?
b) Local Area Network.
c) Principle elements of a public key cryptosystem
d) Masquerade
e) What is Kerberos? What are the uses?
f) Give the benefits of IP security?
g) Firewall.

Section D (6 x 2 Marks = 12 Marks)

8. Answer SIX of the following.

a) Mention the types of errors.
b) What are the two interfaces provided by protocols?
c) Flow Control
d) Different ways to address the framing problem
e) Define cryptanalysis
f) Virus
g) What are the types of network attacks?

PART-A

1. ISO/OSI reference model.

   Physical layer, Data link layer, Network layer, Transport layer,

   Session layer, Presentation layer, Application layer

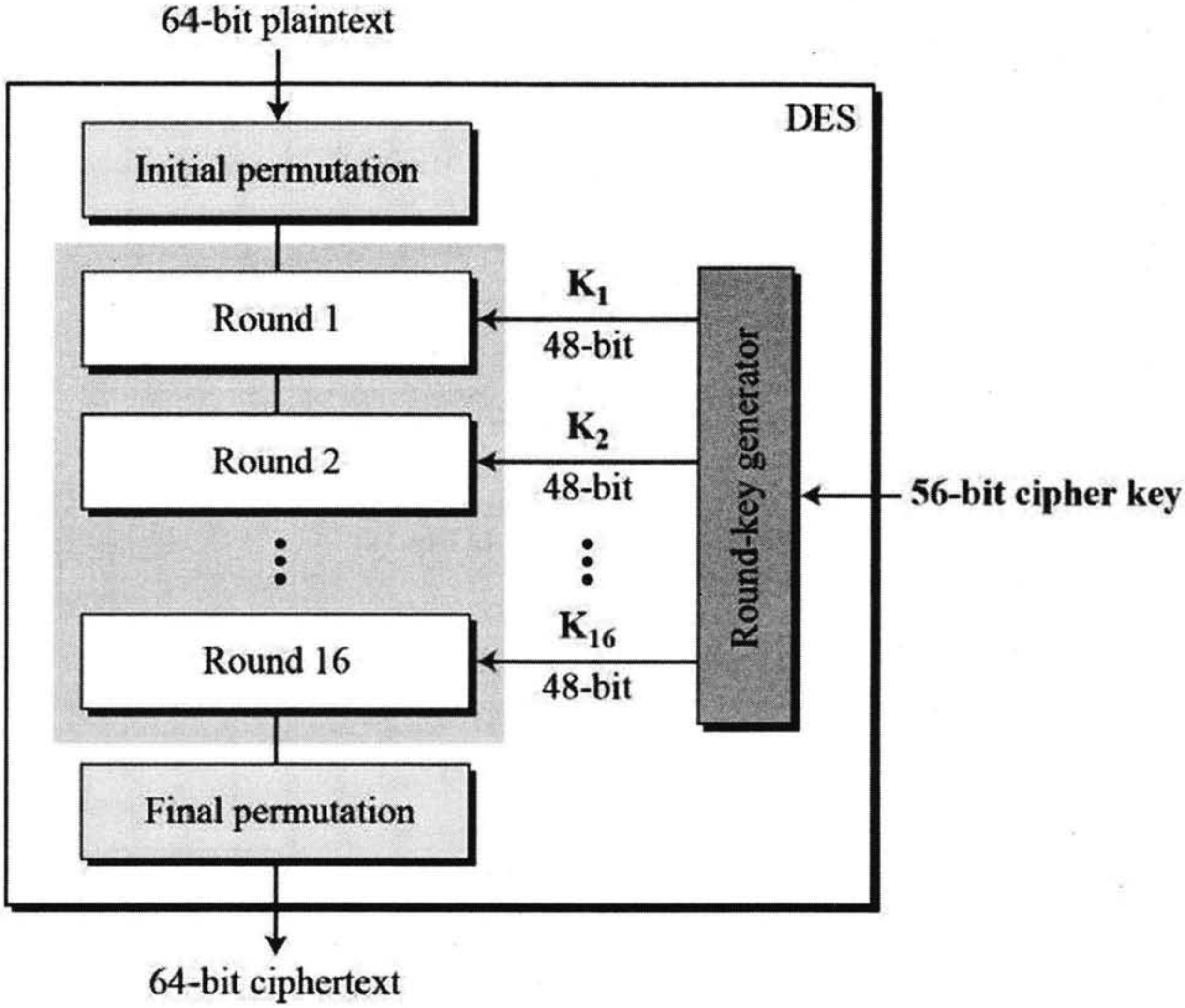
2. Error detection and error correction techniques.

   Types of errors - Single bit error, Burst error

   Error detection- Vertical redundancy check(VRC), Longitudinal redundancy check(LRC), Cyclic redundancy check(CRC) , Checksum

   Error correction - Single-bit error correction, Hamming code Burst error correction.

3. General Structure of DES.



Since DES is based on the Feistel Cipher, all that is required to specify DES is –

- Round function
- Key schedule
- Any additional processing – Initial and final permutation

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** – A small change in plaintext results in the very grate change in the ciphertext.
- **Completeness** – Each bit of ciphertext depends on many bits of plaintext.

PART-B

4. Transmission control protocol.

TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control, and—because it is meant to provide error-free data transmission—handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive. In the Open Systems Interconnection (OSI) communication model, TCP covers parts of Layer 4, the Transport Layer, and parts of Layer 5, the Session Layer.

