UNIT- I

Introduction

An interconnected collection of **autonomous** computers is called a computer network. Two computers are said to be interconnected if they are able to exchange the information. If one computer can forcibly start, stop and control another one, the computers are not autonomous. A system with one control unit and many slaves is not a network, nor is a large computer with remote printers and terminals.

In a **Distributed system**, the existence of multiple autonomous computers is transparent(i.e., not visible) to the user. He can type a command to run a program and it runs. It is up to the operating system to select the best processor, find and transport all the files to that processor, and put the results in the appropriate place.

The user of a distributed system is not aware of that there are multiple processors; it looks like a virtual uniprocessor. Allocation of jobs to processors and files to disks, movement of files between where they are stored and where they are needed, and all system function are automatic.
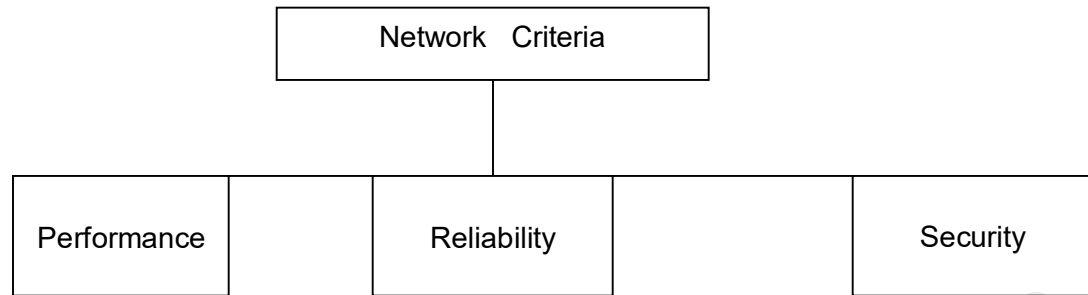
With a network, users must explicitly log onto one machine, explicitly submit jobs remotely, explicitly move files around and generally handle all the network management personally. The distinction between Network and distributed system lies with software (OS) rather than software. In network user invokes, in distributed system the system invokes.

A network is a set of devices connected by media links. Anode can be a computer, printer or any other device capable of sending and receiving data generated by other nodes on the network. The links connecting the devices are often called communication channels.

Networks use **Distributed processing,** in which a task is divided among multiple computers. Advantages of Distributed processing are

- Security/ Encapsulation
- Distributed data bases
- Faster problem solving
- Security through Redundancy
- Collaborative processing

Network Criteria

Computer Networks

```
                    ┌─────────────────────┐
                    │  Network   Criteria │
                    └─────────────────────┘
                               │
        ┌──────────────┬───────┴───────┬──────────────┐
  ┌───────────┐   ┌───────────┐   ┌───────────┐
  │Performance│   │Reliability│   │ Security  │
  └───────────┘   └───────────┘   └───────────┘
```

Performance:

The performance can be measured in many ways and depends on number of factors.

- Number of users
- Type of transmission medium
- Hardware
- Software

Reliability

This is measured by the following factors

- Frequency of failure
- Recovery time of a network after a failure.
- Catastrophe.

Security

Network security issues include protecting data from the following

- **Unauthorized access**

- **Viruses**

Applications
- Accessing Remote databases
- Accessing Remote programs
- Value added communication facility
- Marketing and sales
- Financial services
- Manufacturing
- Electronic message
- Directory services
- Information services
- Teleconferencing
- Cellular telephone
- Cable television

Computer Networks

Network Structure
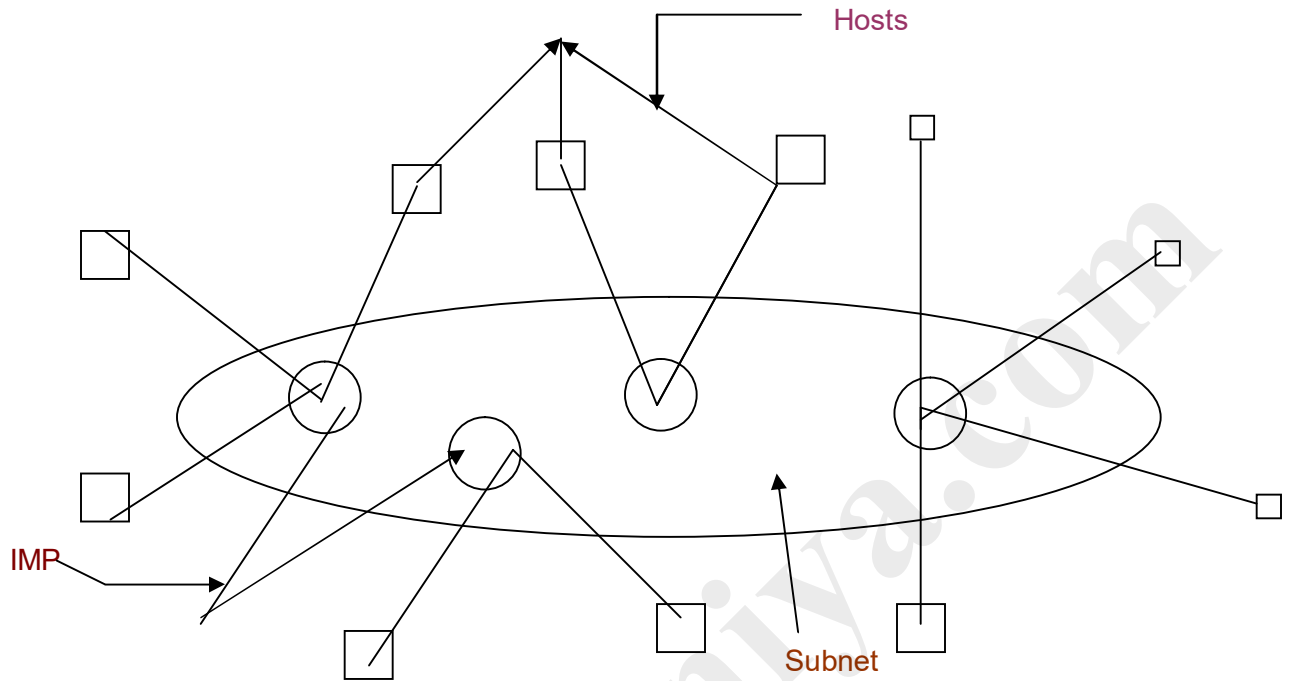
The end systems are called the HOSTS. The hosts are connected through a communication subnet or simply Subnet as shown in fig.

The subnet consists of two parts: a) Transmission lines b) Switching elements.

The Transmission lines transmit the raw bits. The Switching elements are specialized computers, which switches packets. This is called **Interface Message Processor** (IMP) or Router or data switching exchanges or packet switching nodes.

The data can be transmitted through the subnet in two ways. They are

a) Point to point   or   store and forward

b) Broad casting

Network Architecture

To reduce the design complexity, most networks are organized as a series of layers or levels, each built upon on the one below it. The number of layers, the name of each layer ,the contents of each layer ,and the function of each layer differ from network to network However, in all networks the purpose of each layer is to offer certain services to the higher layers ,shielding those layers from the details of how the offered services are actually implemented.

Computer Networks

Layer **n** on one machine carries on a conversation with layer **n** on another machine. The rules and conventions used in this conversation are collectively known as the layer **n** **Protocol.**

The entities comprising the corresponding layers on different machines are called **Peers.**
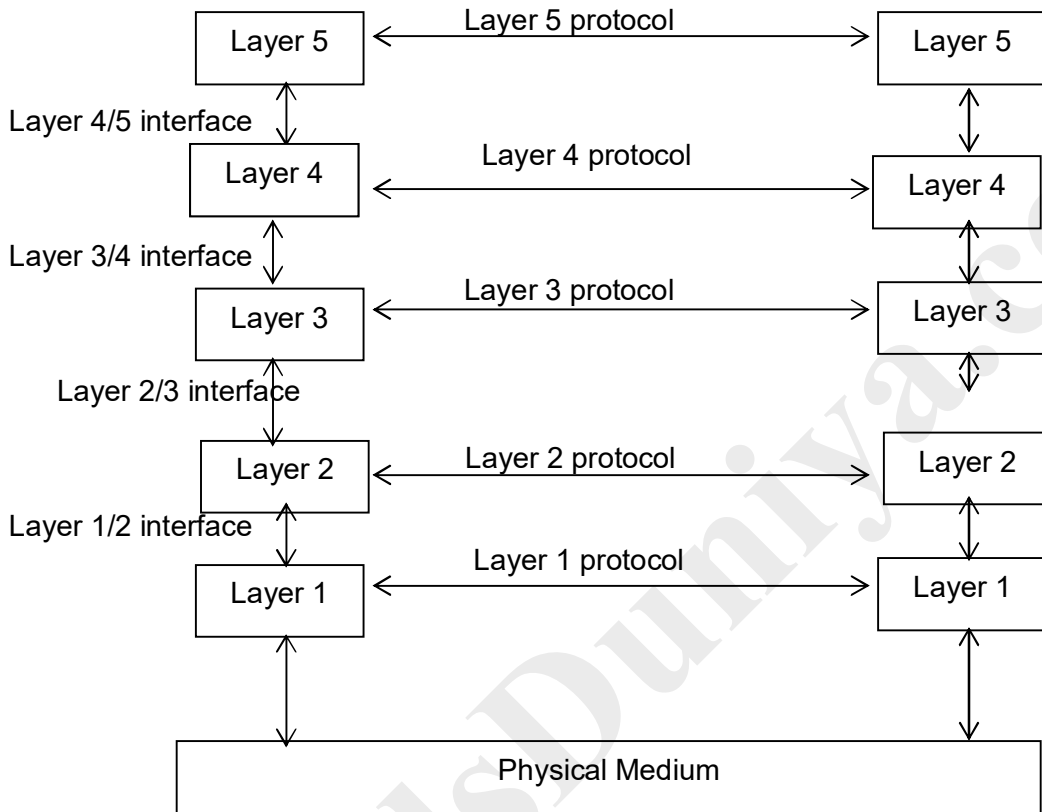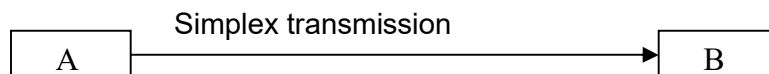

Layers, protocols and interfaces.

The **interface** defines which primitive operation and services the lower layer offers to the upper one.

A set of layers and protocol is called **network architecture**.

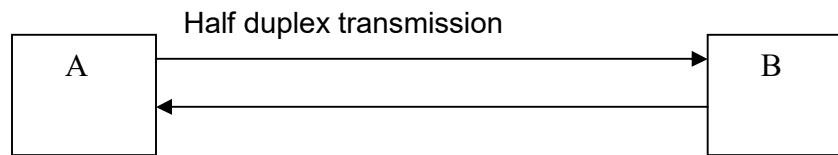**Data transfer methods**:

a. Simplex communication:

Data will be transferred in one direction only.

Ex: Keyboards, Monitors
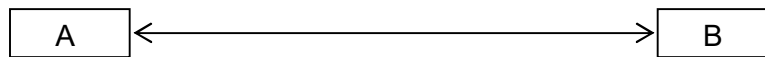
b. Half -- duplex communication:

Data will be transferred in both the directions, but not simultaneously.

Computer Networks

Half duplex transmission

Ex: One way bridge with two directional traffic.

c. Full – duplex   communication:

Data will be transferred in both the directions   simultaneously.

Ex: Two-way road, where traffic will be there in both the directions.

REFERENCE MODELS

The ISO OSI REFERENCE MODEL

In 1947, the International Standards Organization (ISO) proposed a network model that covers all network communications .This model is called Open Systems Interconnection (OSI) model. An open system is a model that allows any two different systems to communicate regardless of their underlying architecture.

The OSI model is built of seven layers: Physical (layer 1), Data link (layer 2), Network (layer 3), Transport (layer 4), Session (layer 5), Presentation (layer 6) and Application layers (layer 7).
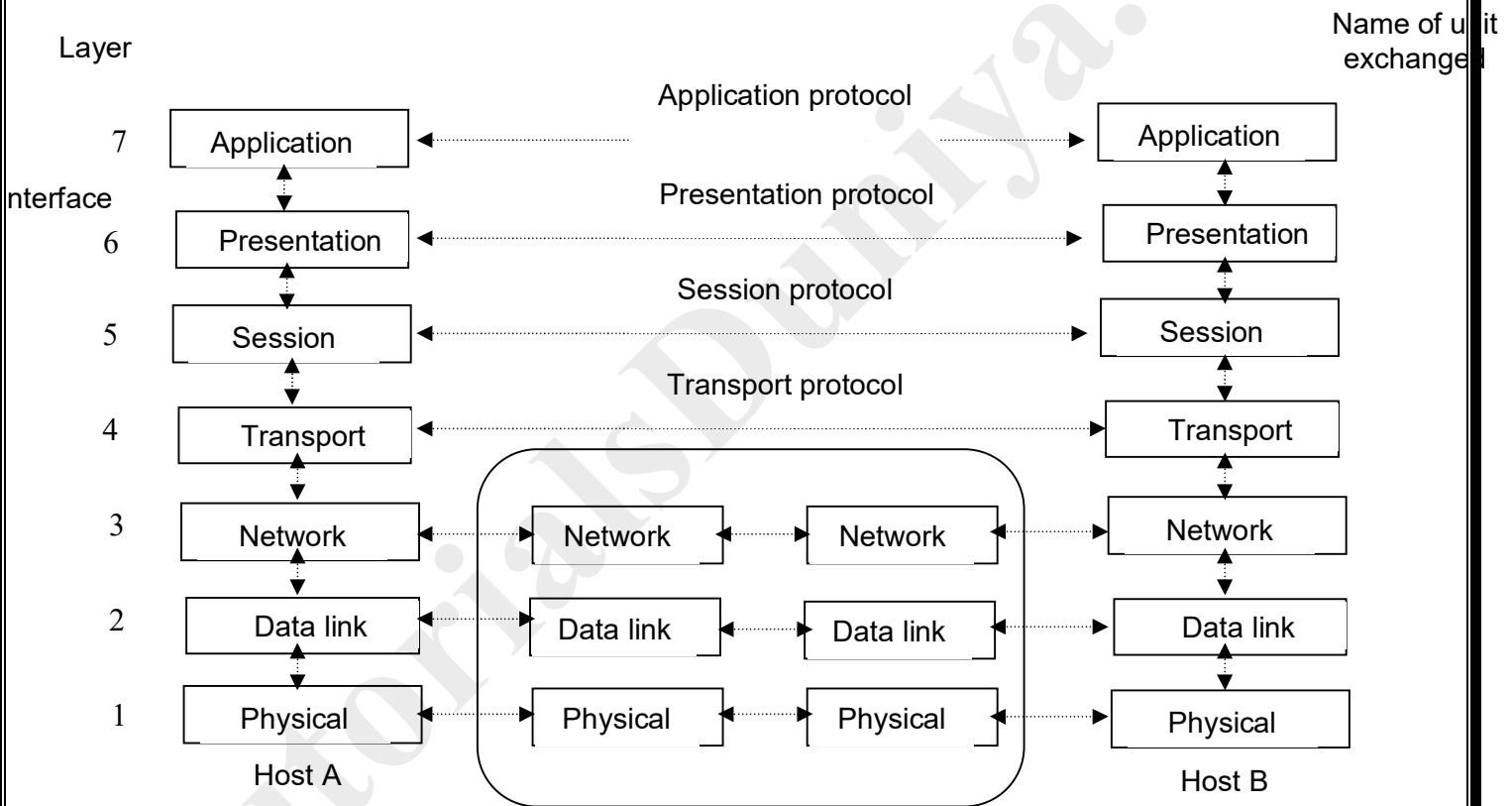
Within a single machine, each layer calls upon the services of the layer just below it.layer 3,for example, uses the services provided by layer 2 and provides for layer 4.Between machines layer on one machine communicates with layer x on another machine. This communication is governed by protocols. The processes on each machine that communicate at a given layer are called peer **–to – peer processor.**

At the physical layer, communicate is direct: Machine A sends a stream of bits to machine B. At the higher layers, however, communication must move down through the layers on machine A, over to machine B, and then back up through the layers. Each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers. Headers are added to the message at layers 6, 5, 4, 3, and 2.At layer 1 the entire message converted to a form that can be transferred to the receiving machine. At the receiving machine,

Computer Networks

the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.

Organization of the layers:

The seven layers can be thought of as belonging to three subgroups. Layers 1, 2, 3 –are the network support layers; they deal with the physical aspects of moving data from onr machine to another. Layers 5, 6, 7—can be thought of as user support layers: they allow interoperability among unrelated software systems. Layer 4,the transport layer, ensures end to end reliable transmission while layer 2 ensures reliable transmission on a single link. The upper layers are implemented almost always in software; lower layers are a combination of hard ware and software, where as physical layer is mostly hardware.

Layer

Name of unit exchanged

7	Application	Application protocol			Application
Interface 6	Presentation	Presentation protocol			Presentation
5	Session	Session protocol			Session
4	Transport	Transport protocol			Transport
3	Network	Network	Network		Network
2	Data link	Data link	Data link		Data link
1	Physical	Physical	Physical		Physical
	Host A				Host B

The OSI reference model

Computer Networks

FUNCTIONS OF LAYERS:

Functions of the Layers

Physical Layer :

- ❖ Physical characteristics of interfaces and media
- ❖ Representation of bits.
- ❖ Data rate
- ❖ Synchronisation of bits
- ❖ Line configuration (point to point or multipoint)
- ❖ Transmission Mode
- ❖ Physical Topology

Data Link Layer :
- ❖ Framing
- ❖ Physical addressing
- ❖ Error control
- ❖ Flow control
- ❖ Access control

Network Layer :
- - Routing
- - Congestion control
- - Billing

Transport Layer :
- - Service – Point addressing
- - Segmentation and reassembly
- - Flow control
- - Error control

Session Layer :
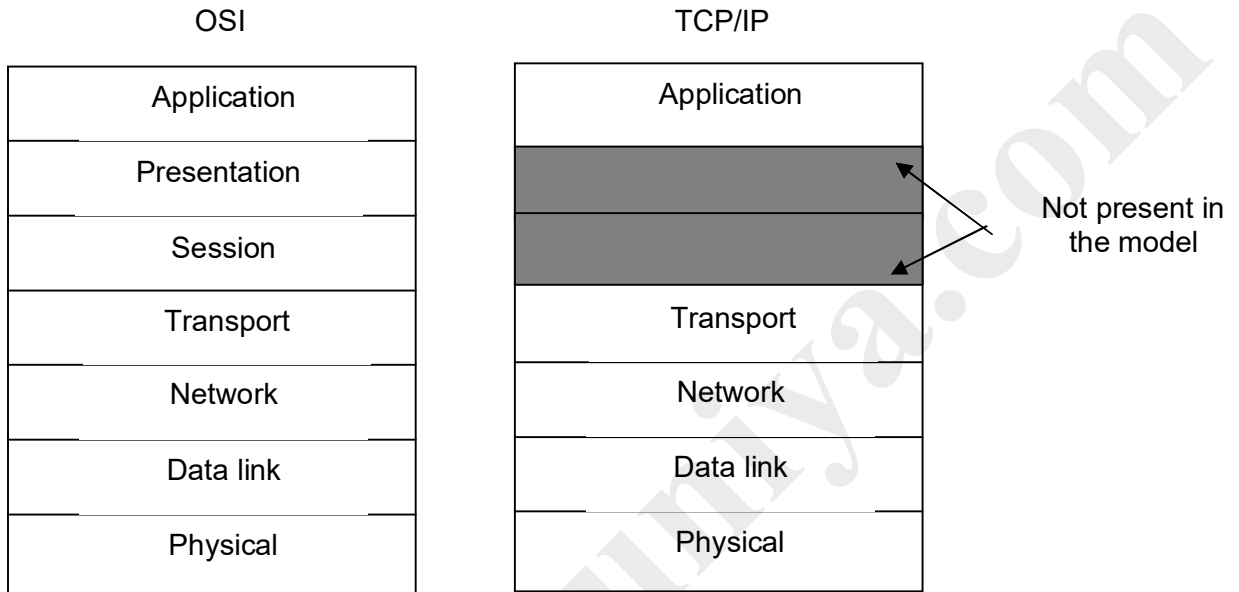- -Dialog control
- -Synchronization

Presentation Layer :
- - Data encoding
- - Encryption
- - Compression

Computer Networks

Application Layer :

- File Transfer

- Mail services

- Directory services
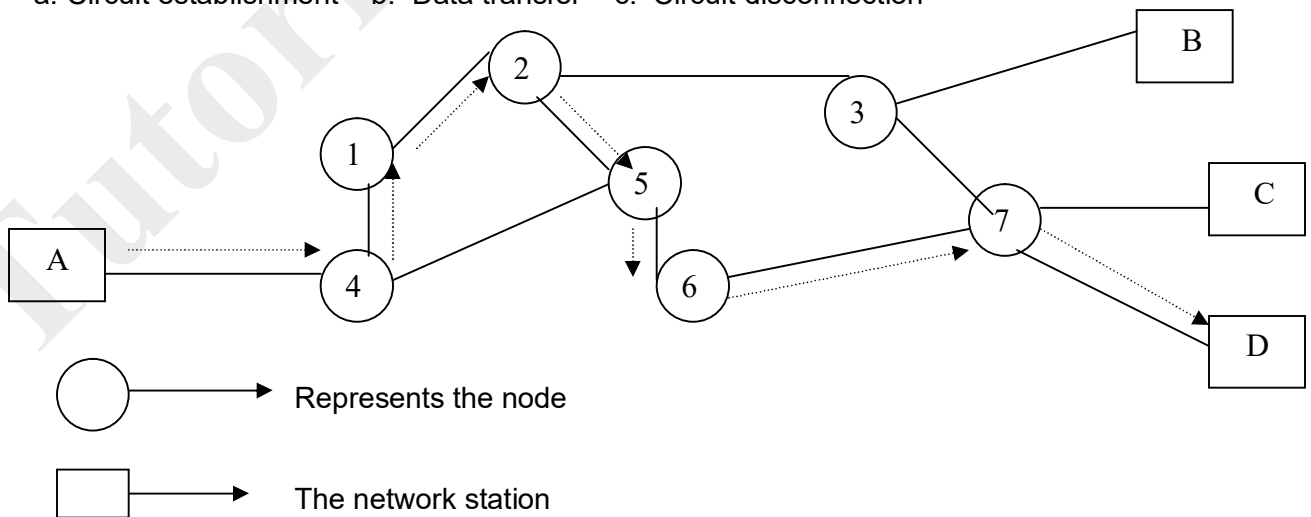
TCP/IP reference model

Switching Methods

Two different types of switching methods are used: Circuit switching and Packet switching.

Circuit Switching

In this switching there are three phases

a. Circuit establishment   b. Data transfer   c. Circuit disconnection

Computer Networks

Suppose if we want to send the data, say, from A to D. before sending the data a circuit will be established between A to D as shown in fig with doted lines. All the data will follow the same path. After data is transferred the circuit will be disconnected.

Circuit switching

Virtual packet switching

Computer Networks
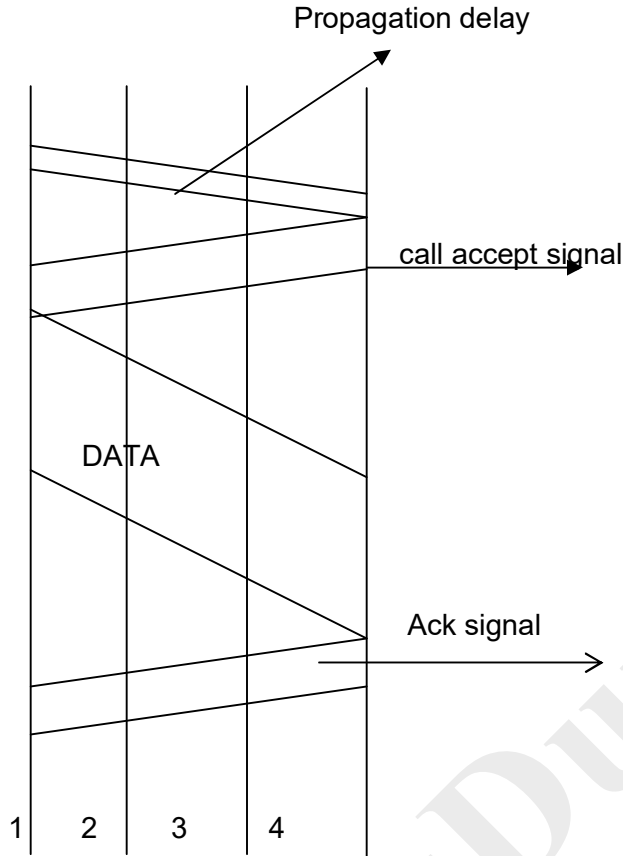
Packet switching will be done in two ways.

1. Virtual Packet switching   2. Data gram Packet switching

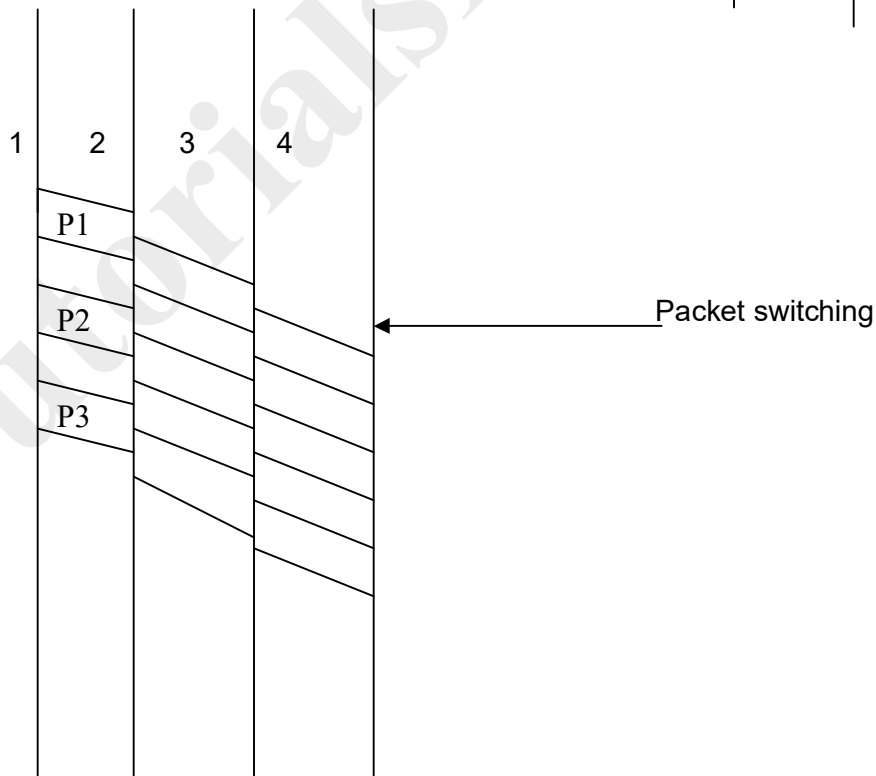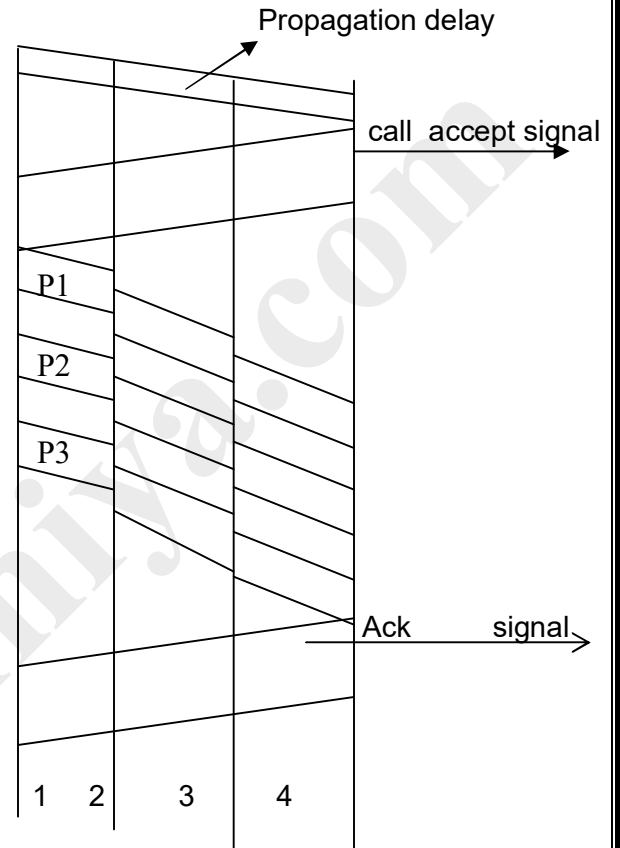| Circuit switching	Data gram packet	Virtual packet
Dedicated transmission	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of packets	Transmission of packets
Messages are not stored	Packets are stored	Packets are stored until delivered
Path will be established for entire conversation	Route will be established for each packet.	Route will be established for entire conversation
Fixed bandwidth transmission	Dynamic use of bandwidth	Dynamic use of bandwidth

X.25

X.25 is a packet switching wide area network.

It is an interface between DCE and DTE for terminal operation in the packet mode on public data networks.

It defines how a packet- mode terminal connected to a packet network for the exchange of data.

It describes the procedures for establishing maintaining and terminating connections.

X.25 is known as a subscriber network interface (SNI).

It defines how the user's DTE communicates with the network and how packets are sent over that network using DCE's.

X.25 has three layers:

- Physical layer
- Frame layer and
- Packet layer

Physical Layer:

At the physical layer, X.25 specifies a protocol called X.21.

This is similar to other physical layer protocols.

Computer Networks

Frame Layer:

X.25 provides data link control using a bit oriented protocol called link access procedure balanced (LAPB).

Packet Layer:

The Network layer in x.25 is called the Packet Layer Protocol (PLP).

- This layer is responsible for establishing the connection, transferring data and terminating the connection.
- It is also responsible for creating the virtual circuits and negotiating network services between two DTEs.
- The Frame layer is responsible for making a connection between a DTE and DCE, the Packet layer is responsible for making a connection between two DTEs.
- End-to-End flow and error control between two DTEs are under the jurisdiction of the Packet Layer.

Examples of Networks

NOVEL NETWARE

The most popular network in pc world system is novel netware.it was designed to be used by companies from a mainframes to a network of PCs.

1. In this system, each user has a desk top PC functioning as a client.
2. Some number of power full PCs operate as servers providing file services ,data base services and other services to a collection of clients it uses a proprietary protocol.
3. It is based an old Xerox network system, XNS with various modifications. Because of five-layers, it looks much like TCP/IP than ISO OSI.
4. Physical and data link layer can choose an Ethernet, IBM token ring and ARC net protocols.
5. The network layer runs an unreliable connectionless Internet work protocol called ARC net protocols.
6. It passes packets from source to destination transparently; even both are of different networks.
7. Application layer uses SAP (Service Advertising protocol), to broadcast a packet and tell what

Computer Networks

service it offered. These packets are collected by special agents of a process running on the router machine. With this information they construct databases of which server are running where.

8. When client machine is booted, it broadcast s a request asking where the nearest server is. The agent on the local router sees, looks into the database of servers and matches up the request with the best server; with this the client can now establish a NCP connection and act like client-server model in all aspects.

Integrated Services Digital Network (ISDN)

ISDN was developed by ITU- T in 1976.It is a set of protocols that combines digital telephony and data transport services. The whole idea is to digitize the telephone network to permit the transmission of audio, video, and text over existing telephone lines.

The goal of isdn is to form a wide network that provides universal end –to – end connectivity over digital media. This can be done by integrating all of the separate transmission services into one without adding links or subscriber lines.

HISTORY

Voice Communication over Analog Networks

Initially, telecommunications networks were entirely *analog networks* and were used for the transmission of analog information in the form of voice.

Voice and Data Communication over Analog Networks

With the advent of digital processing, subscribers needed to exchange data as well as voice. Modems were developed to allow digital exchange over analog lines.

Analog and Digital services to Subscribers

To reduce cost and improve performance, the telephone companies gradually began to add digital technologies while continuing their analog services to their customers.

Computer Networks

Integrated Digital Network (IDN)

Next, customers began to require access to a variety of networks, such as packet- switched networks and circuit –switched networks. To meet these needs the telephone companies created Integrated **Digital Network (IDN).** An IDN is a combination of networks available for different purposes.

Integrated Services Digital Network (ISDN)

The ISDN integrates customer service with the IDN. With ISDN all customers' services become digital rather than analog and will allow the customers services to be made available on demand.

SERVICES

The purpose of the ISDN is to provide fully integrated digital services to users. These services fall in to three categories: bearer services, teleservices, and supplementary services.

Bearer service

Bearer services provide the means to transfer information (voice, data, and voice) between users without the network manipulating the content of information.

Tele Service

In teleservices the network may change or process the contents of the data. These services correspond to layers 4 – 7 of the OSI ISO model. this service include telephony,telefax,videotex, telex and teleconferencing.

Supplementary service

Supplementary services are those services that provide additional functionality to the bearer service and teleservices. These services include call waiting, reverse charging, and message handling.

Computer Networks

Supplementary
services

Tele Services

Telephony	Telefax	Teletex

Telex

| Call
waiting |
|--------|

| Reverse
charging |
|---------|

• • • • •

Teleconferencing

• • •

| Circuit
switching | Packet
switching. | Cell
switching |
|---------|----------|------|

•
•
•
•

| Message
Handling |
|---------|

Bearer Services
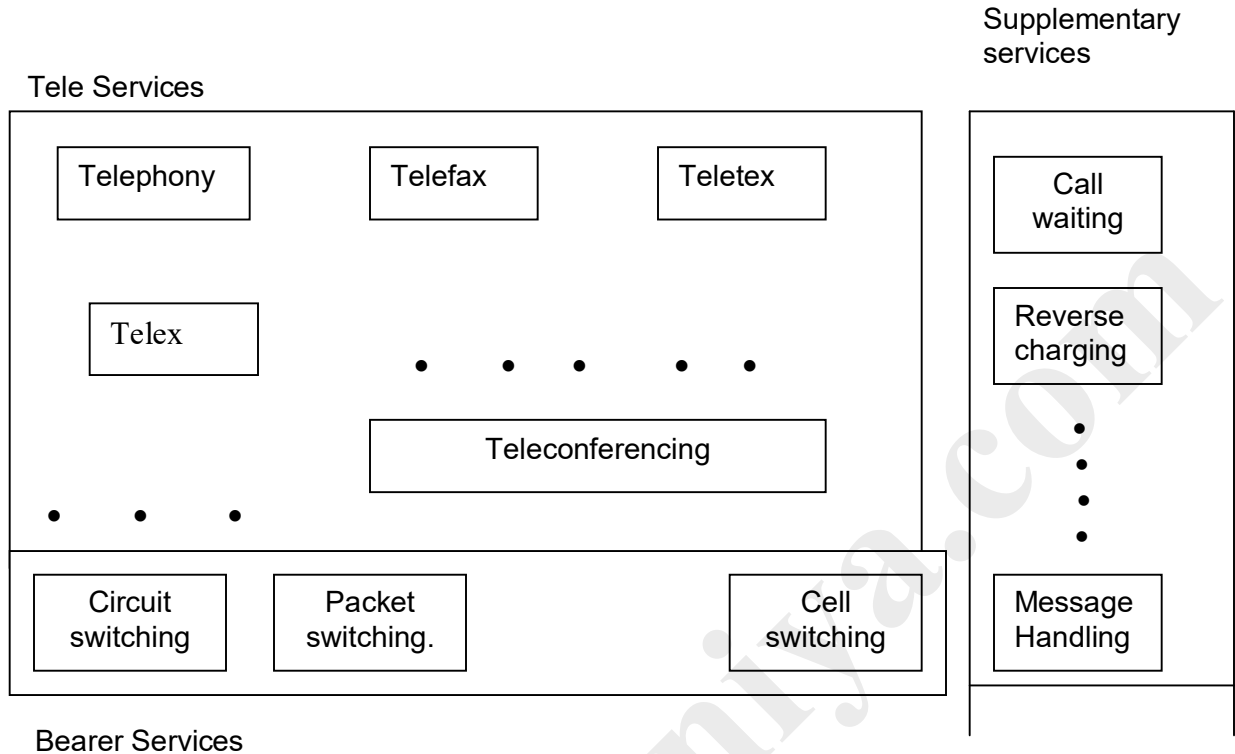
SUBSCRIBER ACCESS TO THE ISDN

To allow flexibility, digital pipes between customers and the ISDN office are organized into multiple channels of different sizes. The ISDN standard defines three channel types, each with a different transmission rate: bearer channels, data channels, and hybrid channels

Channel Rates

Channel	Data Rate(Kbps)
Bearer (B)	64
Data (D)	16,64
Hybrid (H)	384,1536,1920

B Channel

A B channel is defined at a rate of 64 Kbps .It is the basic user channel and can carry any type of digital information in full duplex mode as long as the required transmission rate does not exceed 64 Kbps. A B channel can be used to carry digital data, digitized voice, or other low data – rate information.

D Channel

A D channel can be either 16 or 64 Kbps, depending on the need of the user. The primary function of a D channel is to carry control signaling for the B channels. A D channel carries the

Computer Networks

control signaling for all the channels in a given path, using a method called common – channel (Out – of – band) signaling.

Less common uses for the D channel include low- rate data transfer and applications such as telemetry and alarm transmission.

H Channel

H Channels are available with data rates of 384 Kbps (HO), 1536 Kbps (H11), or 1920(H12). These e rates suit for high data rate applications such as video, teleconferencing and so on.
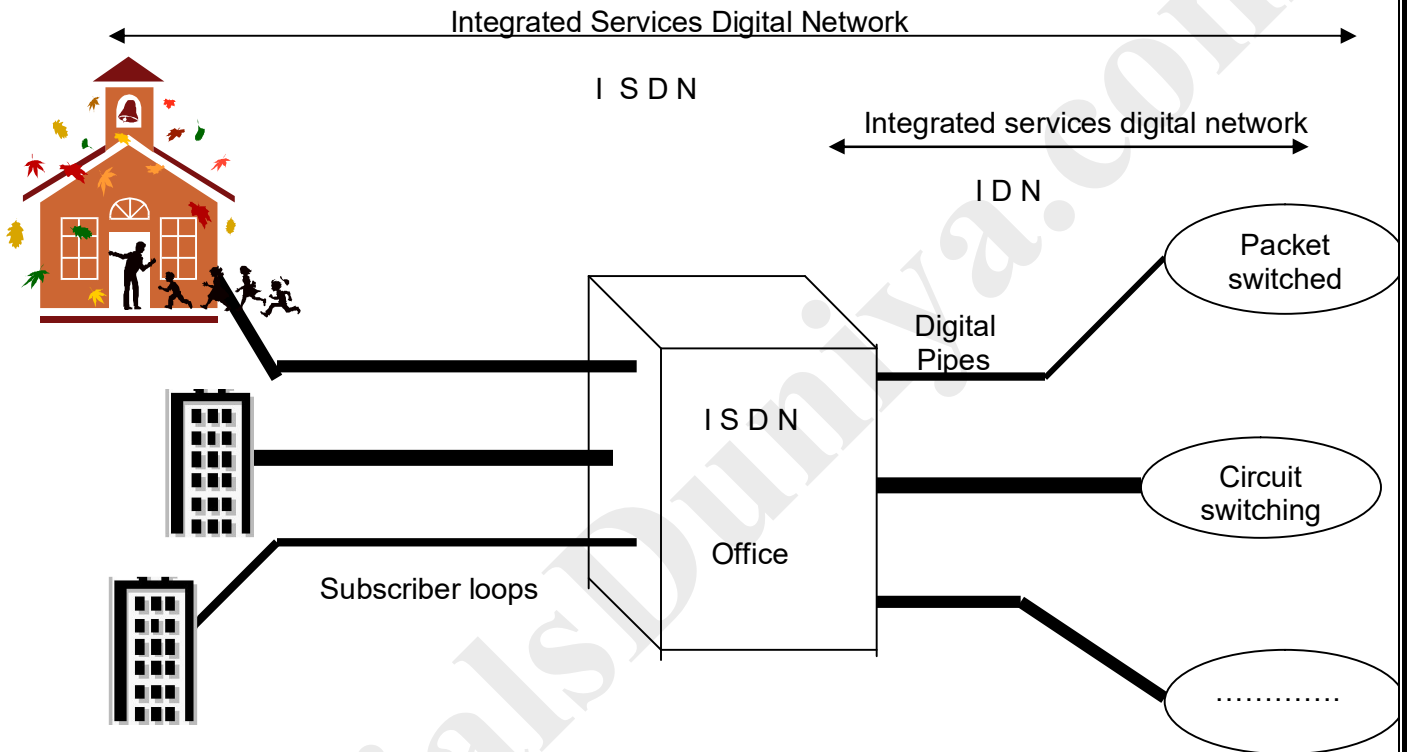
User Interfaces

Digital subscriber loops are two types: basic rate interface (BRI) and primary rate interface (PRI) .Each type is suited to a different level of customer needs .Both include one D channel and some number of either B or H channels.

B R I

The *basic rate interface* specifies a digital pipe consisting of two B channels and one 16Kbps D channel.

64(B1) + 64 (B2) +16(D) +48(over head) = 192Kbps
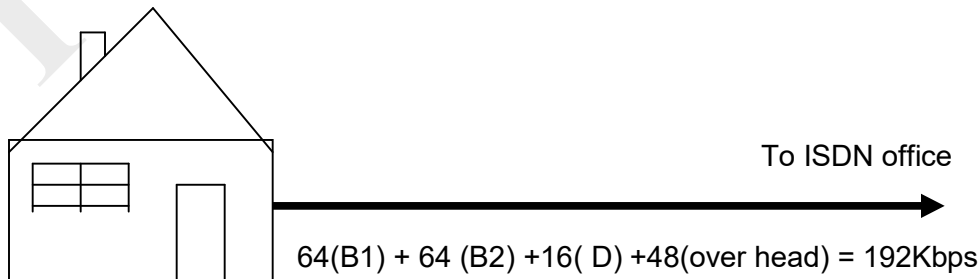
Computer Networks

BRI requires a digital pipe of 192 Kbps as shown in the fig. Conceptually, the BRI service is like a large pipe that contains three smaller pipes, two for the B channels and one for D channel. The remainder of the space inside the large pipe carries overhead bits required for its operation.

The BRI is designed to meet the needs of residential and small – office customers.

P R I

The usual PRI specifies a digital pipe with 23 B channels and one 64 Kbps D channel.

To ISDN office

P R I   1.544 Mbps

64 x 23 (B1 – B23) + 64 (D) + 8 (overhead)
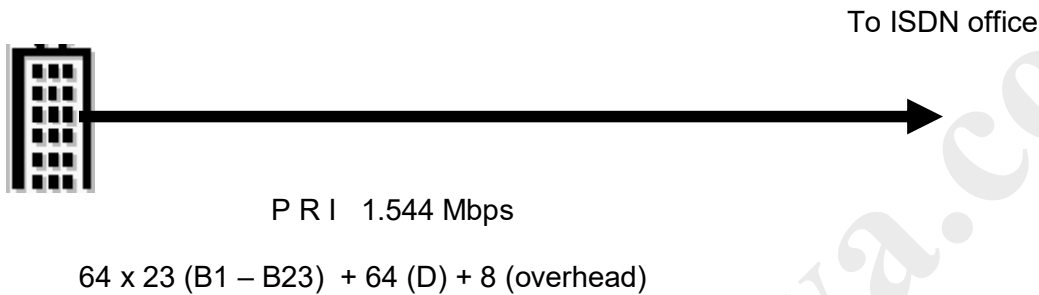
PRI requires a digital pipe of 1.544 Mbps. Conceptually, the PRI services is like a large pipe containing 24 smaller pipes, 23 for the B channels and for the D channel. The rest of the pipe carries the overhead bits.

One PRI can provide full – duplex transmission between as many as 23 sources and receiving nodes. The individual transmission are collected from their source and multiplexed on to a single path for sending to the ISDN office.

Functional Grouping

Functional Grouping used at the subscriber's premises includes network terminations, terminal equipment and terminal adapters, enables users to access the services of the BRI and PRI.

Network Teriminator 1 (NT1)

An NT1 device controls the physical and electrical termination of the ISDN at user's internal system to the digital subscriber loop. These functions are comparable to those defined for the OSI physical layer.

An NT1 organizes the date stream from connected subscribers into frames that can be sent over the digital pipe, and translates the frame received from the network into a format usable by the subscriber's device.

Network Teriminator 2 (NT2)

A NT1 device performs functions at the physical layer, data link, and net work layers of the OSI model.NT2 provide multiplexing (layer 1),flow control (layer 2), and packetzing (layer 3).An NT2 provides intermediate signal processing between the Data – generating devices and an NT1.There must be a point to point connection between an NT1 and NT1 ..NT2s are used primarily to interface between a multi-user system and an NT1 in a PRI.

NT2s can be implemented by a variety of equipment types like a **private branch exchange** (digital **PBX**), a **LAN** can function as an NT2.

Computer Networks

Terminal Equipment 1 (TE1)

The TE is used by ISDN in the same manner as DTE in other protocol. Examples of TE1 are digital telephones, integrated voice/data terminals, digital facsimiles.

Terminal Equipment 2 (TE2)

To provide backward compatibility with a customer's existing equipment, the ISDN standard defines a second level of terminal equipment called **Terminal Equipment 1 (TE1).**This is a non ISDN device, such as terminal, workstation or regular telephone. This can be used with the help of another device called a **terminal adapter (TA).**

Reference Points

This refers to the label used to identify individual interface between two elements of an ISDN installation. There are four reference points that defines the interface between a subscriber's equipment and the network. They are R, S, T and U.

Reference Point R defines the connection between a TE2 and a Ta. Reference Point S defines the connection between a TE1 or TA and an NT1 or NT2. Reference Point T defines the interface between an NT2 and NT1. Reference Point U defines the interface between an NT1 and the ISDN office.

Computer Networks
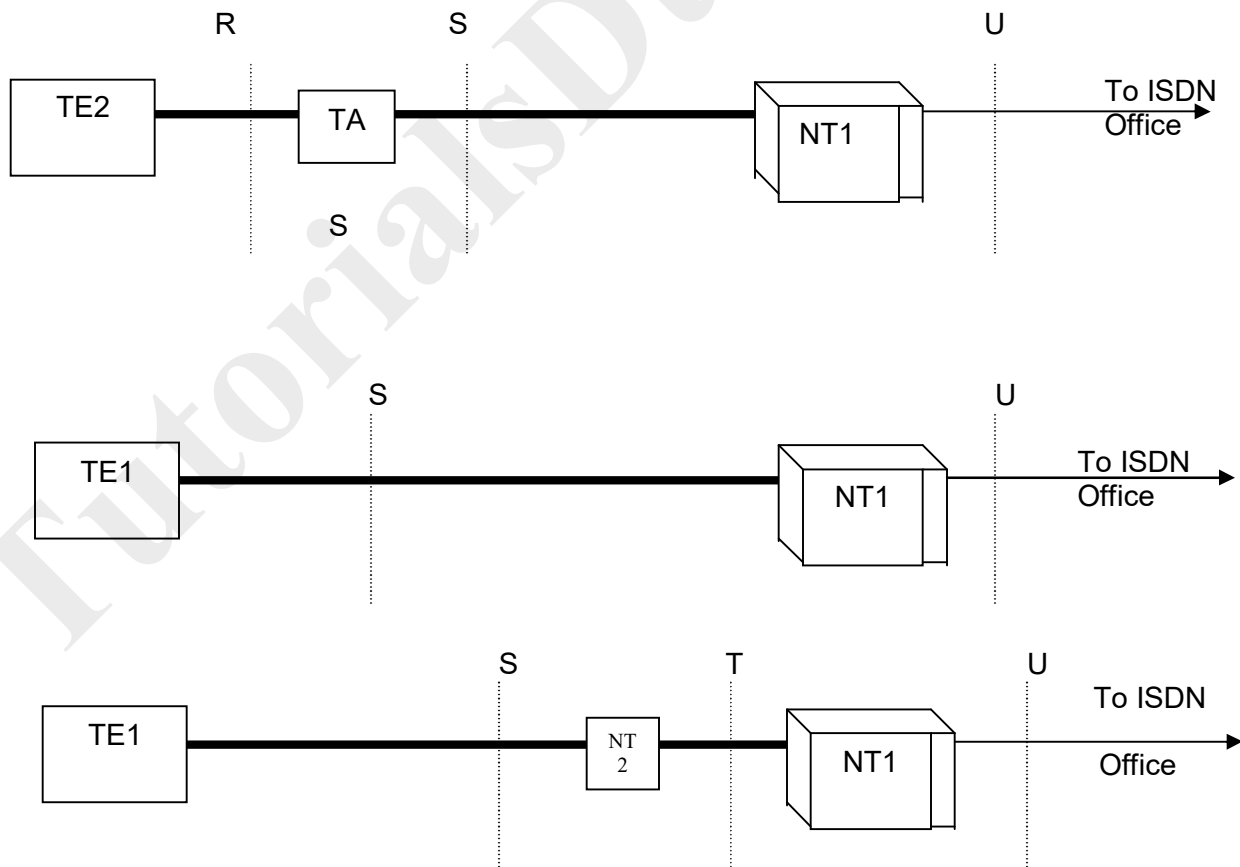
Reference Points

The ISDN Layers

Since the ISDN specifies two different channels (B and D) with different functionalities ,unlike the ISO OSI (which has seven layers) the ISDN is defined in three separate planes : the **user plane**, the **control panel** ,and **the management plane**. All three planes are divided into seven layers that correspond to the OSI model.

	B channel	D channel
Layers 4,5,6,7	User's choice	
Network	X.25 and others	Call control Q.931
Data link	LAPB and others	LAPD
Physical	BRI (I.430) & PRI (I.431)	

Simplified layers of ISDN

Physical Layer

The ISDN physical layer specifications are defined by two ITU-T standards: L430 for BRI access and I.431 for PRI access. These standards define all aspects of the BRI and PRI. Of these aspects, four are of primary importance:

- The mechanical and electrical specifications of interfaces R, S, T and U.
- Encoding
- Multiplexing channels to make them carriable by the BRI and PRI digital pipe.
- Power supply

Data Link Layer

B and D channels use different data link protocols. B channels use LAPB protocol. The D channel uses link access procedure for D channel (LAPD).

Network Layer

Once a connection has been established by the D channel, the B channel sends data using circuit switching, X.25,or other similar protocols. The network layer packet is called a message.

Computer Networks

BROAD BAND ISDN

When the ISDN was originally designed data rates of 64 Kbps to 1.544 Mbps were sufficient to handle all existing transmission needs. As applications using the telecommunications network advanced, however, these rates proved inadequate to support many applications. In addition, the original bandwidths provided too narrow to carry the large numbers of concurrent signals produced by a growing industry of digital services providers.

To provide for the needs of the next generation of technology, an extension of ISDN, called broadband ISDN is under study. B-ISDN provides subscribers to the network with data rates in the range of 600 Mbps, almost 400 times faster than the PRI rate.

Services

B-ISDN provides two types of services: interactive and distributive.

Interactive services

Interactive services are those that require two-way exchanges between either two subscribers or between a subscriber and a service provider. These services are of three types: conversational, messaging and retrieval.

Conversational

These services are those, such as telephone calls, that support real time exchanges. These real time services can be used for telephoning, video telephoning, and video conferencing, data transfer.

Messaging

These services stored and forward exchanges. These are bi-directional, meaning that all parties in an exchange can use them at same time. These services include voice mail, data mail, video mail.

Retrieval

These services are those used to retrieve information from a central source called an information center. These services are like libraries; they must allow public access to retrieve information on demand. And information is not distributed unless asked for.

Distributive services

These services are unidirectional services sent from a provider to subscribers without the subscriber having to transmit a request each time a service is desired. These services can be without or with user control.