5. Email Security

Email security refers to the collective measures used to secure the access and content of an email account or service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts.

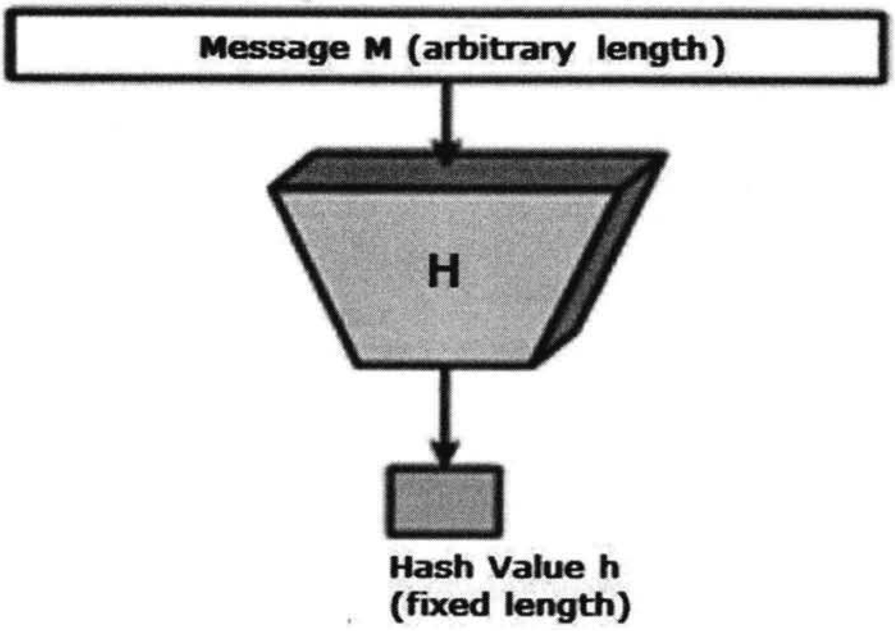
An email service provider implements email security to secure subscriber email accounts and data from hackers - at rest and in transit.

6. Hash functions of cryptography.

Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called **message digest** or simply**hash values**. The following picture illustrated hash function –



PART-C

7. Answer any five

a) What are the responsibilities of data link layer?

Specific responsibilities of data link layer include the following

a) Framing b) Physical addressing c) Flow control d) Error control e) Access control

b) Local Area Network

A LAN is a common name used to describe a group of devices that share a geographic location. LAN is limited to single building or campus.

c) The principle elements of a cryptosystem are:

1.plain text
2.Encryption algoritm
3.Public and private key
4.Cipher text
5.Decryption algorithm

d) Masquerade:

Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgements of message receipt or no receipt by someone other than the message recipient.

e) What is Kerberos? What are the uses?

Kerberos is an authentication service developed as a part of project Athena at MIT. Kerberos provide a centralized authentication server whose functions is to authenticate servers

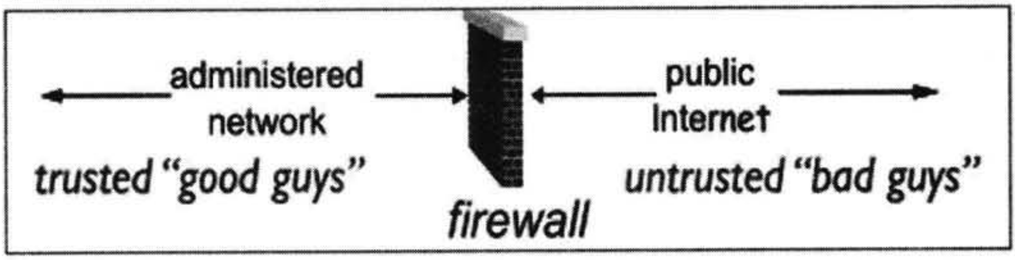
f) Give the benefits of IP security?

- Provide security when IP security implement in router or firewall.
- IP security is below the transport layer is transparent to the application.
- IP security transparent to end-user.
- IP security can provide security for individual user.

g) Firewall

Firewall is a network device that isolates organization's internal network from larger outside network/Internet. It can be a hardware, software, or combined system that prevents unauthorized access to or from internal network.

All data packets entering or leaving the internal network pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.



PART-D

8.Answer any six:

(a) Types of errors

a) Single-bit error. b) Burst-bit error

(b) Two interfaces provided by protocols

Service interface and Peer interface

(c)Flow Control

Flow control refers to a set of procedures used to restrict the amount of data. The sender can send before waiting for acknowledgment.

(d) The ways to address the framing problem

The framing problem can be addressed by the following protocols:

Byte-Oriented Protocols(PPP) ,Bit-Oriented Protocols(HDLC) ,Clock-Based Framing(SONET)

(e) cryptanalysis

It is a process of attempting to discover the key or plaintext or both.

(f) Virus.

A virus is a program that can infect other program by modifying them the modification includes a copy of the virus program, which can then go on to infect other program.

(g) Types of attack

Passive attack: Monitoring the message during transmission. Eg: Interception
Active attack: It involves the modification of data stream or creation of false data stream. E.g.: Fabrication, Modification, and Interruption