Access method

B-ISDN defines three access methods to provide for three levels of user needs. They are:

- 155.520 Mbbs full duplex symmetrical
- 155.520 Mbbs asymmetrical
- 622.080 Mbbs full duplex

*   *   *   *   *

Computer Networks

Expected Questions

1. Describe ISO OSI model with a neat sketch.

2. Compare and contrast the ISO OSI model with TCP/IP model.

3. Explain Novel NetWare and the ARPANET.

4. Explain the working of X.21

5. Explain this network structure

6. Explain different types of transmission media used in data communication

7. Give advantages and disadvantages of fiber optic cable over metallic cable

8. Draw the B-ISDN reference model and explain the functions of each layer.

9. Explain about ATM. What are the advantages of using fixed length cells.

10. Explain X.25 network.

11. What are the applications of networks?

12. Write the difference between B-ISDN and N-ISDN

13. Explain the following items

    a) IMP

    b) HOST

    c) Subnet

14. What are the advantages of layered architecture

15. Explain the goals of a computer network.

****

Computer Networks

Review Questions

1.Which OSI layers are the network support layers?

2. Which OSI layers are the user support layers?

3.What is the difference between network layer delivery and transport layer delivery?

4.List the layers of the OSI model.

5.What is a peer-to-peer process?

6.How does information get passed from one layer to the next?

7.What are the concerns of the Physical Layer?

8.What are the responsibilities of the data link layer?

9. What are the responsibilities of the network layer?

10. What are the responsibilities of the transport layer?

11.The transport layer creates a connection between the source and destination. What are the three events involved in a connection?

12. What are the responsibilities of the session layer?

13. What are the responsibilities of the presentation layer?

14. What are the services provided by the application layer?

15.Name two categories of transmission media.

16.How do guided media differ from unguided?

17.What are the three major classes of guided media.

18.What is the major advantage of shielded twisted pair over unshielded twisted pair?

19.Why is coaxial cable superior to twisted-pair cable?

20.Name the advantages of optical over twisted pair and coaxial cable.

21. What are the disadvantages of optical fiber as a transmission medium?

22.How an IDN differs from ISDN?

23.What type of information can a B channel transmit?

24. What type of information can a D channel transmit?

25. What type of information can a H channel transmit?

26.What is the difference between in band signaling and out of band signaling?

27.What is NT1?

28. What is NT2 ?

29.What is TE1?

30. What is TE2?

31.What are X.25 layers?

32.How does the X.25 layers relate to the OSI model?

33.Name the X.25 frame types?

Computer Networks

34.What are the functions of X.25 frame types?

35.What are the frame layer phases involved in the communication between a DTE and a DCE ?

36.How are packets associated with the virtual circuit on which they travel?

37.What is the purpose of an LCN?

38.What type of virtual circuits does X.25 use?

39.List of the fields of a PLP packet types?

Multiple Choice Questions

1.The OSI model consists of ----------- layers.

  a. three b. five c. seven d. ten

2.The------layer decides the location of synchronization points.

  a.transport b.session. c.physical d.application

3.the end-to-end delivery of the entire message is the responsibility of the------

  a.network b. transport c.net work d.data link

4.The -------layer is the closest to the transmission medium.

  a.physical b.datalink c.session d.application

5.In the ------layer the data unit is called a frame

  a.   data link b.network c. application.d. Network

6.Decryption and encryption of data are the responsibility of the ----- layer

  a.   physical b. data link c. session d. presentation

7.Dialog control is a function of the ----- layer

  a. physical b. data link c. session d. presentation

8.Mail services and directory services are available to network users through the ----layer.

  a. transport b. session. c. physical d. application

9.Node –to-Node delivery of the data units is the responsibility of the ----- layer.

  a. data link b. network c. application. d. Network

10.AS the data packets move from the lower to the upper layers, headers are-------

  a. added b. subtracted c. rearranged d. modified

11. AS the data packets move from the upper to the lower layers, headers are-------

  a. added b. subtracted c. rearranged d. modified

12.When data are transmitted from device A to device B, the header from A's layer 5 is read by B's --------layer.

  a. physical b. transport c. session d. presentation

13.In ----layer, translation from one character code to another occur.

  a. physical b. data link c. session d. presentation

14.The ----- layer changes bits into electromagnetic signals.

Computer Networks

a. physical b. data link c. session d. presentation

15. The ----layer can use the trailer of the frame for error detection.

a. physical b. data link c. session d. presentation

16. The physical layer is concerned with the transmission of --------over the physical medium.

a. programs b. dialogs c. protocols d.bits.

17. Which of the following is an application layer service?

a. network virtual terminal b. file transfer c. mail service d. all of the above

18. Transmission media are usually categorized as------

a. fixed or unfixed b. guided media and unguided c. determinate or in determinate

d. metallic and nonmetallic

19. In fiber optics, the signal source is ------- waves.

a. light b. radio c. infrared d. very low frequency.

20. Which of the following is not a guided medium?

a. twisted pair b. coaxial cable c. fiber optic cable d. atmosphere

21. X.25 protocol uses ---- for end to end transmission.

a. message switching b. circuit switching. C. the datagram approach to packet switching

d. the virtual circuit approach.

22. The X.25 protocol operates in the -----of the OSI model.

a. physical layer b. data link layer c.net work layer d. all the above.

23. The physical layer protocol directly specified for the X.25 protocol is------

a. RS- 232 b. X.21 c. DB-15 d. DB- 37

24. The PLP packet is a product of the ------layer in the X.25 standard.

a. physical b. frame c. packet d. transport

25. The PLP ------1s used to transport data from upper layers in the X.25 standard

a. S-packet b. data packet c. C-packet d. P-packet

26. X.25 protocol requires error checking at the------layer.

a. Physical b. frame c. packet d. b and c

27. X.25 is ------- protocol.

a. a UNI b. an SNI c. AN NNI d. an SSN

28. ISDN is an acronym for ---------------------

a. Information services for digital network b. Internet work system for data networks

c. Integrated signals digital network d. Integrated services digital network

29. The ------channel is used for telemetry and alarms.

a. B b. C c. D d. H

30. ----------- is a group of non—ISDN equipment.

Computer Networks

a.TE1 b. TE2   c. Tex d.T3

Expected Questions

1. Define Computer Network? Give the difference between a network and distributed system?

2. Discuss the applications and goals of the computer networks

3. Explain briefly the functions of different layers of the OSI reference model

4. Give the difference between ISO OSI and TCP /IP model.

5. Discuss the difference between connection –oriented and connections-less services.

6. Give the advantage and disadvantage of frame relay over a leased telephone line.

7. Why does ATM used small, fixed length cells? Explain ATM layers.

8. Explain ISDN design? What are the services that can be provided by the ISDN ?What are the different ISDN phases?

9. What are the advantages of using layered architecture?

10. Briefly explain about the Novel NetWare and ARPANET

11. Explain X.21 digital interface?

12. Explain the following terms

   a) HOST b) IMP c) Subnet d) Protocol e) Interface f) PEER Processor

13. Distinguish between guided and unguided transmission media.

14. Briefly explain the different types of transmission medias?

15. Give the advantages and disadvantages of using fiber optic cable over metallic cable.

* * * * * * * *

Computer Networks

UNIT –II
DATALINK LAYER

Introduction

The Data Link Layer break the bit stream into discrete frames and compute the checksum for each frame. When a Frame arrives at the destination, the checksum is recomputed. If the newly computed checksum is different from one computed contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it.

FRAMING METHODS

1. CHARATER COUNT METHOD

2. STARTING AND ENDING CHARACTERS, WITH CHARATER STUFFING

3. STARTING AND ENDING FLAGS, WITH BIT STUFFING

CHARATER COUNT METHOD:

In this method a field in the header will be used to specify the number of CHARACTERS in the frame. When data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is. The trouble with this algorithm is that the count can be garbed by a transmission error resulting the destination will get out of synchronization and will be unable to locate the start of the next frame. There is no way of telling where the next frame starts. For this reason this method is rarely used.

Computer Networks

Character count

(a)

| 5 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 8 | 7 | 8 | 9 | 0 | 1 | 2 | 3 |

Frame 1   Frame 2   Frame 3   Frame 4

5 characters   5 characters   8 characters   8 characters

Error

| 5 | 1 | 2 | 3 | 4 | 7 | 6 | 7 | 8 | 9 | 8 | 0 | 2 | 3 | 4 | 5 | 6 | 8 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 5 |

Frame 1   Frame 2

(Wrong)   Now a character count
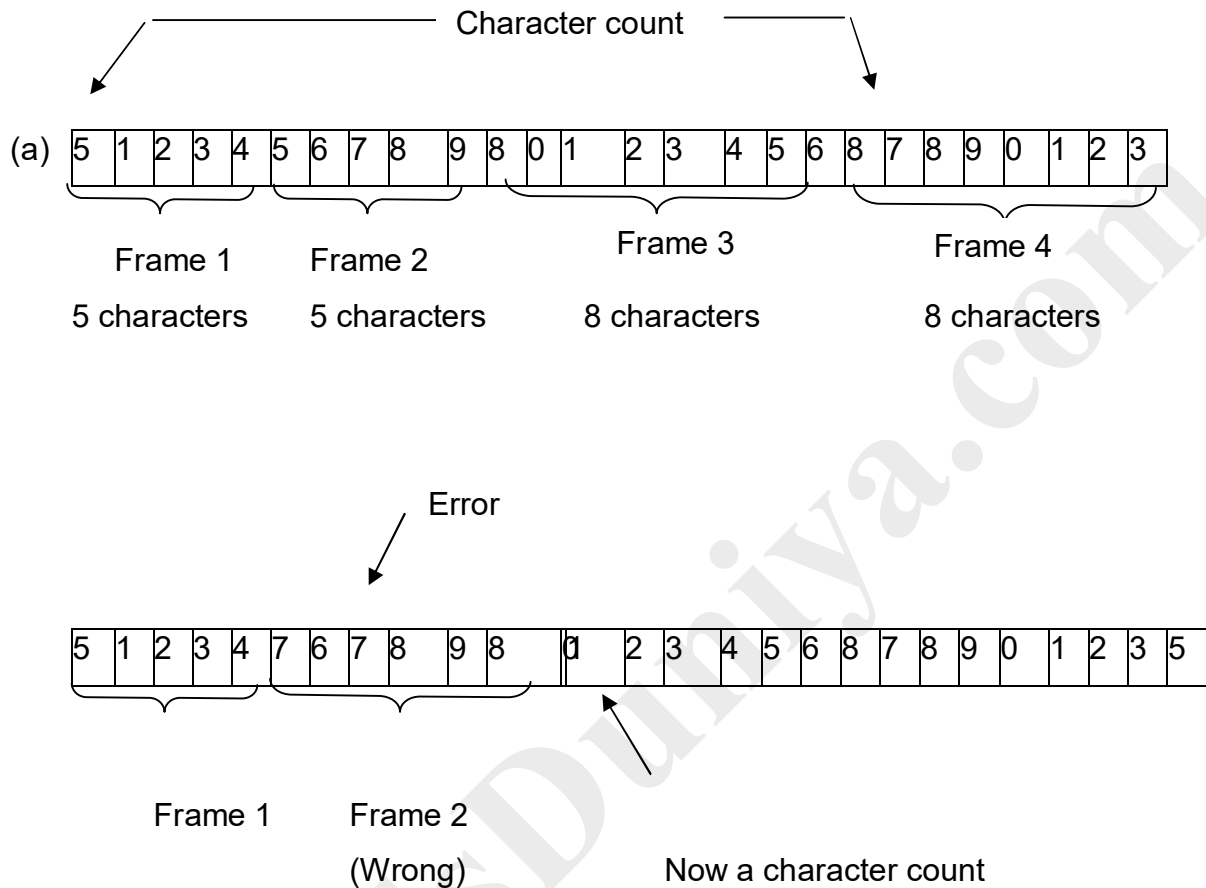
A Character Stream (a) Without errors (b) With one error

CHARATER STUFFING METHOD:

In this method each frame will start with a FLAG and ends with a FLAG.

The starting flag is **DLE STX** ---- **Data Link Escape Start of Text**

The ending flag is **DLE ETX ---- Data link Escape End of Text.**

Computer Networks

Ex 1. The given Data   ABRFCXDGJHKK12435ASBGXRR

The Data will be sent

DLE STX ABRFCXDGJHKK12435ASBGXRR DLE STX

Ex 2. The given Data   **ASHGTRDXZBNHG DLE STX %$#54378**

The data will be sent as

DLE STX ASHGTRDXZBNHG DLE DLE STX %$#54378 DLE ETX

Dis Adv:

1.24 bits are unnecessarily   stuffed.

2. Transmission delay.

BIT STUFFING METHOD

In this method every frame will start with a **flag   01111110.**

In the data if there are **FIVE**   consecutive   ONE 's are there then a ZERO   will be stuffed.

Ex. The given data   is   01111000011111101010011111 10 01111101100

The data will be sent as

01111110 01111000011110110101001111010 011111001100

Stuffed bits
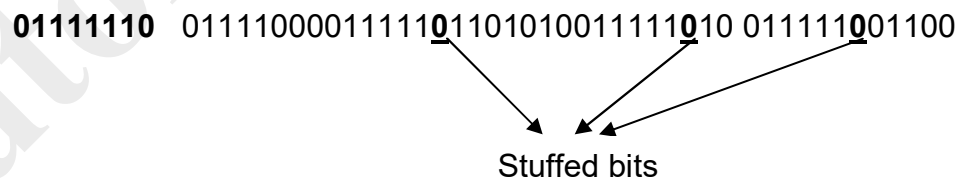
Advantages:

1. Only one bit is stuffed.
2. No transmission delay

Computer Networks

ERROR – CORRECTING AND   DETECTING CODES

Network designers have developed two basics strategies for dealing with errors. One way is to include enough redundant information along with each block of data sent, to enable the receiver to deduce what the transmitted data must have been .The other way is to include only enough redundancy to allow the receiver to deduce that an error occurred, but not which error, and have it request a retransmission. The former strategy uses **Error – correcting codes** and the latter uses **Error- detecting codes**.

The **Error – correcting   and   Error- detecting   methods are**

1. PARITY METHOD
2. LRC METHOD (Longitudinal redundancy check)
3. CRC METHOD   (Cyclic redundancy check)
4. HAMMING CODE   METHOD

PARITY METHOD

- appends a parity bit to the end of each word in the frame

- Even parity is used for asynchronous Transmission

- Odd parity is used for synchronous Transmission

Ex 1.	Character code	even parity	odd parity
	1100100	1100100 1	1100100 0
2.	0011000	0011000 0	0011000 1

If one bit or any odd no bits is erroneously inverted during Transmission, the Receiver will detect an error. How ever if two or even no of bits are inverted an undetected error occurs.

Computer Networks

Ex 3. The Transmitted data is 10011010. The received data is 11011010.

Let both the transmitter and receiver are agreed on EVEN parity.
Now an error will be detected, since the no of ones received are ODD

4. The Transmitted data is 10011010. The received data is 01011010

The received data is wrong even though the no of ones are EVEN.

Science two bits are inverted error can't be detected.

Longitudinal Redundancy Check(LRC)

The frame is viewed as a block of characters arranged in 2-dimensions. To each character is appended a parity bit. In addition a parity bit is generated for each bit position across all characters i.e., an additional character is generated in which the Ith bit of the character is parity bit for the Ith bit of all other characters in the block. This can be expressed mathematically using exclusive OR(+) operation. The parity bit at the end of each character of row parity

$$R_j = b_{1j} + b_{2j} + \text{------} b_{nj}$$

Where R_j=Parity bit of jth character

b_{ij}=ith bit in jth character
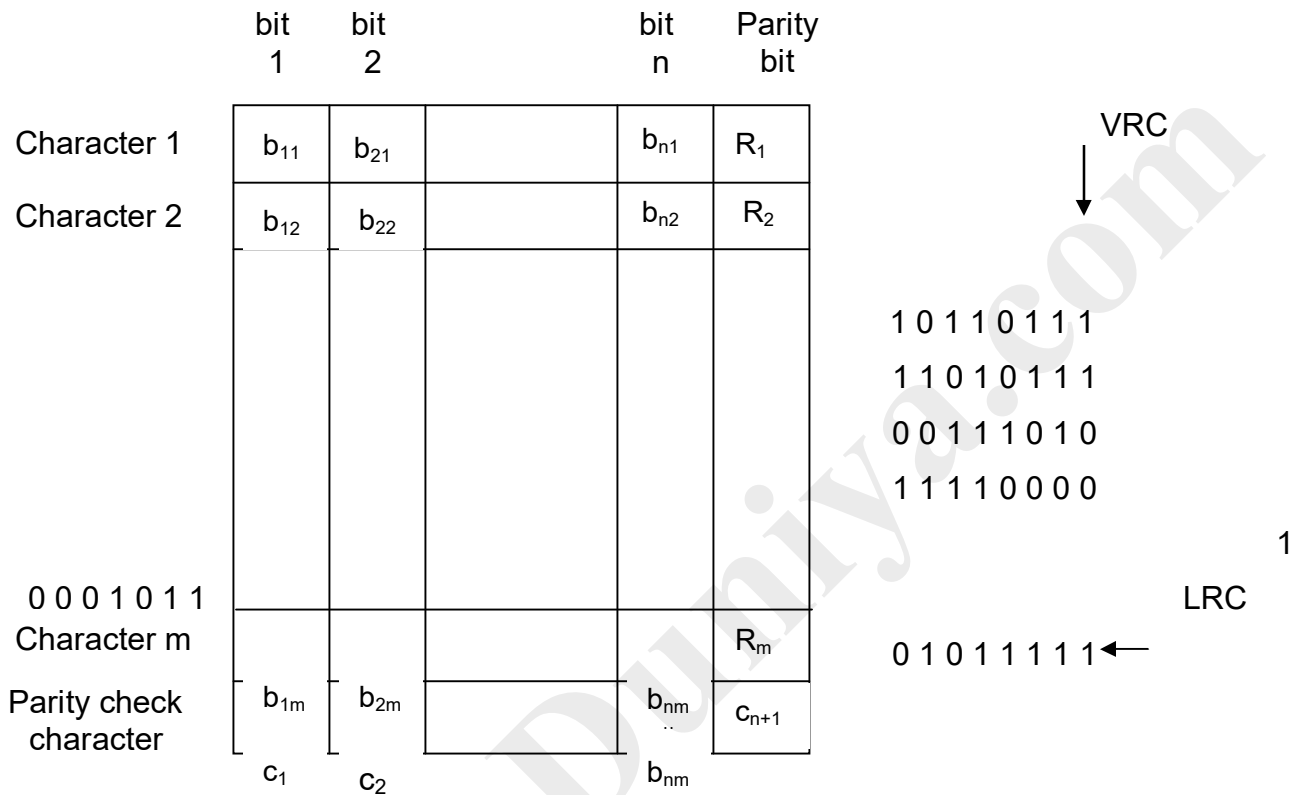
This equation generates even parity.

$$C_i = b_{i1} + b_{i2} + \text{-----} + b_{in}$$

Where C_i=ith bit of parity check character
m=number of characters in a frame
In this format the parity bits at the end of each character are referred to as

Computer Networks

The Vertical Redundancy Check (VRC) and the Parity check character is referred to as the Longitudinal Redundancy Check (LRC).

	bit 1	bit 2		bit n	Parity bit
Character 1	b_{11}	b_{21}		b_{n1}	R_1
Character 2	b_{12}	b_{22}		b_{n2}	R_2

VRC ↓

```
1 0 1 1 0 1 1 1
1 1 0 1 0 1 1 1
0 0 1 1 1 0 1 0
1 1 1 1 0 0 0 0
```
                                                    1

0 0 0 1 0 1 1   LRC

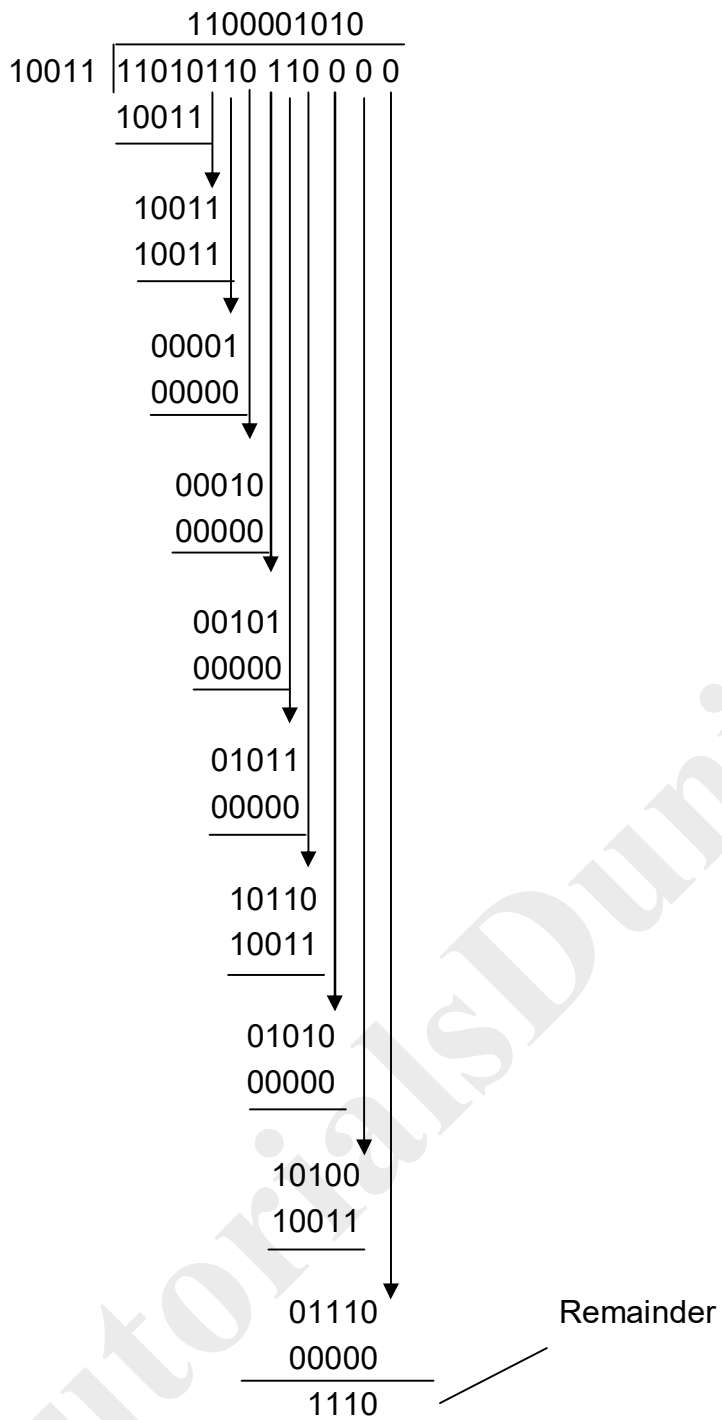| Character m					R_m
Parity check character	b_{1m}	b_{2m}		b_{nm} ..	c_{n+1}
	c_1	c_2		b_{nm}	

0 1 0 1 1 1 1 1 ←

CRC Method

1. The frame is expressed in the form of a Polynomial $F(x)$. 0 1 1 1 1 1 1 0

    2. Both the sender and receiver will agree upon a generator polynomial $G(x)$ in advance.

    3. Let 'r' be the degree of $G(x)$. Append 'r' zero bits to the lower – order end of frame now it contains m+r bits.

4. Divide the bit string by $G(x)$ using Mod 2 operation.

5. Transmitted frame $[T(x)]$ = frame + remainder

6. Divide $T(x)$ by $G(x)$ at the receiver end. If the result is a zero, then the frame is transmitted correctly. Ex. Frame: 1101011011

                 Generator: 10011

    Message after appending 4 zero bits: 11010110000

Computer Networks

```
                         1100001010
              10011 | 11010110 110 0 0 0
                      10011
                       10011
                       10011
                         00001
                         00000
                           00010
                           00000
                             00101
                             00000
                               01011
                               00000
                                 10110
                                 10011
                                   01010
                                   00000
                                     10100
                                     10011
                                       01110
                                       00000
                                       ─────
                                        1110              Remainder
```

Transmitted frame: 11010110111110

Computer Networks

```
                        1100001010
          10011 | 11010110 111 1 1 0
                  10011
                  10011
                  10011
                    00001
                    00000
                      00010
                      00000
                        00101
                        00000
                          01011
                          00000
                            10111
                            10011
                              01001
                              00000
                                10011
                                10011
                                  00000
                                  00000
                                    0000         Remainder
```
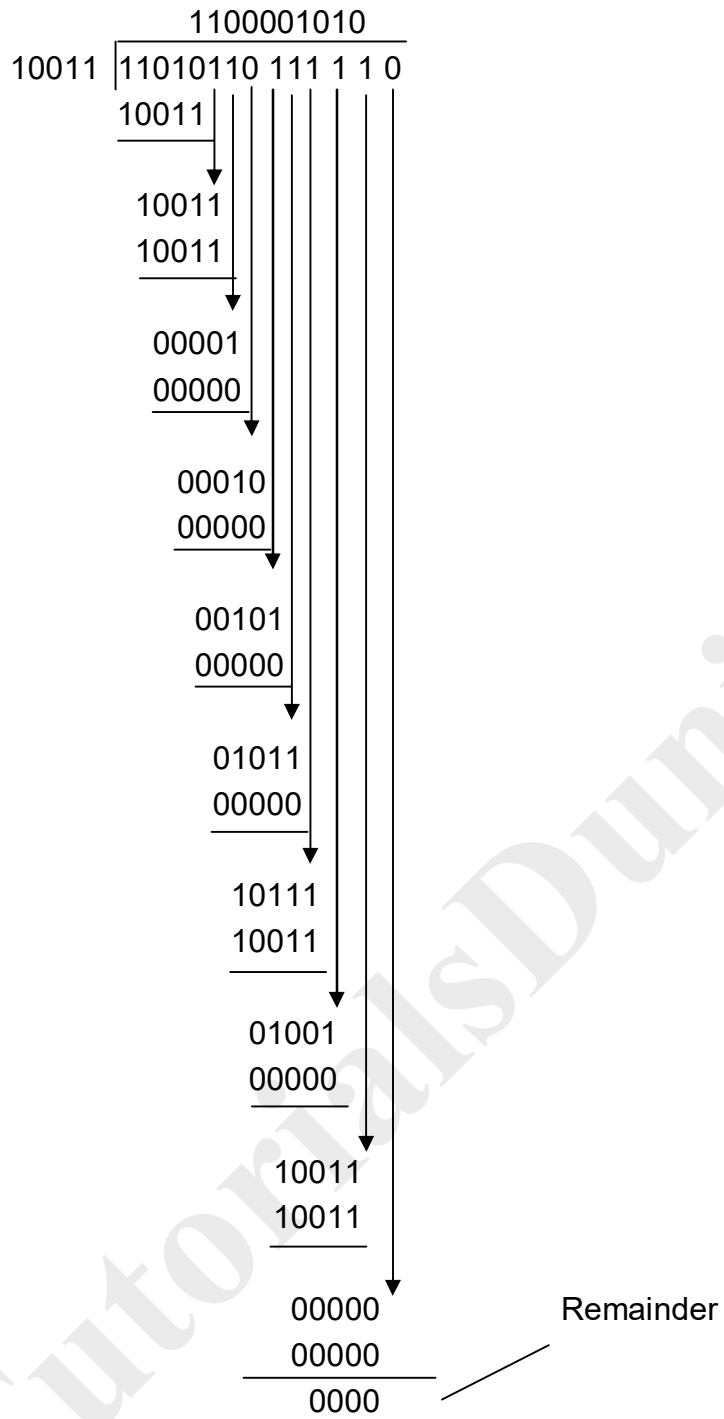
Since the remainder is zero there is no error in the transmitted frame.

Computer Networks

HAMMING CODES

Hamming codes provide another method for error correction. Error bits, called Hamming bits, are inserted into message bits at random locations. It is believed that the randomness of their locations reduces the odds that these Hamming bits themselves would be in error. This is based on a mathematical assumption that because there are so many more message bits compared with Hamming bits, there is a greater chance for a message bit to be in error than for a Hamming bit to be wrong. Determining the placement and binary value of the Hamming bits can be implemented using hardware, but it is often more practical to implement them using software. The number of bits in a message (M) are counted and used to solve the following equation to determine the number of Hamming bits (H) to be used:

$$2^H \geq M + H + 1$$

Once the number of Hamming bits is determined, the actual placement of the bits into the message is performed. It is important to note that despite the random nature of the Hamming bit placements, the exact sample placements must be known and used by both the transmitter and receiver. Once the Hamming bits are inserted into their positions, the numerical values of the bit positions of the logic 1 bits in the original message are listed. The equivalent binary numbers of these values are added in the same manner as used in previous error methods by discarding all carry results. The sum produced is used as the states of the Hamming bits in the message. The numerical difference between the Hamming values transmitted and that produced at the receiver indicates the bit position that contains a bad bit, which is then inverted to correct it.

Ex. The given data

  10010001100101(14- bits)

  The number of hamming codes

  $$2^H \geq M + H + 1$$

H = ?   M = 14   to satisfy this equation   H should be 5 i.e. 5 hamming code bits should be incorporated in the data bits.
1 0 0 1 0 0 0 1 1 0 H 0 H 1 H 0 H 1 H

Now count the positions where binary 1's are present. Add using mod 2 operation (Ex-OR). The result will give the Hamming code at the transmitter end.

<u>1's position</u>   <u>Binary equivalent</u>

Computer Networks

```
         2  -  0  0  0  1  0
         6  -  0  0  1  1  0
        11  -  0  1  0  1  1
        12  -  0  1  1  0  0
        16  -  1  0  0  0  0
        19  -  1  0  0  1  1
Hamming code =  0  0  0  0  0
```

This Hamming code will be incorporated at the places of 'H' in the data bits and the data will be transmitted.

How to find out there is an error in the data?

Let the receiver received the 12th bit as zero. The receiver also finds out the Hamming code in the same way as transmitter.

```
        1's position              Binary equivalent
              2  -  0  0  0  1  0
              6  -  0  0  1  1  0
             11  -  0  1  0  1  1
             16  -  1  0  0  0  0
             19  -  1  0  0  1  1
Hamming
code at the        0  1  1  0  0
receiver
```

```
Hamming code  at the Tx      0  0  0  0  0
Hamming code  at the Rx      0  1  1  0  0
                             0  1  1  0  0
```

The decimal equivalent for the binary is **12** so error is occurred at 12th place.

Computer Networks

Data Link Protocols

1. Unrestricted Simplex Protocol:
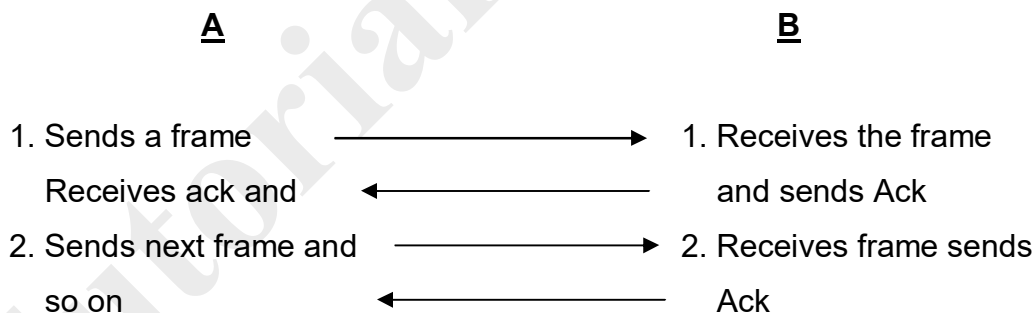
In this the following assumptions are made

      a. Data transmission is simplex i.e. transmitted in one direction only.
      b. Both transmitting and receiving network layers are ready.
      c. Processing time is ignored.
      d. Infinite buffer space is available.
      e. An error free channel.

This is an unrealistic protocol, which has a nickname "Utopia".
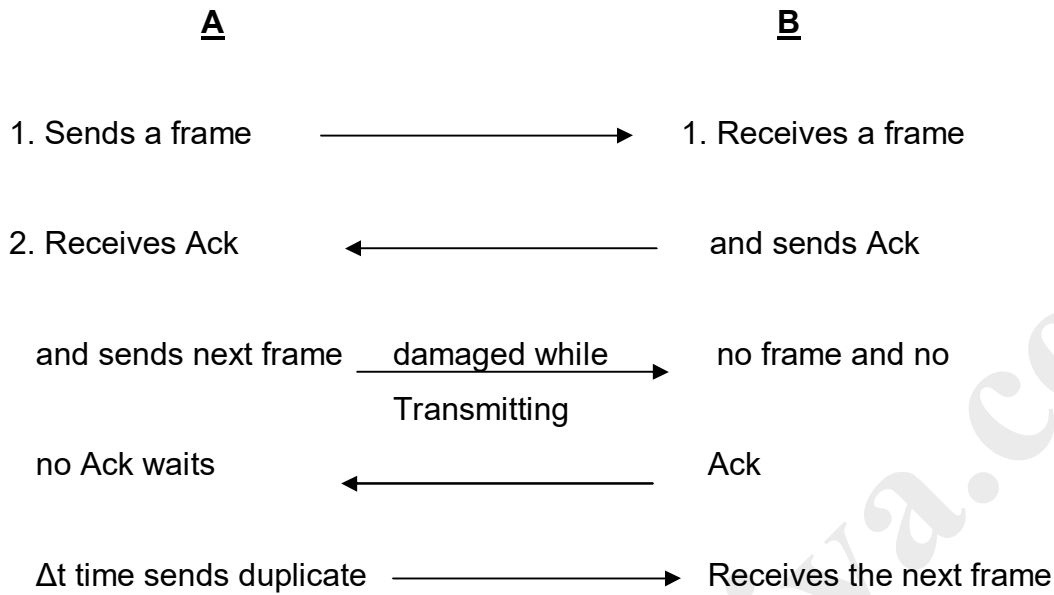
2. A simplex stop and wait protocol:

The following assumptions are made

      a. Error free channel.
      b. Data transmission simplex.

A	B
1. Sends a frame ⟶	1. Receives the frame
Receives ack and ⟵	and sends Ack
2. Sends next frame and ⟶	2. Receives frame sends
so on ⟵	Ack

Since the transmitter waits for Δt time for an Ack this protocol is called stop and wait protocol.

Computer Networks

3. A simplex protocol for a noisy channel

A   **B**

1. Sends a frame   ───────────►   1. Receives a frame

2. Receives Ack   ◄───────────   and sends Ack

   and sends next frame   <u>damaged while</u> ►   no frame and no
                          Transmitting

   no Ack waits   ◄───────────   Ack

   Δt time sends duplicate ───────────►   Receives the next frame

When this protocol fails?

A   **B**

1. Sends a frame   ───────────►   1. Received by B

2. Ack is not received   ◄── <u>Ack damaged while</u>   2. And sends Ack
                            Transmitting

wait some time and sends ───────────►   Received duplicate   duplicate
                                          (same frame)
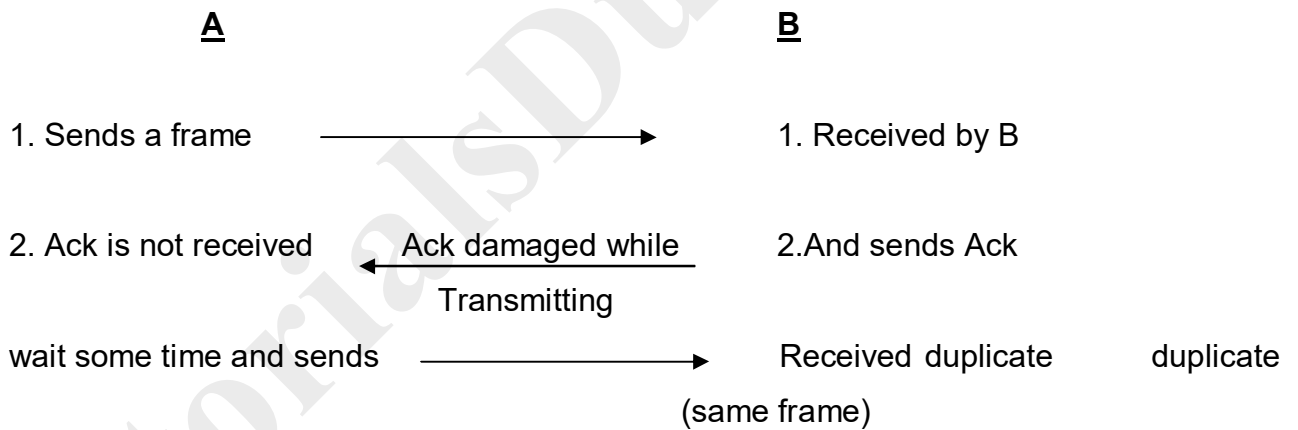
At this situation protocol fails because the receiver receives a duplicate frame and there is no way to find out whether the receiver frame is original or duplicate. So the protocol fails at this situation.

Now what is needed is some way for the Rx to distinguish a frame and a duplicate. To achieve this, the sender has to put a sequence number in the header of each frame it sends. The Rx can check the sequence number of each arriving frame to see if it is a new frame or a duplicate.

Computer Networks

Here a question arises: What is the minimum number of bits needed for the sequence number? The ambiguity is between a frame and its successor. A 1-bit sequence number (0 or 1) is therefore sufficient. At each instant of time, the receiver excepts a particular sequence number next. Any arriving frame containing wrong sequence number is rejected as a duplicate. When a frame containing the correct sequence number arrives, it is accepted, passed to the network layer and then expected sequence number is incremented i.e. 0 becomes 1 and one becomes 0. Protocols in which a sender waits for a positive ack before advancing to the next data item are often called PAR (positive ack with retransmission) or ARQ (automatic repeat request).

When this protocol fails?

A	**B**
1. A Sends a frame F_0	1. B receives it and sends Ack AF_0
2. Receives AF0 send next frame F1	2. B receives F1 and sends Ack AF1 (while transmitting Ack delayed and reached late).
3. A's time out and sends duplicate frame F1	
4. In between received the delayed Ack AF1 and sends frame F0 (while transmitting F0 damaged.)	3. Receives F1 and sends Ack AF1
5. Now the duplicate frame Ack AF1 received	4.B does not get frame and no Ack.

6. Now A thinks that the Ack received is the ack of new frame F0 and A sends next frame F1. So a frame F0 is missed. At this situation this protocol fails.

Computer Networks

PIGGY BACKING

In most practical situations there is a need of transmitting data in both directions. This can be achieved by full duplex transmission. If this is done we have two separate physical circuits each with a 'forward ' and 'reverse' channel. In both cases, the reverse channel is almost wasted. To overcome this problem a technique called **piggy backing** is used.

The technique of temporarily delaying outgoing acknowledgements so that they can be hooked onto the next outgoing data frame is known as **piggy backing**.

However, piggybacking introduces a complication not present with separate acknowledgements. How long should the data link layer wait longer than the sender's timeout period, the frame will be retransmitted, defeating the whole purpose of having acknowledgements. Of course, the data link layer cannot foretell the future, so it must resort to some ad hoc scheme, such as waiting a fixed number of milli seconds. If a new packet arrives quickly, the acknowledgement is piggy backed onto it; otherwise, if no new packet has arrived by the end of this time period, the data link layer just sends a separate acknowledgement frame.

SLIDING WINDOW PROTOCOLS

In all sliding window protocols, each outbound frame contains a sequence number, ranging from 0 up to some maximum. The maximum is usually $2^n - 1$ so the sequence number fits nicely in an n-bit field. The stop-and-wait sliding window protocol uses n=1, restricting the sequence numbers to 0 and 1, but more sophisticated versions can use arbitrary n.

The essence of all sliding window protocols is that at any instant of time, the sender maintains a set of sequence numbers corresponding to frames it is permitted to send. These frames are said to fall with in the sending window. Similarly the receiver also maintains a receiving window corresponding to the set of frames it is permitted to accept. The sender's window and the receiver's window need not have the same lower and upper limits, or even have the same size. In some protocols they are fixed in size, but in others they can grow or shrink as frames are sent and received.

The sequence numbers with in the sender's window represent frames sent but as yet not acknowledged. Whenever a new packet arrives from the network layer, it is given the next

Computer Networks

highest sequence number, and the upper edge of the window is advanced by one. When an acknowledgement comes in, the lower edge is advanced by one. In this way the continuously maintains a list of unacknowledged frames.

Sender
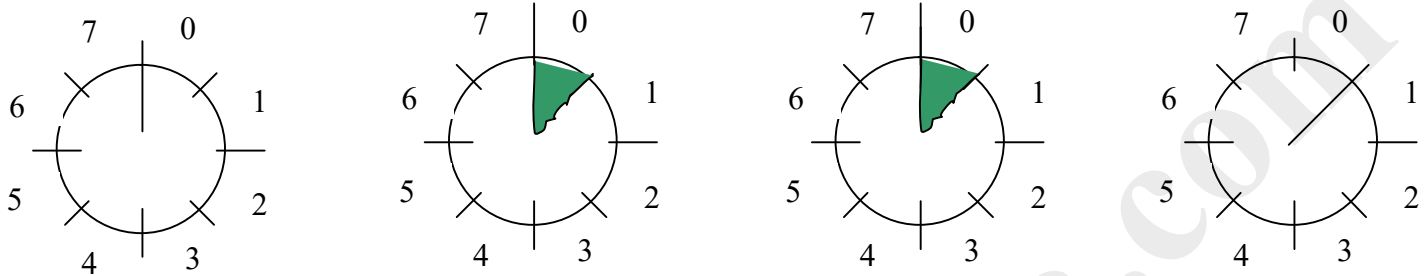
Receiver
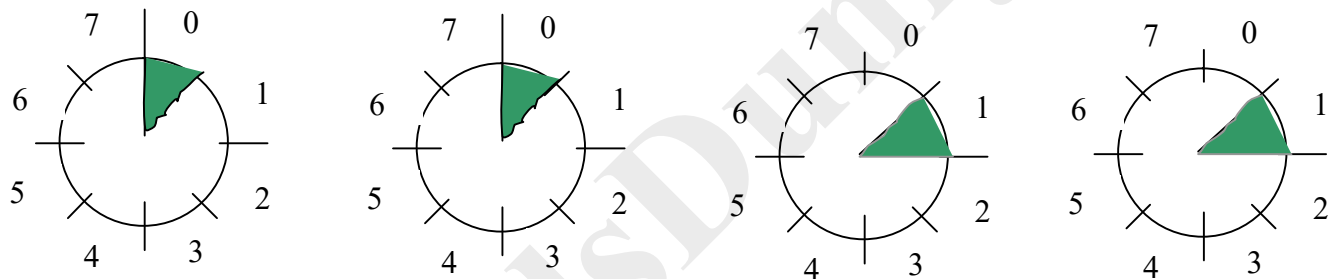
(a)	(b)	(c)	(d)

(a) Initially   (b) After the first frame has been sent   c) After the first frame has been received.   d) After the first acknowledgement has been received.

PIPELINING

1. Upto now we made the assumption that the transmission time required for a frame to arrive at the receiver plus the transmission time for the ack to come back is negligible.

2. Sometimes this is not true, when there is a long round trip propagation time is there.

3. In these cases round trip propagation time can have important implications for the efficiency of the bandwidth utilization.

Computer Networks

Consider the below example.

Let the channel capacity   b   = 50Kbps.

round trip propagation delay   = 500ms

Frame size   = 1000bits

Without considering the round trip propagation delay

For one frame the time taken will be   = 1000/500 ms
                                                            = 20 ms

Considering the round trip propagation delay

For one frame the time taken will be   = 500 ms +20 ms
                                                            = 270 ms
The channel utilization   = (20/520)*100 = 4%

 i.e.   We are wasting 96% of channel time. To overcome this problem we will go for a technique   called **PIPELIING.**

 In this technique, the sender is allowed to transmit upto 'w ' frames before blocking, instead of just 1.With an appropriate choice of w the sender will be able to continuously

Computer Networks

transmit frames for a time equal to the round trip transmit time without filling up the window.

In the above example w would be at least 26 frames. (520/20 = 26 frames)

By the time it has finished sending 26 frames, at t=520 ms, the ack for frame 0 will have just arrived. Thereafter ack will arrive every 20 ms, so the sender always gets permission to continue just when it needs it.

Hence, we can say the sender window size is 26.

Derivation:

Let the channel capacity = b Bps

Let the frame size = l bits

Let the round trip delay = R secs

To send one frame the time will be l/b secs

Due to round trip delay the time taken will be (l/b + R) Sec = l+Rb/b Sec

The channel utilization is l/b (l/b + R) Sec = (l / l + Rb) Sec

If l > bR the efficiency will be greater than 50%.
If l < bR the efficiency will be less than 50%.

If l = bR the efficiency will be 50%.

Ex 1. A channel has a bit rate of 4 kbps and a propagation delay of 20msec.For what rage of frame sizes does stop and wait give an efficiency of at least 50 % ?

Computer Networks

2.consider an error free 64 kbps channel used to send 512 –byte data frames in one direction, with very short acknowledgements coming back the other way. What is the maximum throughput for window sizes of 1,7,15,and 127?

Pipelining frames over an unreliable channel raises some serious issues.

First, what happens if a frame in the middle of a long stream is   damaged   or lost?

When a damaged frame arrives at the receiver, it obviously should discarded, but what should the receiver do with all the correct frames following it?

There are two basic approaches to dealing with errors .

1. Go Back 'n'
2. Selective repeat or Selective Reject

One way called in **go back n**, the receiver simply to discard all subsequent frames, sending no acknowledgements for the discard frames. In the other words, the data link layer refuses to accept any frame except the next one it must give to the network layer.

Selective Repeat:

The receiving data link layer store all the correct frames following the bad frame, not all its successors. If the second try succeeds the receiving data link layer will now have many correct frames in sequence, so they can all be handed off to the network layer quickly and the highest number acknowledged. This strategy corresponds to a receiver window larger than 1.

(a) Go-back-N

Error   Discarded frames

Computer Networks

Error   Buffered by receiver   Frames 2-5 released
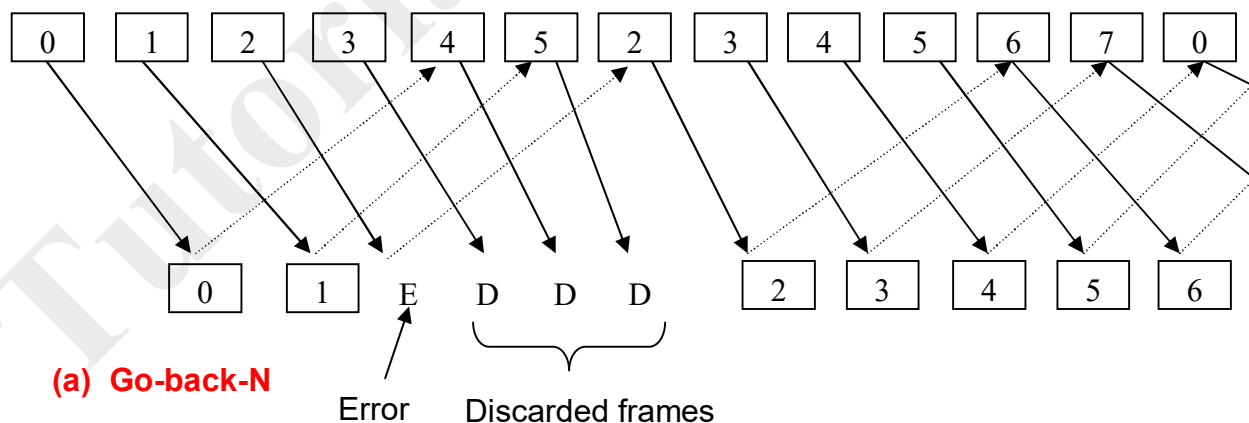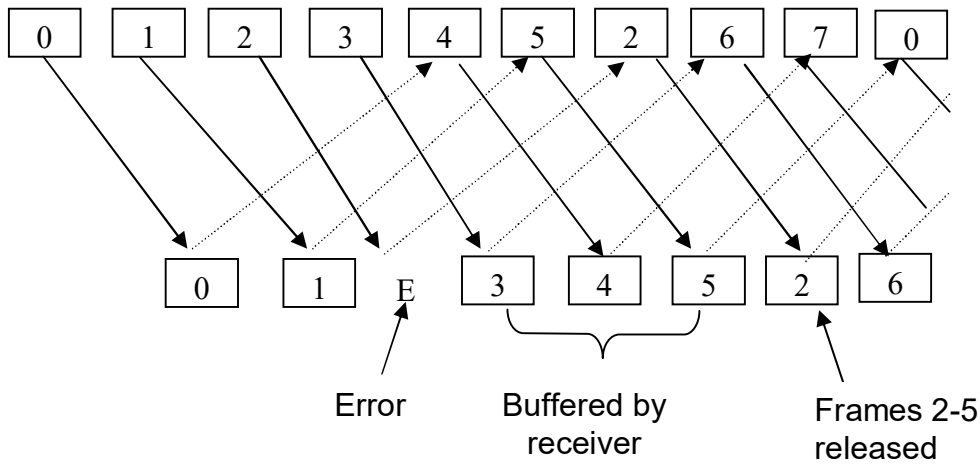
b) Selective reject

MEDIUM ACCESS CONTROL SUBLAYER (MAC)

Networks can be categories in to two ways

a) Point to point b) Broad cast channel

- In broadcast network, the key issue is how to share the channel among several users.

- <u>Ex</u> *a conference call with five people*

-Broadcast channels are also called as multi-access channels or random access channels.

-Multi-access channel belong to a sublayer at the DL layer called the MAC sublayer.

The Channel Allocation problem:

a) **Static channel allocation** in LANs & MANs

    i) **FDM**   ii) **TDM**

Drawbacks: -1) Channel is wasted if one or more stations do not send data.

         2) If users increases this will not support.

b) Dynamic channel allocation

i) Pure **ALOHA** & Slotted **ALOHA**

                CSMA/CD

ii)   **CSMA**

                CSMA/CA

Computer Networks

Pure ALOHA

-1970's Norman Abramson end his colleagues devised this method, used ground –based radio broad costing. This is called the **ALOHA** system.

-The basic idea, many users are competing for the use of a single shared channel.

-There are two versions of ALOHA: **Pure and Slotted**.

-Pure ALOHA does not require global time synchronization, where as in slotted ALOHA the time is divided into discrete slots into which all frames must fit.

-Let users transmit whenever they have data to be sent.

-There will be collisions and all collided frames will be damaged.

-Senders will know through feedback property whether the frame is destroyed or not by listening channel.

[-With a LAN it is immediate, with a satellite, it will take 270m sec.]

-If the frame was destroyed, the sender waits random amount of time and again sends the frame.

-The waiting time must be random otherwise the same frame will collide over and over.

USER
_____

A [____]   [____]

_____

B   [____]   [_____]

_____

C [____]   [____]

_____

D [____]   [____]   [____]

_____

————————→   TIME

Computer Networks
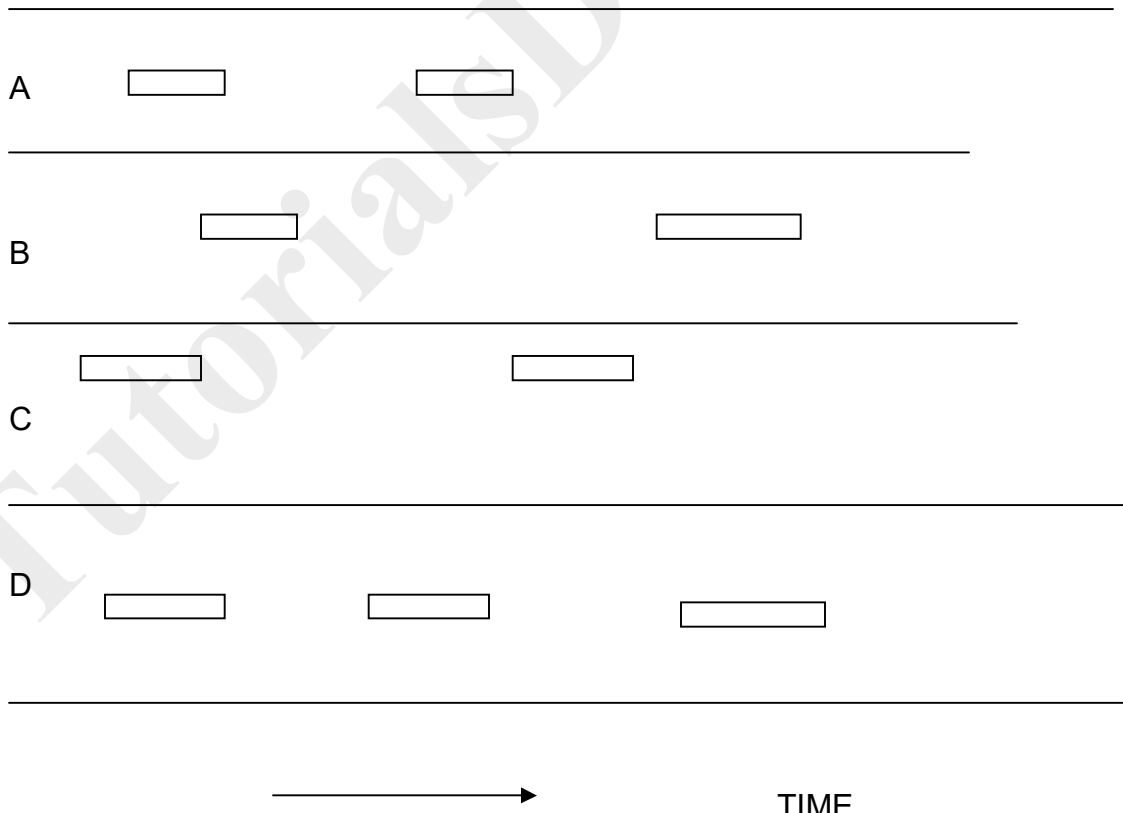
Frames are transmitted at completely arbitrary times

-Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be destroyed.

-We have to find out what is the efficiency of an ALOHA channel?

-Let us consider an infinite collection of interactive users sitting at their systems (stations).

-A user will always in two states **typing or waiting**.

-Let the 'Frame time' denotes the time required to transmit one fixed length frame.

-Assume that infinite populations of users are generating new frames according to possion distribution with mean N frames per frame time.

-If N>1 users are generating frames at a higher rate than the channel can handle.

-For reasonable throughput 0<N<1.

-In addition to new frames, the station also generates retransmission of frames.

-Old and new frames are G per frame time.

-$G \geq N$

-At low load there will be few collisions, so G ~ N

-Under all loads, the throughput $S = GP_o$, where P_o is the probability that a frame does not suffer a collision.

-A frame will not suffer a collision if no other frames are sent with one frame time of its start.

-Let 't' be the time required to send a frame.

-If any other user has generated a frame between time t_o and t_o+t, the end of that frame will collide with the beginning of the shaded frame.

-Similarly, any other frame started b/w t_o+t and t_o+2t will bump into the end of the shaded frame.

-The probability that 'k' frames are generated during a given frame time is given by the possion distribution:

$$P_r[k] = \frac{G^k e^{-G}}{k!}$$

-The probability of zero frames is just e^{-G}

-In an interval two frame times long, the mean number at frames generated is 2G.

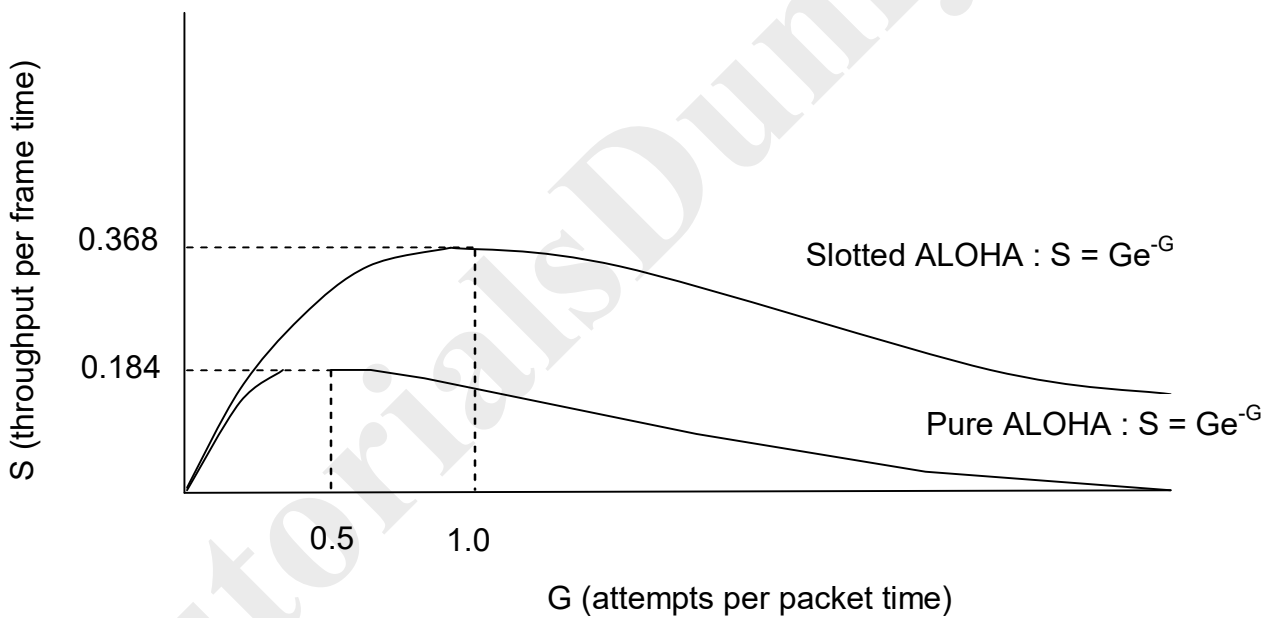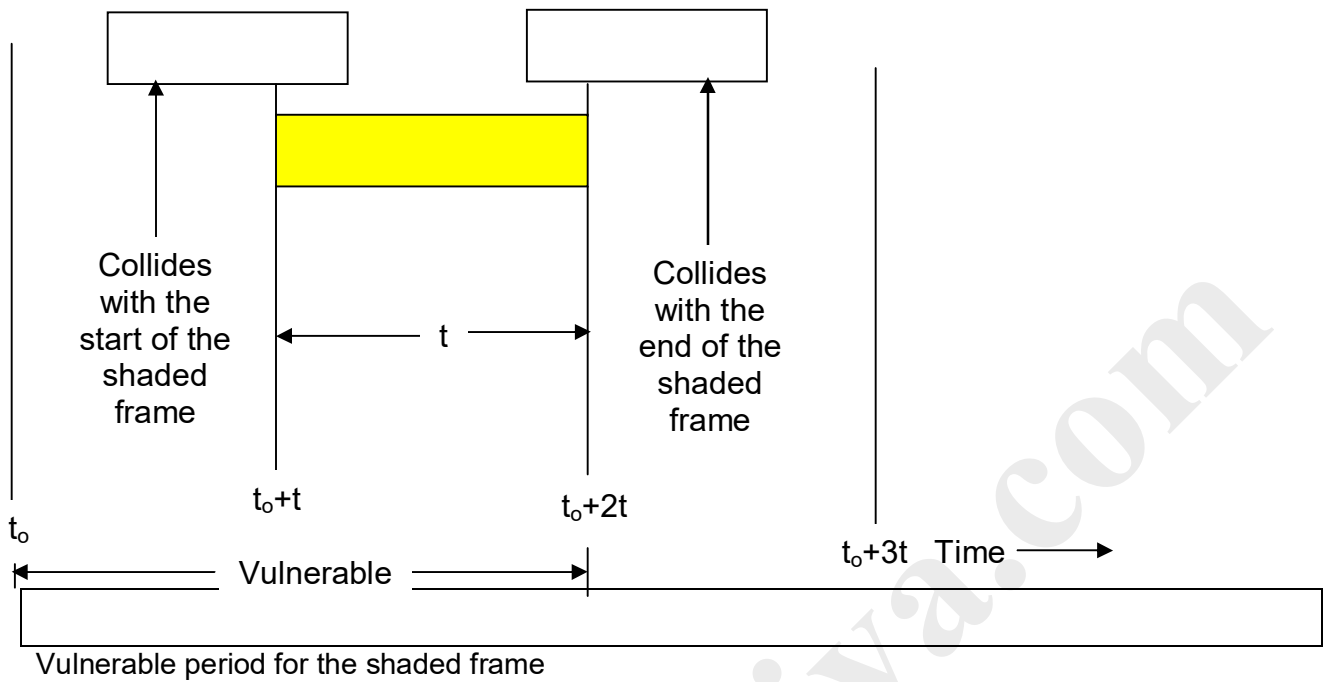-The probability at no other traffic being initiated during the entire vulnerable period is given by

$$P_o = e^{-2G}$$

$$S = Ge^{-2G} \qquad [S=GP_o]$$

The Maximum through put occurs at G=0.5 with S=1/2e = 0.184

The channel utilization at pure ALOHA =18%.

Computer Networks

Collides with the start of the shaded frame

Collides with the end of the shaded frame

t

t_o+t

t_o+2t

t_o

t_o+3t Time →

Vulnerable

Vulnerable period for the shaded frame

S (throughput per frame time)

0.368

0.184

Slotted ALOHA : $S = Ge^{-G}$

Pure ALOHA : $S = Ge^{-G}$

0.5

1.0

G (attempts per packet time)

Throughput versus offered traffic for ALOHA systems

Slotted ALOHA

-In 1972, Roberts' devised a method for doubling the capacity of ALOHA system.

-In this system the time is divided into discrete intervals, each interval corresponding to one frame.

Computer Networks

-One way to achieve synchronization would be to have one special station emit a pip at the start of each interval, like a clock.

-In Roberts' method, which has come to be known as slotted ALOHA, in contrast to Abramson's pure ALOHA; a computer is not permitted to send whenever a carriage return is typed.

-Instead, it is required to wait for the beginning of the next slot.

-Thus the continuous pure ALOHA is turned into a discrete one.

-Since the vulnerable period is now halved, the of no other traffic during the same slot as our test frame is e^{-G} which leads to

$S = Ge^{-G}$

- At G=1, slotted ALOHA will have maximum throughput.

- So S=1/e or about 0.368, twice that of pure ALOHA.

- The channel utilization is 37% in slotted ALOHA.

Carrier Sense Multiple Access Protocols

Protocols in which stations listen for a carrier (transmission) and act accordingly are called carries sense protocols.

Persistent CSMA

When a station has data to send, it first listens to the channel to see if any one else is transmitting at that moment. If the channel is busy, the station waits until it become idle. When the station detects an idle channel, it transmits a frame. If a collision occurs, the station waits a random amount of time and starts all over again. The protocol is called 1-persistent also because the station transmits with a probability of 1 when it finds the channel idle.

The propagation delay has an important effect on the performance of the protocol. The longer the propagation delay the worse the performance of the protocol.

Even if the propagation delay is zero, there will be collisions. If two stations listen the channel, that is idle at the same, both will send frame and there will be collision.

Computer Networks

Non persistent CSMA

In this, before sending, a station sense the channel. If no one else is sending, the station begins doing so it self. However, if the channel is busy, the station does not continually sense it but it waits a random amount of time and repeats the process.

This algorithms leads to better channel utilization but longer delays then 1-persistent CSMA.

With persistent CSMA, what happens if two stations become active when a third station is busy? Both wait for the active station to finish, then simultaneously launch a packet, resulting a collision. There are two ways to handle this problem.

a) P-persistent CSMA   b) exponential backoff.

P-persistent CSMA

The first technique is for a waiting station not to launch a packet immediately when the channel becomes idle, but first toss a coin, and send a packet only if the coin comes up heads. If the coin comes up tails, the station waits for some time (one slot for slotted CSMA), then repeats the process. The idea is that if two stations are both waiting for the medium, this reduces the chance of a collision from 100% to 25%. A simple generalization of the scheme is to use a biased coin, so that the probability of sending a packet when the medium becomes idle is not 0.5, but p, where $0 < p < 1$. We call such a scheme **P-persistent CSMA**. The original scheme, where p=1, is thus called 1-persitent CSMA.

Exponential backoff

The key idea is that each station, after transmitting a packet, checks whether the packet transmission was successful. Successful transmission is indicated either by an explicit acknowledgement from the receiver or the absence of a signal from a collision detection circuit. If the transmission is successful, the station is done. Otherwise, the station retransmits the packet, simultaneously realizing that at least one other station is also contending for the medium. To prevent its retransmission from colliding with the other station's retransmission, each station backs off (that is, idles) for a random time chosen from   the   interval

Computer Networks

[0,2*max-propagation_delay] before retransmitting its packet. If the retransmission also fails, then the station backs off for a random time in the interval [0,4* max_propagation_delay], and tries again. Each subsequent collision doubles the backoff interval length, until the retransmission finally succeeds. On a successful transmission, the backoff interval is reset to the initial value. We call this type of backoff exponential backoff.

CSMA/CA

In many wireless LANS, unlike wired LANS, the station has no idea whether the packet collided with another packet or not until it receives an acknowledgement from receiver. In this situation, collisions have a greater effect on performance than with CSMA/CD, where colliding packets can be quickly detected and aborted. Thus, it makes sense to try to avoid collisions, if possible. CSMA/CA is basically p-persistence, with the twist that when the medium becomes idle, a station must wait for a time called the interframe spacing or IFS before contending for a slot. A station gets a higher priority if it is allocated smaller inter frame spacing.

When a station wants to transmit data, it first checks if the medium is busy. If it is, it continuously senses the medium, waiting for it to become idle. When the medium becomes idle, the station first waits for an interframe spacing corresponding to its priority level, then sets a contention timer to a time interval randomly selected in the range [0,CW], where CW is a predefined contention window length. When this timer expires, it transmits a packet and waits for the receiver to send an ack. If no ack is received, the packet is assumed lost to collision, and the source tries again, choosing a contention timer at random from an interval twice as long as the one before(binary exponential backoff). If the station senses that another station has begun transmission while it was waiting for the expiration of the contention timer, it does not reset its timer, but merely freezer it, and restarts the countdown when the packet completes transmission. In this way, stations that happen to choose a longer timer value get higher priority in the next round of contention.
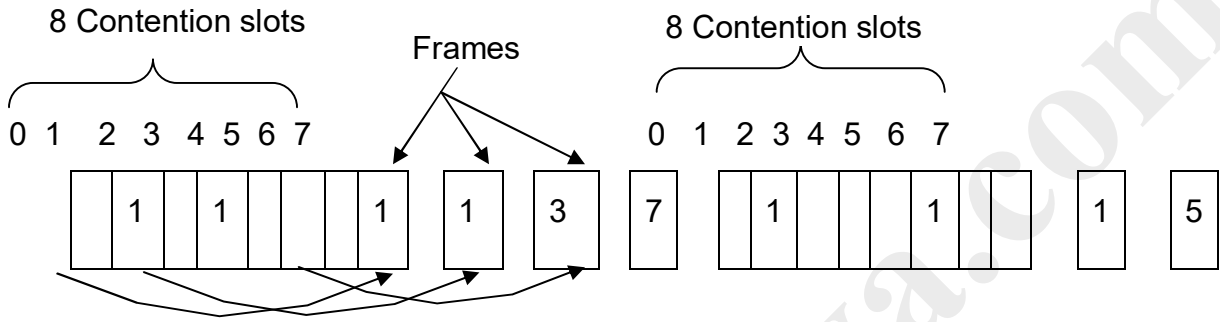
Collision-Free Protocols

A Bit-Map Protocol

In the basic bit-map method, each contention period consists of exactly N slots. If station 0 has a frame to send, it transmits a 1 bit during the zeroth slot. No other station is allowed to transmit during this slot. Regardless of what station 0 does, station 1 gets the

Computer Networks

opportunity to transmit a 1during slot 1, but only if it has a frame queued. In general, station j may announce the fact that it has a frame to send by inserting a 1 bit into slot j. after all N slots have passed by, each station has complete knowledge of which stations with to transmit.

The basic bit-map protocol

Since everyone agrees on who goes next, there will never be any collisions. After the last ready station has transmitted its frame, an event all stations can easily monitor, another N bit contention period is begun. If a station becomes ready just after its bit slot has passed by, it is out of luck and must remain silent until every station has had a chance and the bit map has come around again. Protocols like this in which the desire to transmit is broadcast before the actual transmission are called reservation protocols.

Binary Countdown

A problem with the basic bit-map protocol is that the overhead is 1 bit per station. A station wanting to use the channel now broadcasts its address as a binary bit string, starting with the high-order bit. All addresses are assumed to be the same length. The bits in each address position from different stations are BOOLEAN ORed together. We will call this protocol binary countdown. It is used in Datakit.

As soon as a station sees that a high-order bit position that is 0 in its address has been overwritten with a 1, it gives up. For example, if station 0010,0100,1001, and 1010 are all trying to get the channel, in the first bit time the stations transmit 0,0,1, and 1, respectively. Stations 0010 and 0100 see the 1 and know that a higher-numbered station is competing for the channel, so they give up for the current round. Stations 1001 and 1010 continue.

Computer Networks

The next bit is 0, and both stations continue. The next bit is 1, so station 1001 gives up. The winner is station 1010, because it has the highest address. After winning the bidding, it may now transmit a frame, after which another bidding cycle starts.

The binary countdown protocol. A dash indicates silence

Bit time

0 1 2 3

| 0 0 1 0 | 0 - - -

| 0 1 0 0 | 0 - - -

| 1 0 0 1 | 1 0 0 -

| 1 0 1 0 | 1 0 1 0

Result 1 0 1 0

Stations 0010 and 0100 see this 1 and give up

Station 1001 sees this 1 and gives up

IEEE Standard 802 for LANS and MANS

The IEEE 802.3 is for a 1-persistent CSMA/CD LAN. Xerox built a 2.94 Mbps CSMA/CD system to connect over 100 personal workstations on 1-Km cable. This system was called Ethernet through which electromagnetic radiation was once thought to propagate. Xerox DEC and Intel came with another standard for 100 Mbps Ethernet. This differs from old one that it runs at speeds from 1 to 10 Mbps on various media. The second difference between these two is in one header (802.3 length field is used for packet type in Ethernet).

Computer Networks

```
                        ┌──────────┐
                        │  802.3   │
                        └────┬─────┘
              ┌──────────────┴──────────────┐
              ▼                              ▼
    ┌──────────────────┐          ┌──────────────────┐
    │   Base band      │          │   Broad band     │
    │   Digital        │          │   Analog         │
    │   (Manchester)   │          │   ( PSK)         │
    └──────────────────┘          └──────────────────┘
```

10Base5, 10Base2   10 Broad 36

10Base-T, 1Base5

100 Base-T

802.3 Cabling

Five types of cabling are commonly used, 10Base5 cabling called thick Ethernet, came first. It resembles a yellow garden hose, with markings every 2.5 m to show where the taps go. Connections to it are generally made using **vampire taps**, in which a pin is carefully forced halfway into the coaxial cable's core. The notation 10Base5 means that it operates at 10 Mbps, uses baseband signaling, and can support segments of up to 500m.

Name	Cable	Max. segment	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Good for backbones
10Base2	Thin coax	200 m	30	Cheapest system
10Base-T	Twisted pair	100 m	1024	Easy maintenance
10Base-F	Fiber optics	2000 m	1024	Best between buildings

The second cable type was **10Base2** or thin Ethernet, which, in contrast to the garden-hose-like thick Ethernet, bends easily. Connections to it are made using industry standard BNC connectors to form T-junctions, rather than using vampire taps. These are easier to use and more reliable. Thin Ethernet is much cheaper and easier to install, but it can run for only 200m and can handle only 30 machines per cable segment.

Cable breaks, bad taps, or loose connectors can be detected by a devise called time domain reflectometry.

For 10Base5, a transceiver is clamped securely around the cable so that its tap makes contact with the inner core. The transceiver contains the electronics that handle carrier detection and collision detection. When a collision is detected, the transceiver also puts a

Computer Networks

special invalid signal on the cable to ensure that all other transceivers also realize that a collision has occurred.

The transceiver cable terminates on an interface board inside the computer. The interface board contains a controller chip that transmits frames to, and receives frames from, the transceiver. The controller is responsible for assembling the data into the proper frame format, as well as computing checksums on outgoing frames and verifying them on incoming frames.
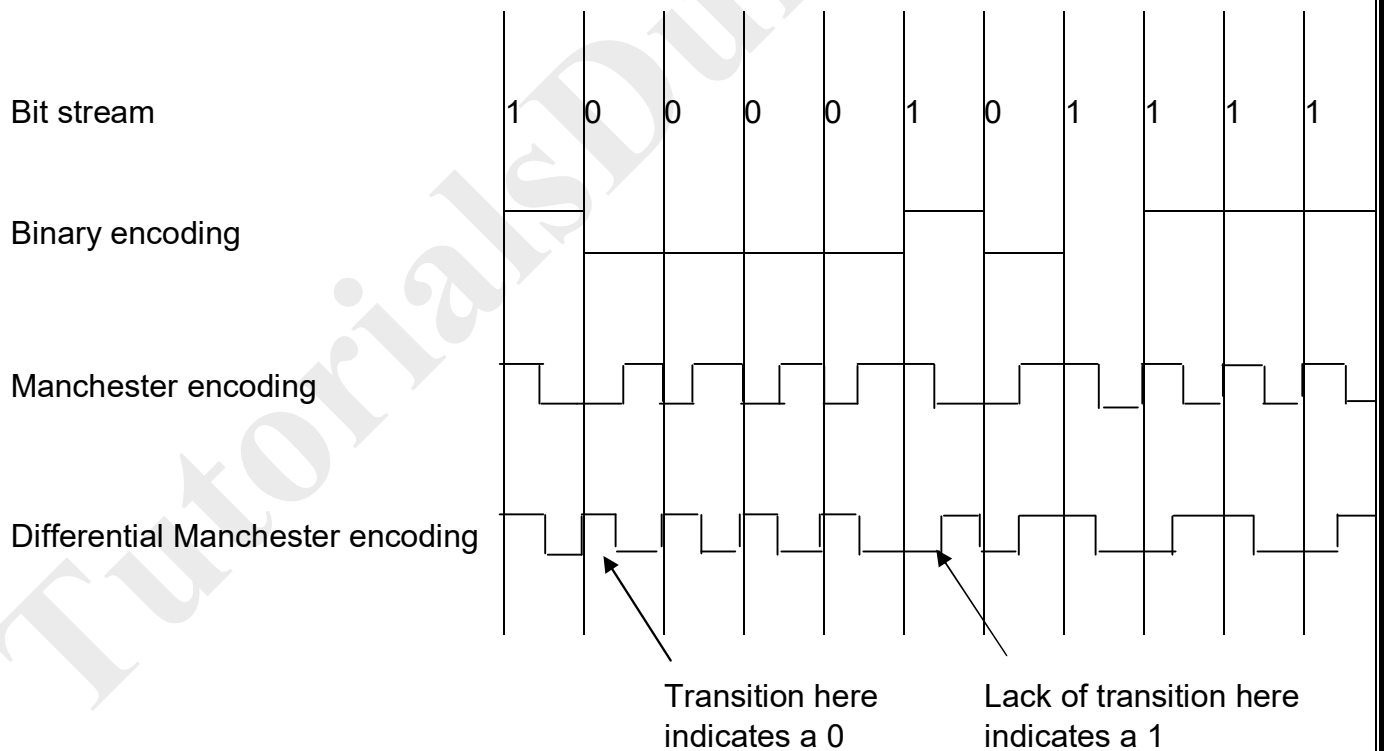
With 10Base2, the connection to the cable is just a passive BNC T-junction connector. The transceiver electronics are on the controller board, and each station always has its own transceiver.

With 10Base-T, there is no cable at all, just the hub (a box full of electronics). Adding or removing a station is simple in this configuration, and cable breaks can be detected easily. The disadvantage of 10Base-T is that the maximum cable run from the hub is only 100m, may be 150m if high-quality (category 5) twisted pairs are used. 10Base-Tis becoming steadily more popular due to the ease of maintenance. 10Base-F, which uses fiber optics. This alternative is expensive due to the cost of the connectors and terminators, but it has excellent noise immunity and is the method of choice when running between buildings or widely separated hubs.

Each version of 802.3 has a maximum cable length per segment. To allow larger networks, multiple cables can be connected by repeaters. A repeater is a physical layer device. It receives, amplifies, and retransmits signals in both directions. As far as the software is concerned, a series of cable segments connected by repeaters is no different than a single cable (except for some delay introduced by the repeater). A system may contain multiple cable segments and multiple repeaters, but no two transceivers may be more than 2.5km apart and no path between any two transceivers any traverse more than four repeaters.

Computer Networks

A   B

C

Trap

D

Backbone

A B   C   D

Repeater
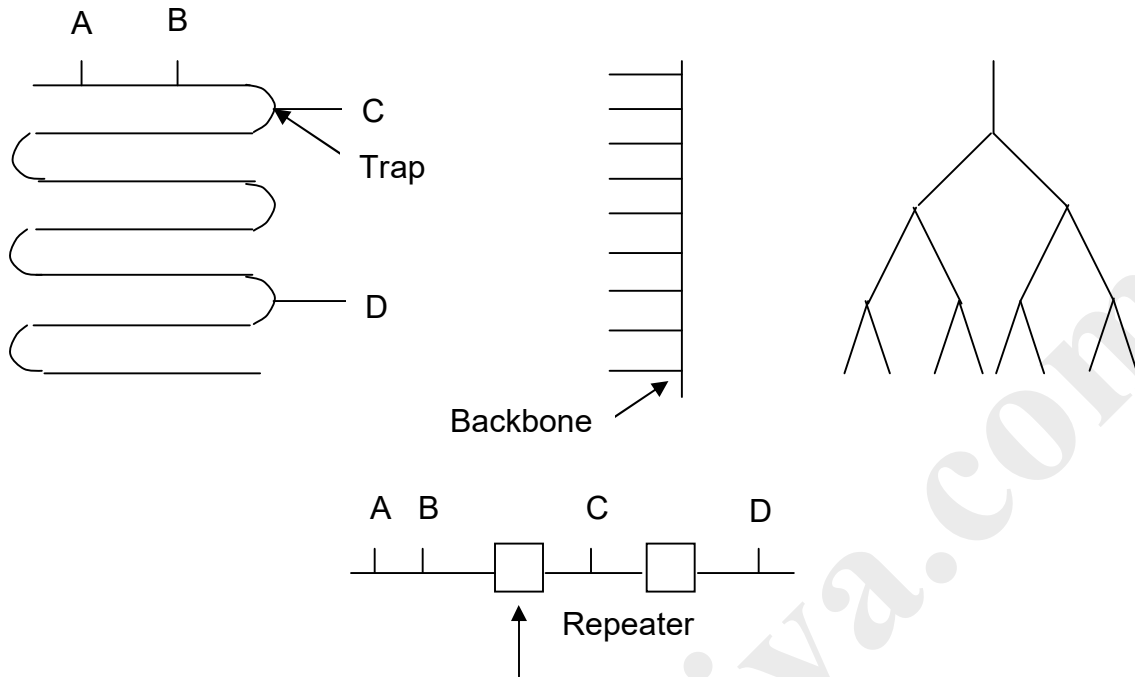
802.3 uses Manchester Encoding and differential Manchester Encoding

Bit stream   1 0 0 0 0 1 0 1 1 1 1

Binary encoding

Manchester encoding

Differential Manchester encoding

Transition here indicates a 0

Lack of transition here indicates a 1

Computer Networks

Bytes

7	1	2 or 6	2 or 6	2	0-1500	0-46	4
Preamble		Destination address	Source address		Data	Pad	Checksum

Start of frame delimiter

Length of data field
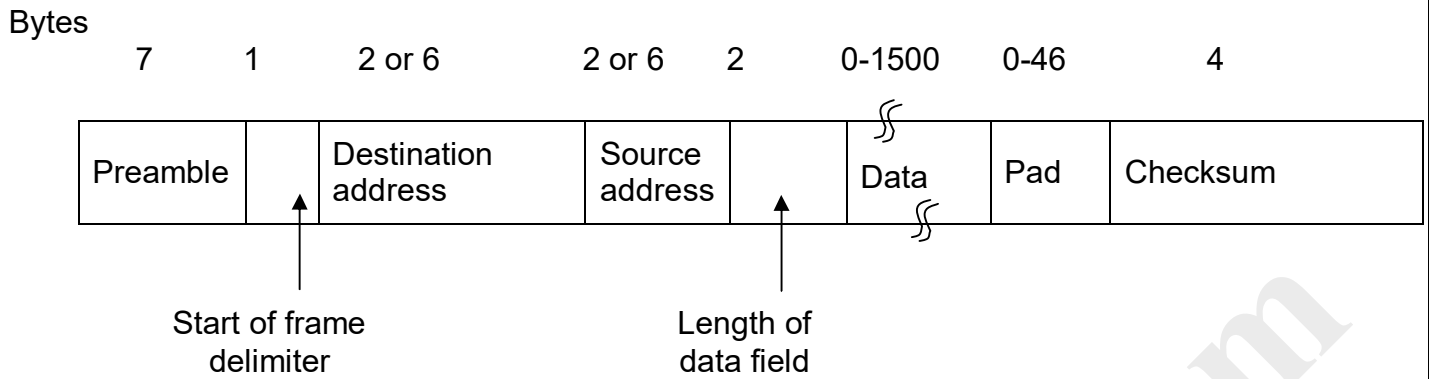
The 802.3 MAC sub layer protocol:

I) Preamble:

Each frame start with a preamble of 7 bytes each containing a bit pattern 10101010.

II) Start of frame byte:

It denotes the start of the frame itself. It contains 10101011.

III) Destination address:

This gives the destination address. The higher order bit is zero for ordinary address and 1for group address (Multi casting). All bits are 1s in the destination field frame will be delivered to all stations (Broad casting).

The 46th bit (adjacent to the high-order bit) is used to distinguish local from global addresses.

IV) Length field:

This tells how many bytes are present in the data field from 0 to 1500.

V) Data field:

This contains the actual data that the frame contains.

VI) Pad:

Valid frame must have 64 bytes long from destination to checksum. If the frame size less than 64 bytes pad field is used to fill out the frame to the minimum size.

VII) Checksum:

It is used to find out the receiver frame is correct or not. CRC will be used here.

Computer Networks

Other Ethernet Networks

```
                              │
        ┌─────────────────────┼─────────────────────┐
        ↓                     ↓                     ↓
     Switched               Fast                 Gigabit
```
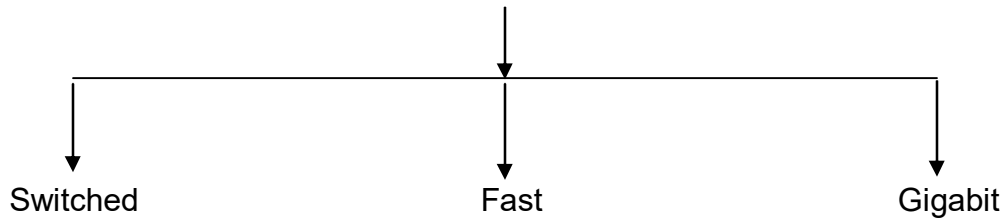
Switched Ethernet:

- 10 Base-T Ethernet is a shared media network.

- The entire media is involved in each transmission.

- The HUB used in this network is a passive device. (not intelligent).

- In switched Ethernet the HUB is replaced with switch. Which is a active device (intelligent)

Fast Ethernet

```
                              │
        ┌─────────────────────┼─────────────────────────────────┐
        ↓                                                        │
 ┌──────────────┐                                                │
 │  100 Base_x  │                                                │
 └──────────────┘                                                │
        │                                                        │
   ┌────┴───────────────────────┐                                │
   ↓                            ↓                                ↓
┌──────────────┐        ┌──────────────┐              ┌──────────────┐
│ 100 Base_Tx  │        │ 100 Base_Fx  │              │ 100 Base_T4  │
└──────────────┘        └──────────────┘              └──────────────┘

  2 pairs of                2 optical                    4 pairs of
  UTP or STP                 fibers                          UTP
```

Gigabit Ethernet

```
                              │
        ┌──────────────┬──────┴───────┬──────────────┐
        ↓              ↓              ↓              ↓
 ┌────────────┐ ┌────────────┐ ┌────────────┐ ┌────────────┐
 │ 100 Base_Sx│ │ 100 Base_Lx│ │ 1000 Base_Cx│ │ 1000 Base_T│
 │(optical fiber│ │(optical fiber│ │    STP     │ │    UTP     │
 │ multi mode)│ │multi or single│ │            │ │            │
 │            │ │    mode)   │ │            │ │            │
 └────────────┘ └────────────┘ └────────────┘ └────────────┘
```

Computer Networks
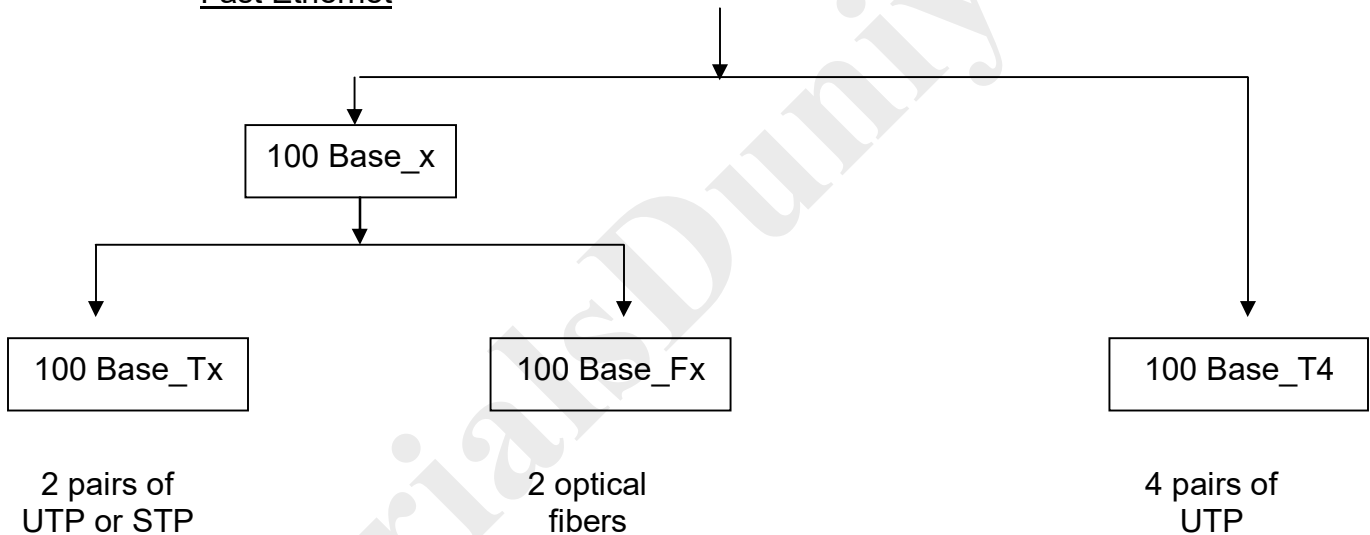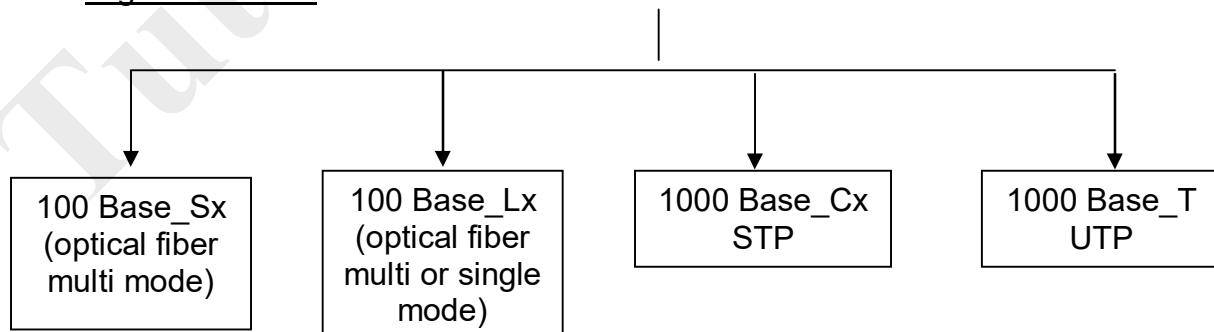
IEEE 802.4 (Token Bus)

802.3 frames do not have priorities, making them unsuited for real-time systems in which important frames should not be held up waiting for unimportant frames. A simple system with a known worst case is a ring in which the stations take turns sending frames. If there are n stations and it takes T sec to send a frame, no frame will ever have to wait more than nT sec to be sent.
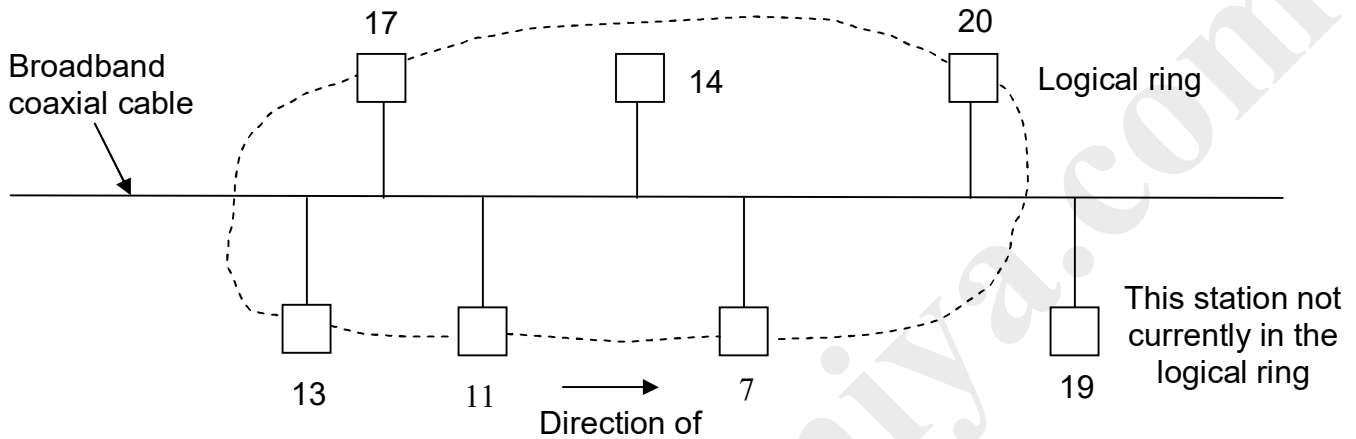
This standard, 802.4, describes a token bus. Physically, the token bus is a linear or tree-shaped cable onto which the stations are attached. Logically, the stations are organized into a ring, with each station knowing the address of the station to its "left" and "right." When the logical ring is initialized, the highest numbered station may send the first frame. After it is done, it passes permission to its immediate neighbor by sending the neighbor a special control frame called a token. The token propagates around the logical ring, with only the token holder being permitted to transmit frames. Since only one station at a time holds the token, collisions do not occur.

Since the cable is inherently a broadcast medium, each station receives each frame, discarding those not addressed to it. When a station passes the token, it sends a token frame specifically addressed to its logical neighbor in the ring, irrespective of where that station is physically located on the cable. It is also worth noting that when stations are first powered on, they will not be in the ring, so the MAC protocol has provisions for adding stations to, and deleting stations from, the ring. For the physical layer, the token bus uses the 75-ohm broadband coaxial cable used for cable television. Both single and dual-cable systems are allowed, with or without head-ends.

Bytes ≥	1	1	1	2 or 6	2 or 6	0-8182	4	1

∬

Computer Networks

			Destination address	Source address	Data	Checksum	

Frame control

Start of delimiter

End delimiter

Preamble
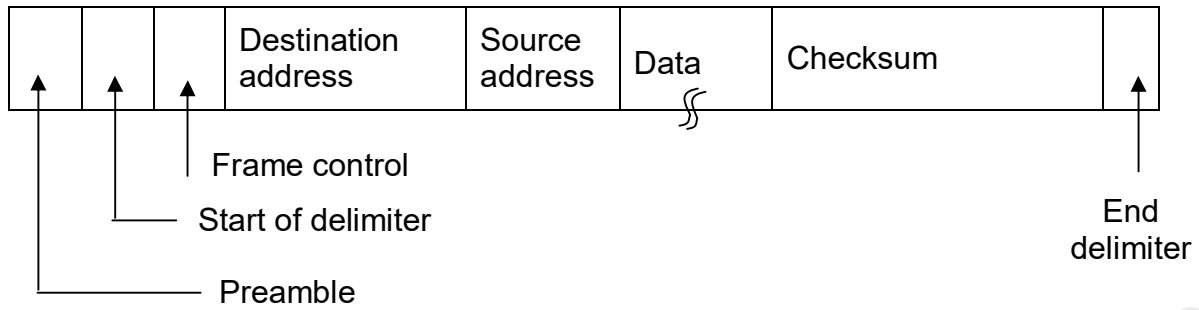
The frame control field is used to distinguish data frames from control frames. Fro data frames, it carries the frame's priority. It can also carry an indicator requiring the destination station to acknowledge correct or incorrect receipt of the frame.

For control frames, the frame control field is used to specify the frame type. The allowed types include token passing and various ring maintenance frames, including the mechanism for letting new stations enter the ring, the mechanism for allowing stations to leave the ring, and so on.

Connecting devices

```
                    Connecting
                     devices
                        |
          _____|_____
         |                             |
    Networking                   Internetworking
     devices                        devices
         |                             |
    _____|_____                  _____|_____
   |           |                |             |
Repeaters   Bridges          Routers      Gateways
```
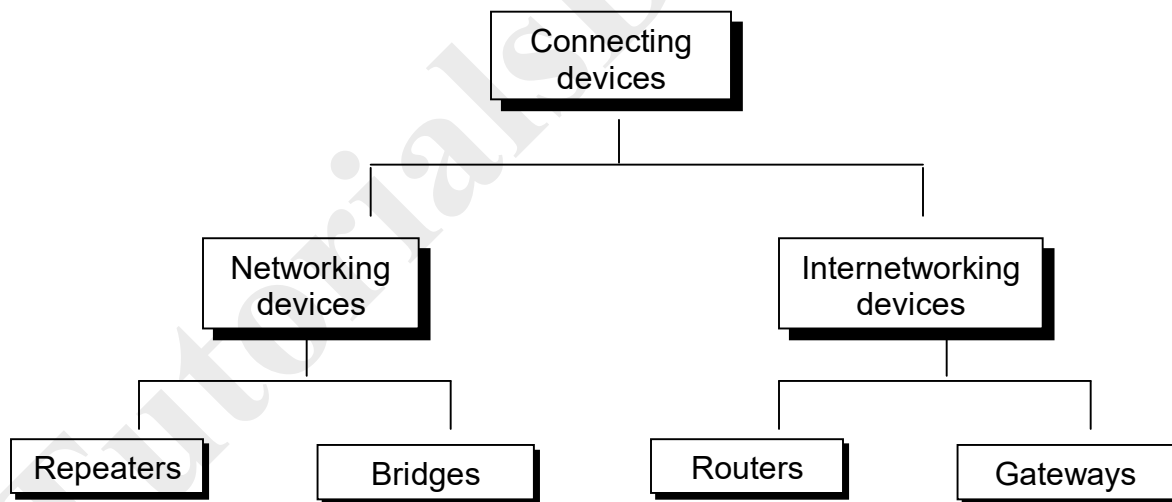
Connecting devices and the OSI model

Computer Networks

Application		Application
Presentation	**Gateway**	Presentation
Session		Session
Transport		Transport
Network		Network
Data link	**Router**	Data link
Physical	**Bridge**	Physical
	Repeate	
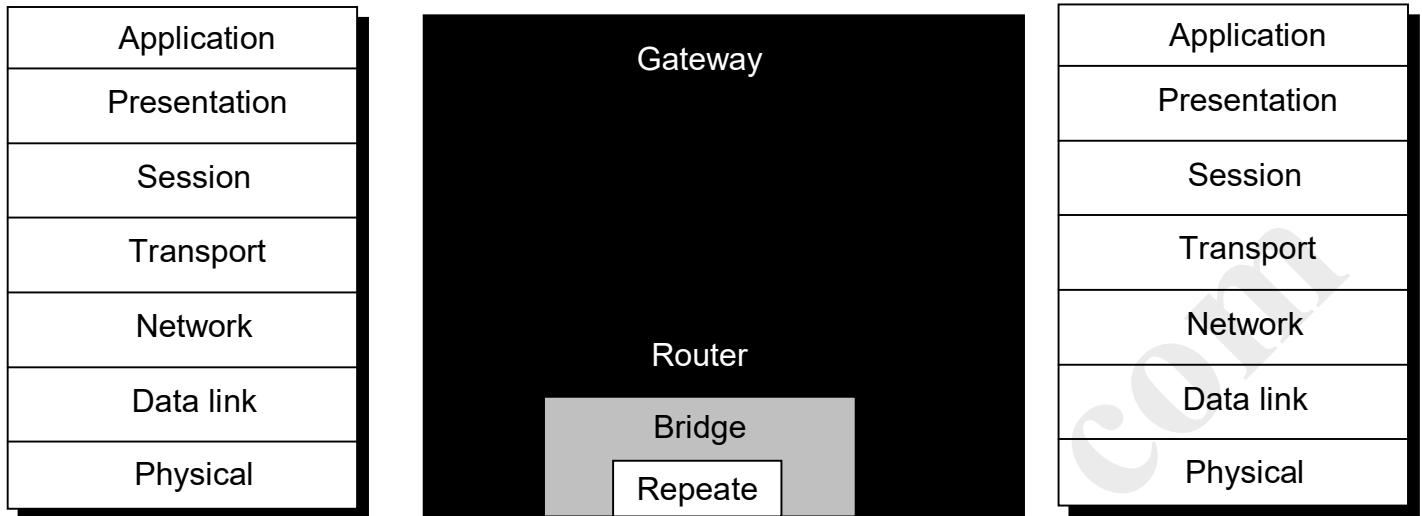
Bridges

LANS can be connected by devices called bridges, which operate in the data link layer. Bridges do not examine the network layer header and can thus copy IP, IPX, and OSI packets equally well.

The various reasons why the bridges are used.

1) Many university and corporate departments have their own LANS, primarily to connect their own personal computers, workstations, and servers. Since the goals of the various departments differ, different departments choose different LANS, without regard to what other departments are doing. Sooner or later, there is a need for interaction, so bridges are needed.

2) The organization may be geographically spread over several buildings separated by considerable distances. It may be cheaper to have separate LANS in each building and connect them with bridges and infrared links than to run a single coaxial cable over the entire site.

3) It may be necessary to split what is logically a single LAN into separate LANS to accommodate the load. Putting all the workstations on a single LAN- the total bandwidth needed is far too high. Instead multiple LANS connected by bridges are used.

4) In some situations, a single LAN would be adequate in terms of the load, but the physical distance between the most distant machines is too great (e.g., more than 2.5km for 802.3). Even if laying the cable is easy to do, the network would not work due to the

Computer Networks

excessively long round-trip delay. Only solution is to partition the LAN and install bridges between the segments.

5) There is the matter of reliability. On a single LAN, a defective node that keeps outputting a continuous stream of garbage will cripple the LAN. Bridges can be inserted at critical places, to prevent a single node which has gone berserk from bringing down the entire system.

6) And last, bridges can contribute to the organization's security. By inserting bridges at various places and being careful not to forward sensitive traffic, it is possible to isolate parts of the network so that its traffic cannot escape and fall into the wrong hands.

Types of Bridges

Simple Bridge

Simple bridges are the most primitive and least expensive type of bridge. A simple bridge links two segments and contains a table that lists the addresses of all the stations included in each of them. Before a simple bridge can be used, an operator must sit down and enter the addresses of every station. Whenever a new station is added, the table must be modified. If a station is removed, the newly invalid address must be deleted. Installation and maintenance of simple bridges are time-consuming and potentially more trouble than the cost savings are worth.

Transparent Bridge

A transparent, or learning, bridge builds its table of station addresses on its own as it performs its bridge functions. When the transparent bridge is first installed, its table is empty .As it encounters each packet, it looks at both the destination and the source addresses. It checks the destination to decide where to send the packet. If it does not yet recognize the destination address, it relays the packet to all of the stations on both segments. It uses the source address to build its table. As it reads the source address, it notes which side the packet came from and associates that address with the segment to which it belongs. By continuing this process even after the table is complete, a transparent bridge is also self-updating.

This bridge uses flooding and backward landing algorithms.

The routing procedure for an incoming frame depends on the LAN it arrives on (the source LAN) and the LAN its destination is on (the destination LAN), as follows.

1) If destination and source LANS are the same, discard the frame.

2) If the destination and source LANS are different, forward the frame.

Computer Networks

3) If the destination LAN is unknown, use flooding.

Two Parallel transparent bridges
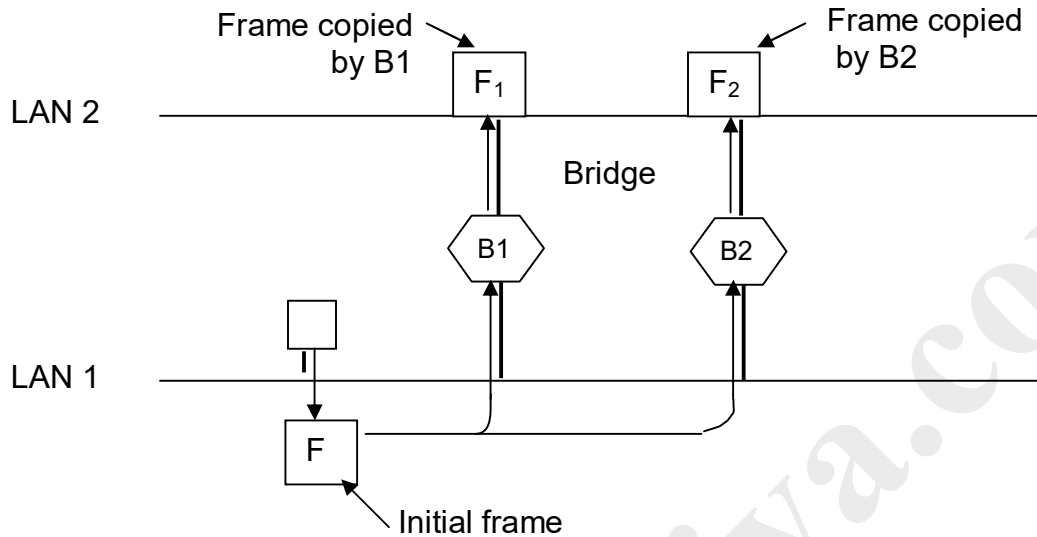
Spanning Tree Algorithm

Bridges are normally installed redundantly, which means that two LANs may be connected by more than one bridge. In this case, if the bridges are transparent bridges, they may create a loop, which means a packet may be going round and round, from one LAN to another and back again to the first LAN. To avoid this situation, bridges today use what is called the **spanning tree algorithm.**

Computer Networks

Expected Questions

1 Briefly explain the functions of Data Link Layer.

2 Discuss different types of Framing Methods.

3 Discuss various Error detecting and correcting methods.

4 Explain CRC method with your own example.

5 Explain Hamming code method with your own example.

6 What is meant by Flow control? Discuss different flow control methods.

7 Discuss various stop and wait protocols.

8 Explain Piggy backing, pipelining techniques.

9 Explain sliding window protocol.

10 Explain Go back 'n' and selective repeat protocols.

11 Prove that the channel utilization is 18% in ALOHA and 37% slotted ALOHA.

12 Discuss the CSMA protocols.

13 Explain different STOP and WAIT protocols.

14 Explain persistence and non-persistence CSMA protocol.

15 Discuss HDLC in detail.

16 What is the difference information fields in an HDLC I – frame and an U –frame.

17 Explain IEEE 802.3

18 Explain IEEE 802.4

19 Explain IEEE 802.5

20 Compare IEEE 802.3, IEEE802.4, IEEE802.5

21 Explain the operation of token bus

22 Explain the operation of token ring.

23 Prove that the channel utilization will be 37% in slotted ALOHA system.

24 Compare and Contrast pure ALOHA and Slotted ALOHA systems.

25 Write short note on CSMA/CD protocol.

26 Explain the collision free protocols.

27 Compare the ALOHA and CSMA protocols.

28 Explain Token bus and its frame format.

29 Explain token ring and its frame format.

30 Explain 802.3 frame format.

Computer Networks

31 Explain different connecting devices.

32 Explain different types of Bridges.

33 Give different reasons why a bridge is required.

****

Quiz Questions

1. What is the principle involved in the ALOHA?

2. What is the principle involved in Slotted ALOHA?

3. What is the principle involved in CSMA?

4. What is meant by Non Persistence CSMA?

5. What is meant by Persistence CSMA?

6. What is meant by P-Persistence CSMA?

7. The channel utilization in slotted ALOHA is _____ and in pure ALOHA _____.

8. What is meant by exponential back-off algorithm?

9. What is meant by Vulnerable period w.r.t ALOHA?

10. What is meant by bit map protocol?

11. What is meant by binary count down protocol?

12. What is the function of Data Link Layer?

13. IEEE 802.3 is called _____.
14. IEEE 802.3 will use _____ protocol.
15. 10 Base 5 is called _____.
16. What is meant by preamble in 802.3 frame format?
17. Why pad filed is used in 802.3 frame format?
18. Which purpose the time domain reflectometry is used?
19. In transparent bridge which algorithms are used to fill the routing table.
20. Why Spanning tree bridges are used?

Computer Networks

21. Gateways are used in which layer?
22. IEEE 802.4 is called _____.
23. IEEE 802.5 is called _____.
24. How frames will be transmitted in IEEE 802.4?
25. Give 802.3 frame format?
26. Give 802.4 frame format?
27. What are different types of Ethernet available?
28. 802.3 uses _____ type of encoding.
29. To join two or more segments of Ethernet _____will be used.
30. What is a token w.r.t 802.4.
31. How the cable breaks problem can be solved in 802.5?
32. Give the 802.5 Frame format ?
33. Give an example for character count framing method and explain the fields.
34. What is the draw back with the above method?
35. What are characters that are used in character stuffing method at the beginning and ending of a frame?
36. Expand the above characters?
37. For the data given below : how it will be sent using character stuffing method?
    abcdefghijka DLE 123456789RAMARAO DLE
38. What is the draw back with this method?
39. In bit stuffing method how a frame will start?
40. For the given data using bit stuffing method. How data will be sent?
01101111101111101111101111111011
41. Find out the LRC & VRC for the below characters?

    0   0   1   1   0   1
    1   1   0   1   0   0
    0   1   1   0   1   0
    0   0   1   0   1   1

42. What is the draw back with the LRC method?
43. How many zero bits will be append for the frame in CRC method?
44. What is meant by 'piggy backing' ?
45. What is meant by stop and wait protocol?
46. What is meant by pipelining?
47. What is the essence of sliding window protocol?
48. A channel has a propagation delay of 20m sec and has a frame size of 80bits. For what range of band width does stop and wait give an efficiency of at least 50 percent?
49. How will you find out how many Hamming code bits should be incorporated?

Computer Networks

UNIT – III
NETWORK LAYER

Functions of Net Work layer

1. Routing   2. Congestion Control

Routing algorithms

The main function of the network layer is routing packets from the source machine to the destination machine. Routing algorithm can be grouped into two major classes. Nonadaptive and Adaptive algorithms.

Non adaptive	**Adaptive**
1) Routing decisions are not based on measurements or estimates of the current traffic and topology.	1) Routing decisions are based on measurements of the current traffic and topology.
2) The route is computed well in advance.	2) The route is computed depends on situation.
3) When the network is booted the routers are downloaded.	3) The routers are not downloaded.
4) This is a static routing.	4) This is a dynamic routing.

Shortest Path Routing:

This is a static routing algorithm. The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line. To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.

Computer Networks

(a)

(b)

(c)

(d)

(e)

(f)

Computer Networks
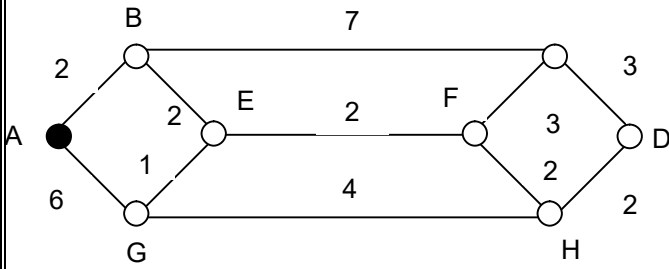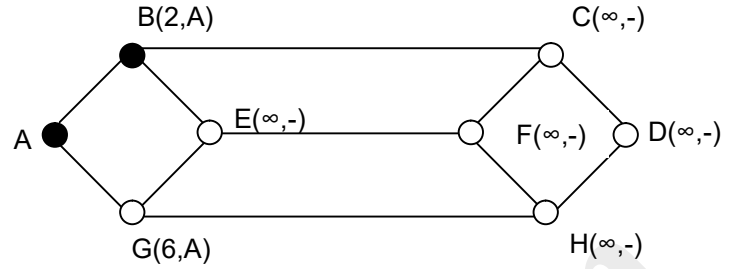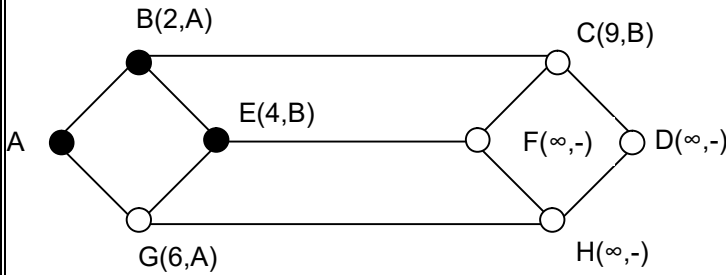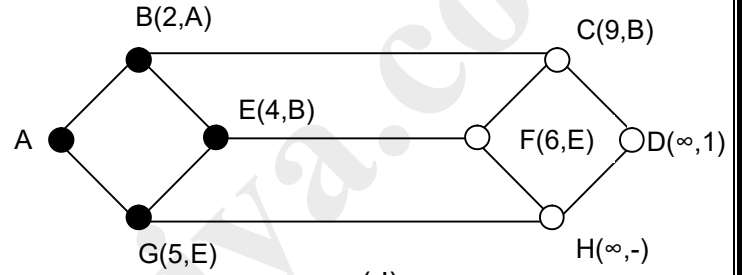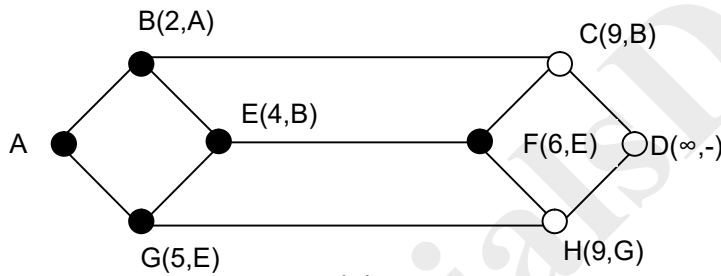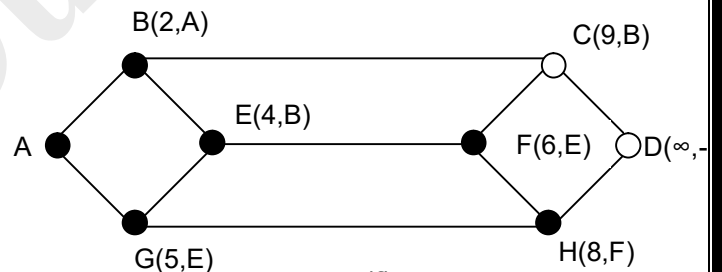
One-way of measuring path length is the number of hops. Using this metric, the paths ABC and ABE are equally long. (Two hops).

Another metric is the Geographic distance in Kilometers. ABC is clearly longer than ABE.

Many other metrics are also possible besides hops and physical distance. Each are could be labeled with the mean queuing and transmission delay for some standard test packets as determined by hourly test runs. With this graph labeling, the shortest path is the fastest path, rather than the path with the fewest arc or kilometers.

In most general case, the labels on the arcs could be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured delay and other factors.

The shortest path can be calculated using Dijkstra method. Each node is labeled with its distance from the source along the best known path. Initially, no paths are known, so all nodes are labeled with infinity. As the algorithm proceeds and paths are found, the labels may change, reflecting better paths. Initially all labels are tentative. When it is discovered that a label represents the shortest path from the source to that node, it is made permanent and never changed thereafter.

In the above diagram, let the weights represents the distance. To find out the shortest path from A to D. We start by marking A as permanent. The examine each one with the distance to A, relabeling each one with the distance to A. Whenever a node is relabeling also label it with the node from which the probe was made. After examing each of the nodes adjacent to A, examine all the tentatively labeled nodes in the whole graph and make the one with the smallest label permanent. This one becomes the new working node.

The same procedure is adopted to all the nodes and the shortest path is found.

Flooding:

This is a static algorithm. In this, every incoming packet is sent out on every outgoing line except the one it arrived on. Flooding will generate vast numbers of duplicate packets, some measures have to take to dump the duplicate packets. One such measure is to have a hop counter contained in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero. The hop counter should be initialized to the length of the path from source to destination. If the sender does not know how long the path is it can initialize the counter to full diameter of the subnet.

A variation of flooding is 'Selective Flooding'. In this the routers do not send every incoming packet on every line, instead only on those lines that are going approximately in the right direction which leads to the destination.

Computer Networks

Advantages

1) In military applications, where large numbers of routers are blown, flooding is desirable.

2) In Distributed database applications, it is some times necessary to update all the databases concurrently, in which flooding is useful.

3) It is used as a metric against which other routing algorithms are compared.

4) Flooding chooses the shortest path, because it chooses all possible path in parallel.

Flow-based Routing:

        The flooding and shortest path algorithm takes the topology in to account. Flow based routing algorithm uses both topology and load for routing.

        In some networks the mean data flow between each pair of nodes is relatively stable and predictable. The average traffic is known in advance and to a reasonable approximation, constant in time, it is possible to analyze the flows mathematically to optimize routing.

        The basic idea behind this, for a given line, if the capacity and average flow are known, it is possible to compute the mean packet delay on that line. From the mean delays on all the lines, the mean packet delay for the whole subnet.

        To use this technique, certain information must be known in advance. 1) About the subnet topology 2) about the traffic 3) the line capacity 4) a routing algorithm

The fig.(b) gives the information packets /sec go from source i to destination j. Given this information, it is easy to calculate the total in line for i i.e. λ_i. Using the traffic from the source to destination the mean number of packets/sec on each line. μc_i can be calculated, assuming a mean packet size $1/\mu$. The mean delay for each line can be derived where $1/\mu$ is the mean packet size in bits, λ is the mean flow in packets/sec.

With a capacity μc = 25 packets/sec and an actual flow λ = 14 packets/sec, the mean delay is 91 m sec. When λ =0, the mean delay is 40m sec. With this example we can say the delay depends on both queuing and service time.

The mean delay time for the entire subnet can be calculated as the sum of each of the eight lines, with the weight being the fraction of the total traffic using that line.

Computer Networks
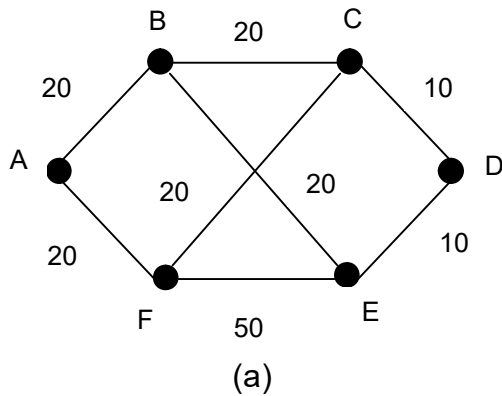
Destination

	A	B	C	D	E	F
A		9 AB	4 ABC	1 ABFD	7 AE	4 AEF
B	9 AB		8 BC	3 BFD	2 BFE	4 BF
C	4 CBA	8 CB		3 CD	3 CE	2 CEF
D	1 DFBA	3 DFB	3 DC		3 DCE	4 DF
E	7 EA	2 EFB	3 EC	3 ECD		4 EF
F	4 FEA	4 FB	4 FEC	4 FD	4 FE	

(Source, rows labeled A–F on the left)

(a)

(b)

Distance Vector Routing:

This is a dynamic routing algorithm. This algorithm operates by having each router maintain a table (i.e. a vector) giving the best known distance to each destination and which line to use. These tables are updated by exchanging information with the neighbors.

The routing table indexed by and containing one entry for each router in the subnet. This entry contains two parts: The preferred outgoing line to use for the destination and an estimate of time or distance to that destination. The metric used might be number of hops, time delay in msec, total number of packets queued along the path or something similar.

The router is assumed to know the distance to each of its neighbors. If the metric is hops, the distance is just one hop. If the metric is queue length, the router examines each queue. If the metric is delay the router can measure it directly with a special ECHO packets.

Consider an example, in which the delay is used as metric and the router knows the delay to each of its neighbors. Once every T msec each router send to each neighbor a list of its estimated delays to each destination. It also receives a similar list from each neighbor. Let x_i being x's estimate of how long it takes to get router 'i'. If the router knows that the delay to x is 'm' m sec. To get router i via x is (x_i +m) m sec. By performing this calculation for each neighbor, a router can find out which estimate is the best and use that estimate and the corresponding line in its new routing table.

Computer Networks

Subnet

New estimated delay from J

	A	I	H	K		Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	-
K	24	22	22	0	6	K
L	29	33	9	9	15	K

JA delay is 8   JI delay is 10   JH delay is 12   JK delay is 6

New routing table for J

Vectors received from J's four neighbors
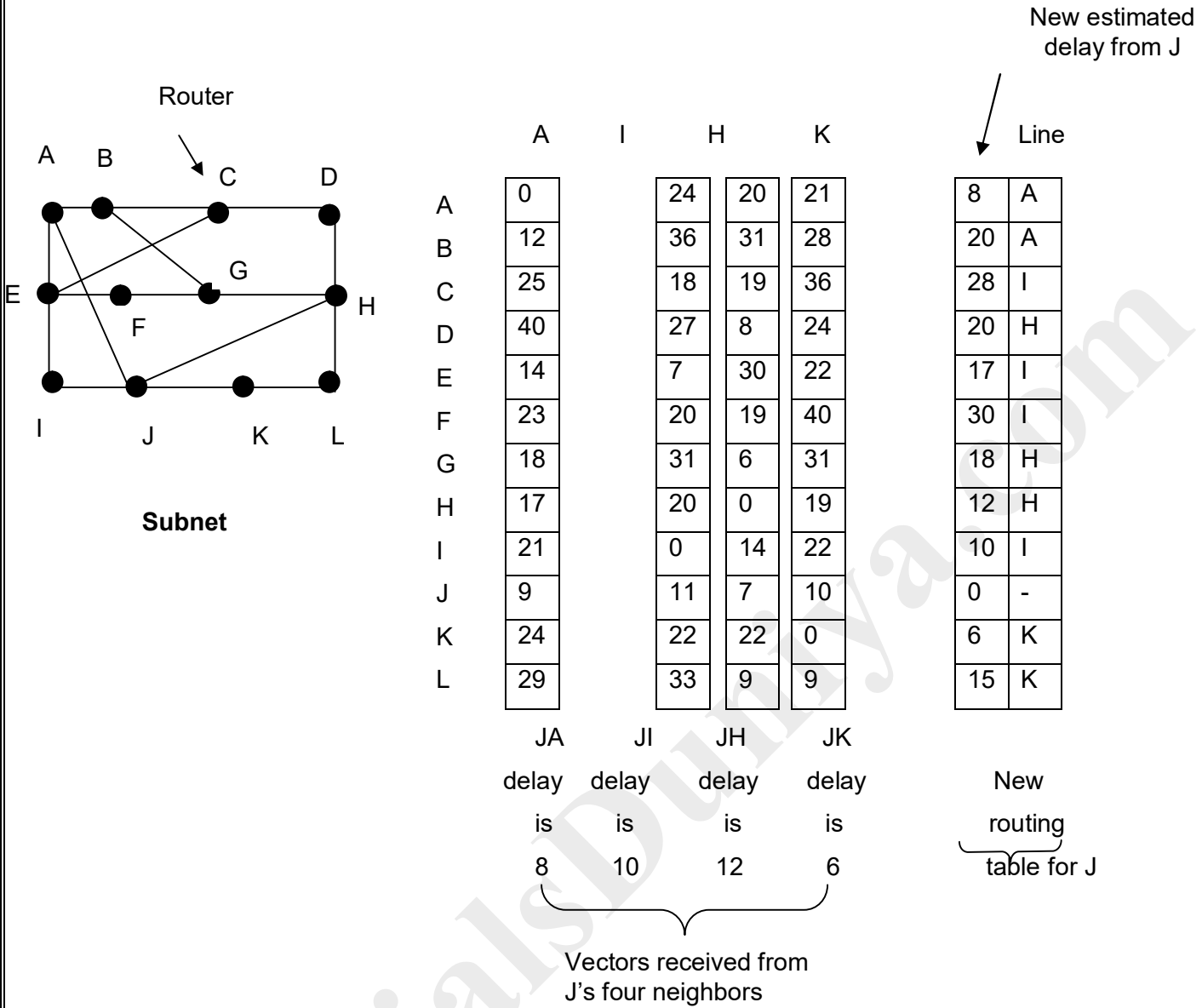
Input from A,I,H, K and new routing table for J

Fig.(a) shows the subnet and fig.(b) shows the vectors of J for its neighbors. Fig.(c) shows the new routing table for J. Let JA delay is 8, JI delay is 10, JH is 12, JK is 6.

The new route to G from J can be calculated as follows.

J can get A in 8 m sec.

A can get G in 18 m sec(from table)

∴ J can get G in (8+18) 26 m sec.

Similarly the delay to G via I,H and K is (31 +10) 41, (6+12)18, (31+6)37 m sec.

The best of these values is 18, so it makes an entry in its routing table that the delay to G is 18 m sec and that route is via H.

Computer Networks

Hierarchical Routing:

As network grow in size, the router routing tables grow proportionally. Not only more memory consumed by ever increasing tables, but more CPU time is needed to scan them more bandwidth is needed to send status reports about them. At a certain point the network may grow to the point where it is no longer feasible for every router to have an entry for every other router, so the routing will have to be done hierarchically.

When hierarchical routing is used, the routers are divided into 'Regions'. Each router knows all the details about how to route packets to destinations within its own region, but doesn't know the internal structure of other regions. For huge networks, a two-level hierarchy may be insufficient, it may be necessary to divide the regions into clusters, clusters into zones and zones into groups and soon.

Consider a two level hierarchy with five regions as shown in fig. one router needs 17 entries for one table. The network contains 17 routers. So the total no. of entries will be 17 x 17. This is for when we are not using hierarchy.

When routing is done hierarchically a router will consists of entries for all the local routers and regions only.

For Ex. The router 1A consists of entries as shown in fig.(c). Hierarchical routing has reduced the table from 17 to 7 entries.

Full table for 1A
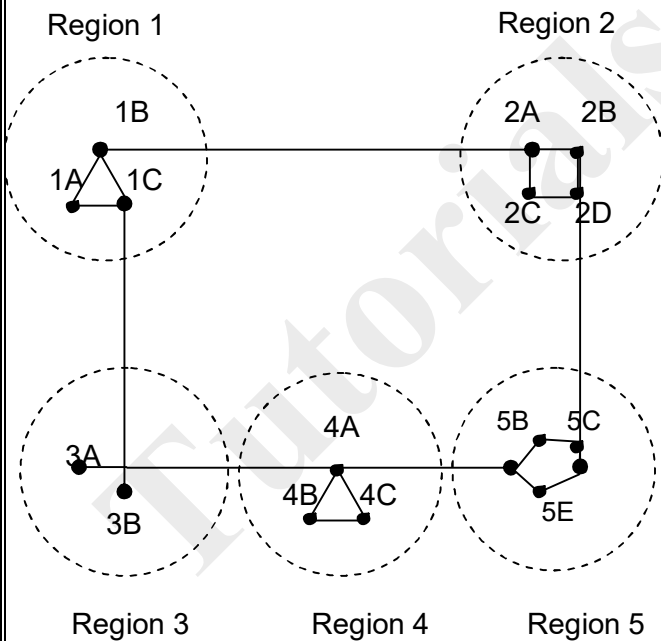
Hierarchical table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
3A	1C	4
3B	1C	3
3C	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(a)   (b)   (c)

Disadvantages:

Computer Networks

Using hierarchy the path lengths will be increased. For Ex. The best path from 1A to 5C is via region 2. But using hierarchy routing all traffic to region 5 goes via region 3, because it is the best for most destination in region 5.

Ex. Consider a 720 routers subnet.

Without hierarchy each router required 720 entries. Total entries will be 720 x 720, with hierarchy, if the subnet is portioned into 24 regions and 30 routers/region, then each router needs 30+23 = 53 entries only.

If a 3-level hierarchy used, with 8 clusters, each contains 9 regions and 10 routers/region. Each router needs 10 + 8 + 7 = 25 entries

For a 'N' router subnet the optimal number of routers = lnN

The total no. of entries /router = elnN

Broadcast Routing:

In some applications, hosts need to send messages to many or all other hosts. For Ex. Weather reports, stock market, updates etc. Sending a packet to all destinations simultaneously is called 'Broad Casting'.

1) One method is sending distinct packet to each destination by the source. This method wastes the bandwidth and also requires the source to have a complete list of all destinations.

2) The second is using Flooding technique. This generates too many packets and consumes too much bandwidth.

3) Another method is multi destination routing. In this each packet contains either a list of destinations or a bit map indicating the desired destinations. When a packet arrives at a router, the router checks all the destinations to determine the set of output lines that will be needed. The router generates a new copy of the copy for each output line to be used and includes in each packet only those destinations that are to use the line. This routing is like separately addressed packets except that several packets must follow the same route.

4) Another algorithm which uses the spanning tree. A spanning tree is a subnet of the subnet that includes all the routers but contains no loop. If each router knows which of its lines belong to the spanning tree, it can copy an incoming broadcast packet onto all spanning tree lines except the one it arrived on. This method makes use of bandwidth excellently and generates minimum no. of packets necessary to do the job. The only disadvantage is that each router must have knowledge of some spanning tree.

5) One more algorithm is an attempt to approximate the behavior of the previous one, even when the routers do not know anything at all about spanning trees. The idea is remarkably simple once it has been pointed out. When a broadcast packet arrives at a router, the router checks to see if the packet arrived on that line that is normally used for sending packets to the source of the broadcast. If so, there is an excellent chance that the broadcast packet itself followed the best
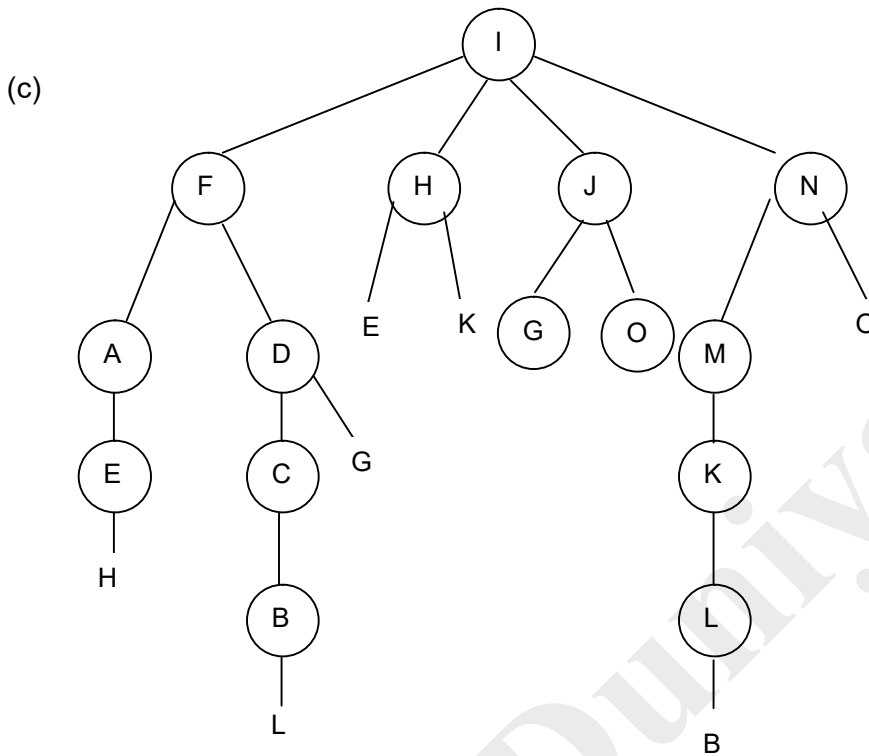
Computer Networks

route from the router and is therefore the first copy to arrive at the router. This being the case, the router forwards copies of it onto all lines except the one it arrived on. If, however, the broadcast packet arrived on a line other than the preferred one for reaching the source the packet is discarded as a likely duplicate.

(a)

(b)

(c)
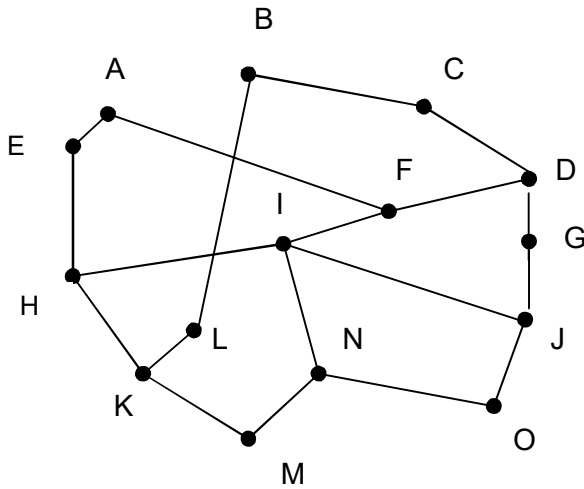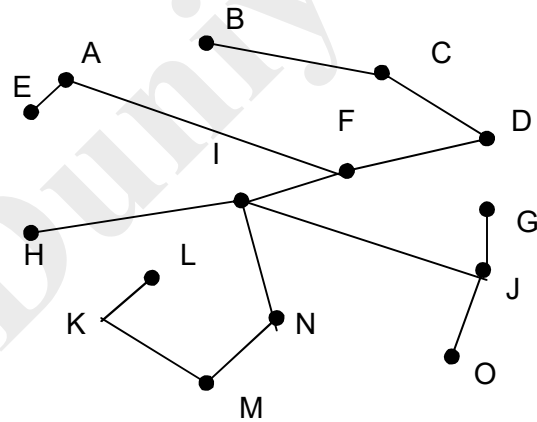
Multicast Routing :

For some applications, it is necessary for one process to send a message to all other members of the group. If the group is small, it can just send each other member a point-to-point message. If the group is large this strategy is expensive. Some times broad casting is used, but using broad casting is used, but using broadcasting to inform 1000 machines on a million node network is inefficient because most receivers are not interested in the message. Thus it is needed to send message to well-defined groups. Sending message to such a group is called 'multicasting'.

To do multicasting, group management is required. Some way is needed to create and destroy groups and for processes to join and leave groups. When process joins a group, it informs its host of this fact. It is important that routers know which of their hosts belong to which group. Either hosts most inform their routers about change in group membership or routers must query their hosts periodically. Routers tell their neighbors, so the information propagates through the subnet.

To do multicast routing, each router computes a spanning tree covering all other routers in the subnet. When a process sends a multicast packet, to a group, the first router examines its spanning tree and prunes it, removing all lines that do not lead to hosts that are members in the group. Multicast packets are forwarded. Only along the appropriate spanning tree.

Computer Networks

Congestion Control Algorithms

What is Congestion?

When too many packets are present in the subnet performance degrades. This situation is called Congestion.

The number of packets dumped into the subnet are within its carrying capacity, they are all delivered.

However, if the traffic increases too far, the routers are unable to cope and begin losing packets.

At very high traffic, performance collapse completely and almost no packets are delivered.

What factors will lead to congestion?

1. Three or four input lines and only one output line queue will build up.

    If there is insufficient memory to hold all of them, packets will lost.

    Adding infinite memory congestion gets worse, because by the time packets get to the front of the queue, the time out and duplicates have been sent.

2. Slow processors (routers) can cause congestion.

    - A slow processor perform the book keeping tasks very slow, queues will build up.

3. Low band-width lines also cause congestion

    - Upgrading lines but not changing the processor and vice-versa shifts the bottleneck.

    This problem will persist until all components are in balance.

What is the difference between Congestion control and Flow control?

Congestion control is global issue and flow control is local issue.

Ex:

- Consider a network with a capacity of 1000Gbps on which a super computer is trying to transfer a file to a personal computer at 1Gbps.Here a flow control is needed.

- Consider a network with 1Mbps lines and 1000 large computers, more than half are trying to transfer files a 100kbps to the other half. The problem is here is the total offered traffic exceeds than the network handle.

Computer Networks

General Principles Of Congestion Control:

The congestion control can be done by two methods

Open loop

Closed loop

Open loop: These solutions attempt to solve the problem by good design, to make sure that it does not occur in the first place. Once the system is up and running, midcourse corrections are not made.

Tools for doing open-loop control include deciding when to accept new traffic, deciding when to discard packets and which ones, and making scheduling decisions at various points in the network.

In contrast, closed loop solutions are based on the concept of a feedback loop. This approach has three parts when applied to congestion control:

1. Monitor the system to detect when and where congestion occurs.
2. Pass this information to places where action can be taken.
3. Adjust system operation to correct the problem.

Congestion Prevention Policy :

Traffic Shaping:

One of the main causes of congestion is that traffic is often bursty. If hosts could be made to transmit at a uniform rate, congestion would be less common. Another open loop method to help manage congestion is forcing the packets to be transmitted at a more predictable rate. This approach to congestion management is widely used in ATM networks and is called traffic shaping.

Monitoring a traffic flow is called traffic policing. Agreeing to a traffic shape and policing it afterward are easier with virtual circuit subnet than with datagram subnets.

Leaky Bucket Algorithm

Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at a constant rate, ρ, when there is any water in the bucket, and zero when the bucket is empty. Also, once the bucket is full, any additional water entering it spills over the sides and is lost.

Computer Networks

Host
Computer

Packet

Unregulated
Flow

Interface
Containing
a leaky bucket

The bucket
holds
packets

Regulated
flow
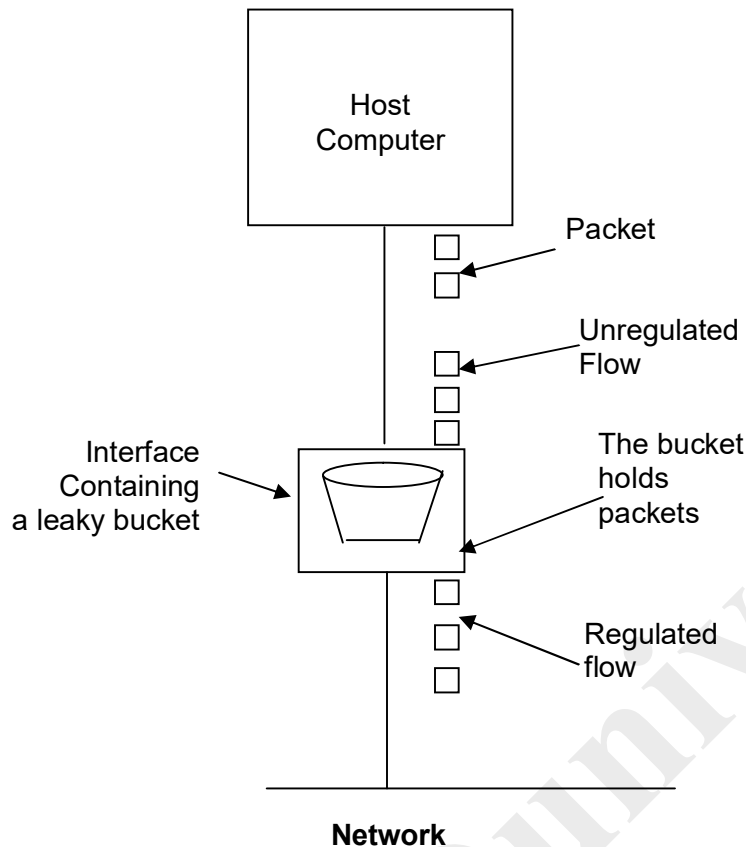
Network

The same idea can be applied to packets, as shown in fig. Conceptually, each host is connected to the network by an interface containing a leaky bucket, that is, a finite internal queue. If a packet arrives at the queue when it is full, the packet is discarded. In other words, if one or more processes within the host try to send a packet when the maximum numbers are already queued, the new packet is unceremoniously discarded. This arrangement can be built into the hardware interface or simulated by the host operating system.

The host is allowed to put one packet per clock tick onto the network. Again, this can be enforced by the interface card or by the operating system. This mechanism turns an uneven flow of packets from the user processes inside the host into an even flow of packets onto the network, smoothing out bursts and greatly reducing the chances of congestion.

Implementing the original leaky bucket algorithm is easy. The leaky bucket consists of a finite queue. When a packet arrives, if there is room on the queue it is appended to the queue; otherwise, it is discarded. At every clock tick, one packet is transmitted (unless the queue is empty).

Computer Networks

The Token Bucket Algorithm:

The leaky bucket algorithm enforces a rigid output pattern at the average rate, no matter how bursty the traffic is. For many applications, it is better to allow the output to speed up somewhat when large bursts arrive, so a more flexible algorithm is needed, preferably one that never loses data. One such algorithm is the **token bucket algorithm**.
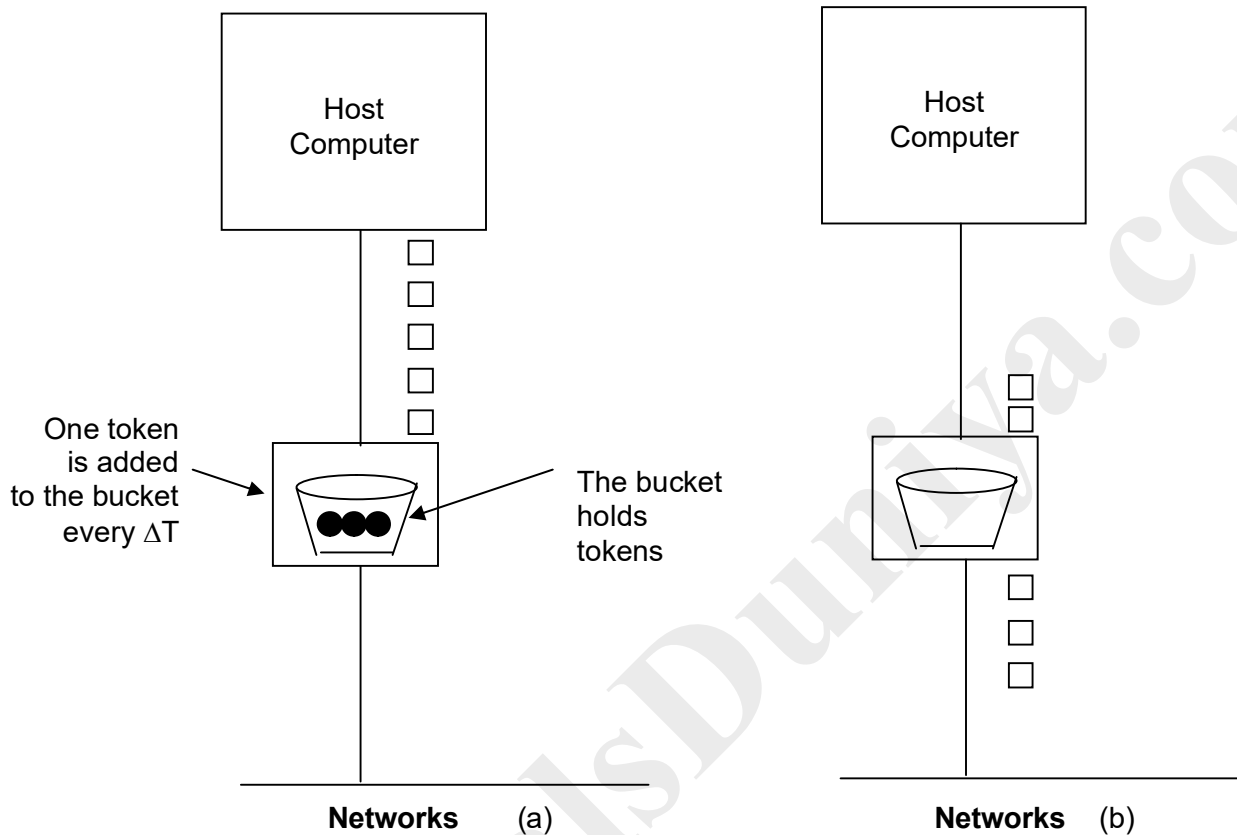
In this algorithm, the leaky bucket holds tokens, generated by a clock at the rate of one token ever ∆T sec. In figure (a), we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure(b), we see that three of the five packets have gotten through, but the other two are stuck waiting for two more tokens to be generated.

The leaky bucket algorithm does not allow idle hosts to save up permission to send large bursts later. The token bucket algorithm does allow saving, up to the maximum size of the bucket, n.

Another difference between the two algorithms is that the token bucket algorithm throws away tokens when the bucket fills up but never discards packets. In contrast, the leaky bucket algorithm discards packets when the bucket fills up.

Computer Networks

Congestion Control in Datagram Subnets:

Each router can easily monitor the utilization of its output lines and other resources. It can estimate each line about the recent utilization of that line (u). Periodically a sample at the instantaneous line utilization (f) can be mad and u updated.

$u_{new} = a \, u_{old} + (1-a)f$

Where a is constant determines how fast the router forgets recent history.

Whenever u moves above the threshold, the output line enters a 'warning' state. Each new arriving packet is checked if its output line is warning state. If it is some action is taken.

The Warning Bit:

When the output line reaches to warning state it is signaled by setting a special bit in the packet's header. When the packet arrived at its destination, the transport entity copied the bit into the next acknowledgement sent back to source. The source then cot back on traffic. As long as the router was in warning state, it continued to set warning bit. As long as the warning bits continued to flow in, the source continued to decrease its transmission rate.

Choke packets:

In this algorithm, the router sends a choke packet back to the source host. The original packet is tagged so that it will not generate any more choke packets farther along the path and is then forwarded in the usual way.

When the source host gets the choke packet, it is required to reduce the traffic sent to the specified destination by X percent. Since other packets aimed at the same destination are probably already under way and will generate yet more choke packets, the host should ignore choke packets referring to that destination for a fixed time interval. After that period has expired, the host listens for more choke packets for another interval. If one arrives, the line is still congested, so the host reduces the flow still more and begins ignoring choke packets again. If no choke packets arrive during the listening period, the host may increase the flow again.
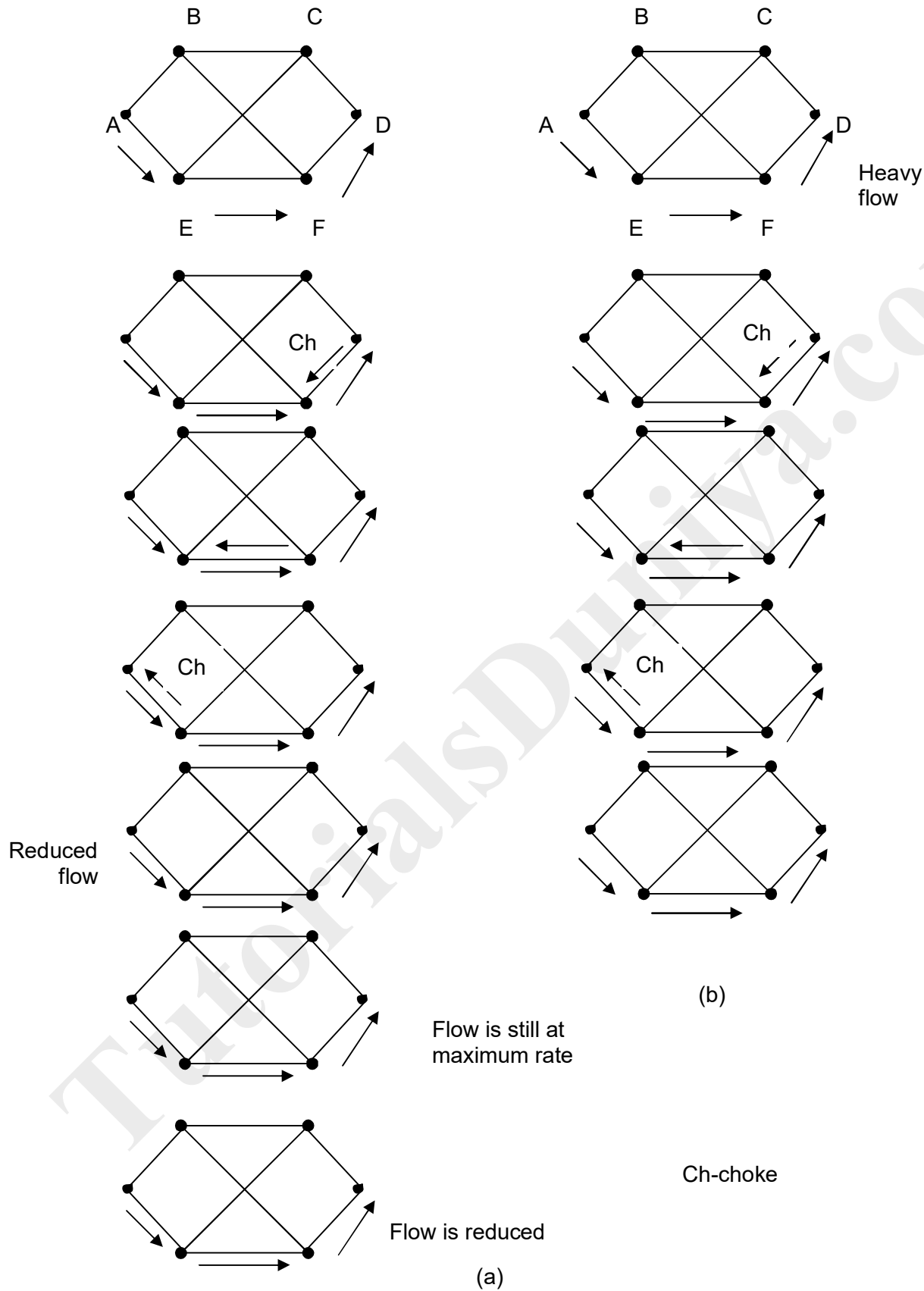
The first choke packet causes the data rate to be reduced to 0.50 of its previous rate, the next one causes a reduction to 0.25, and so on. Increases are done in smaller increments to prevent congestion from reoccurring quickly.

Hop by Hop choke packets:

For example, let the host A is sending packets to D. as shown in fig.(1). If D runs out of buffers, it will take sometime for a choke packet to reach A to tell it to slow down. This is shown in fig 2,3,4.In this time another packets will be sent. Only after some more time the router D will be noticing a slower flow (fig.7).

In other approach, as soon as choked packet reaches to F it cuts down the flow to D and D will get immediate relief. (like a headache remedy in a TV). In the next set up, when choke reaches to E it also cuts down the flow to F which in turn gives relief to F. Finally, when the choke packet richer A and the flow genuinely slows down.

Computer Networks

(a) A choke packet that affects only the source   (b) A choke packet that affects each hop it passes through.

Heavy flow

Reduced flow

Flow is still at maximum rate

Ch-choke

Flow is reduced

(a)

(b)

Computer Networks

Load Shedding:

Load Shedding is a fancy way of saying that when routers are being inundated by packets that they cannot handle, they just throw them away.

A router drowning in packets can just pick packets at random to drop, but usually it can do better than that. Which packet to discard may depend on the applications running. For file transfer, an old packet is worth more than a new one because dropping packet 6 and keeping packets 7 through 10 will cause a gap at the receiver that may force packets 6 through 10 to be retransmitted (if the receiver routinely discards out-of –order packets). In a 12-packet file, dropping 6 may require 7 through 12 to be retransmitted, whereas dropping 10 may require only 10 through 12 to be retransmitted. In contrast, for multimedia, a new packet is more important than an old one. The former policy (old is better than new) is often called wine and the latter (new is better than old) is often called milk.

A step above this in intelligence requires cooperation from the senders. For many applications, some packets are more important than others. For example, certain algorithms for compressing video periodically transmit an entire frame and then send subsequent frames as differences from the last full frame. In this case, dropping a packet that is part of a difference is preferable to dropping one that is part of a full frame. As another example, consider transmitting a document containing ASCII text and pictures. Losing a line of pixels in some image is far less damaging than losing a line of readable text.

Internetworking

When two or more networks are connected it is called Internet. There will be a variety of different networks will always be around, for the following reasons.

1) Different networks will use different technologies like personal computers run TCP/IP, mainframes run on IBM's SNA.

2) As computers and networks get cheaper, the place where decisions get made moves downwards in organizations.

3) As new hardware developments occur, new software will be created to fit the new hardware.

The purpose of interconnecting all these networks is to allow users on any of them to communicate with users don all the other ones to allow users on any of them to access data on any of them.

Networks differ in many ways. In the network layer the following differences can occur (fig.5.43).

Computer Networks

How networks can be connected:

Networks can inter connected by different devices. In the physical layer networks are connected by repeaters or hubs, which just move the bits from one network to an identical network.

At the Data Link layer bridges and switches are used. In network layer, routers are used to connect two network layers, the router may be able to translate between the packet formats. A router that can handle multiple protocols is called a ' multi protocol' router.

In a switched network the entire frame is transported on the basis of its MAC address. With router, the packet is extracted from the frame and the address in the packet is used for deciding where to send it. Switches do not have to understand the network layer protocol used to switch packets. Routers do.

Two ways of internetworking is possible.(i) a connection-oriented concatenated virtual subnets and (ii) datagram internet. In the past most networks were connection oriented. Then with the rapid acceptance of the Internet, datagrams became more popular. With growing importance of multimedia networking, it is likely that connection-orientation is back in one form or another since it is easier to guarantee quality of service with connections than without them.

In the concatenated virtual-circuit model a sequence of virtual circuit is set up from the source through one or more gateways to the destination. Each gateway maintains tables telling which virtual circuit pass through it, where they are to be routed, and what the new virtual –circuit number.

In datagrams from one host to other host the packets will be routed in different routes through the inter network. A routing decision is made separately for each packet, possibly depending on the traffic at the moment the packet is sent. This strategy can use multiple routes and thus achieve a higher bandwidth than the concatenated virtual circuit model.

Tunneling

The source and destination hosts are on the same type of network but there is a different network in between 'Tunneling' will be used. An ex, think of an organization with TCP/IP based Ethernet at one place and a TCP/IP base Ethernet in otherplace, and a PTT WAN in between as shown in fig. Consider an example a person driving his car from one place to other under its own power. Let in between he has to cross a river, which has no bridge. Hence his car has to be kept on a boat and transported to other end. From there the car continues to move under its own power. Tunneling of packets through a foreign network works the same way.

To send an IP packet to host 2, host 1, constructs the packet containing IP address of host 2, inserts it into an Ethernet frame addressed to the multi protocol router, and puts it on the Ethernet. When the multiprotocol router gets the frame, it removes the IP packet, inserts it in the payload field of the WAN network layer packet, and addresses the latter to the WAN address of the other

Computer Networks

multi protocol router to the other. Only the multiprotocol router has to understand IP and WAN packets.

The IP Protocol

At the network layer, the Internet can be viewed as a collection of subnet-works or Autonomous systems that are connected together. The network layer protocol that used for Internet is Internet Protocol (IP). Its job is to provide a best-efforts way to transport datagrams from source to destination, without regard to whether or not these machines are on the same network or not these are other networks in between them.

Communication in the Internet works as follows. Each datagram is transmitted, after getting from Transport layer, through the Internet, possibly being fragmented into smaller units as it goes. When all pieces finally get to the destination machine, they are reassembled by the network layer into the original datagram.

Internetwork protocol

At the network layer, TCP/IP supports the internetwork protocol .IP, in turn, contains four supporting protocols:ARP ,RARP ,ICMP,and IGMP.

IP is the transmission mechanism used by the TCP/IP protocols. It is an un –reliable and connectionless datagram protocol – a best effort delivery service. This is like a post office service. The post office does its best to deliver the mail but does not always succeed. If an unregistered letter is lost. it is up to the sender or would recipient to discover the loss and rectify the problem. The post office itself does not keep track of every letter and cannot notify a sender of loss or damage. An example of a situation similar to pairing IP with a protocol that contains reliability functions is a self addressed ,stamped postcard included in a letter mailed through the post office. when the letter is delivered , the receiver mails the postcard back to the sender to indicate success. If the sender never receives the postcard, he or she assumes the letter was lost and sends out another copy.

 IP transports data in packets called Datagrams,each of which is transported separately. Datagrams may travel along different routes and may arrive out of sequence or duplicated. IP does not create virtual circuits for delivery.

Datagram

Packets in IP layer are called Datagrams. A Datagram is a variable length packet(upto 65,536 bytes) consisting of two parts : Header and Data. The header can be from 20 to 60 bytes and contains information essential to routing and delivery.

Computer Networks

Version   The first field defines the version number of the IP. The current version is 4(IPv4),with binary value 0100.

Header length (HLEN)   The HLEN field defines the length of the header in multiples of four bytes .The four bits can represent a number between 0 to 15,which,when multiplied by 4,gives a maximum of 60 bytes.

Service Type.   The service type field defines how datagram should be handled. It includes bits that define the priority of the datagram. It also contains bits that specify the type of service the sender desires such as the level of throughput, reliability, and delay.

Total Length The total length field defines the total length of the IP datagram. It is a two-byte field (16 bits) and can define up to 65,535 bytes.

Identification The identification field is used in fragmentation. A datagram, when passing through different networks, may be divided into fragments to match the network frame size. When this happens, each fragment is identified with a sequence number in this field.

Flags The bits in the flags field deal with fragmentation (the datagram can or can not be fragmented; can be first, middle, or last fragment; etc.).

Fragmentation offset The fragmentation offset is a pointer that shows the offset of the data in the original datagram (if it is fragmented).

Time to live The time to live field defines the number of hops a datagram can travel before it is discarded. The source host, when it creates the datagram, sets this field to an initial value. Then, as the datagram travels through the Internet, router by router, each router decrements this value by 1. If this value becomes 0 before the datagram reaches its final destination, the datagram is discarded. This prevents a datagram from going back and forth forever between routers.

Protocol The protocol field defines which upper-layer protocol data are encapsulated in datagram (TCP, UDP, ICMP etc.).

Header Checksum This is a 16-bit field used to check the integrity of the header, not the rest of the packet.

Source address The source address field is a four-byte (32-bit) Internet address. It identifies the original source of the datagram.

Destination address The destination address field is a four-byte (32-bit) Internet address. It identifies the final destination of the datagram.

Options The options field gives more functionality to IP datagram. It can carry fields that control routing, timing, management, and alignment.

ADDRESSING

In addition to the physical address the internet requires an additional addressing convention : an address that identifies the connection of a host to its network.

Computer Networks

Each Internet address consists of 4 bytes defining three fields : class type,netid,and hosted. These parts are varying lengths depending on the class of the address.

CLASSES

There are currently five different classes:

They are Class A, Class B**,** Class C, Class D, Class E

Class A   :

This can accommodate more hosts since 3 bytes are reserved for HOSTID. Class A will begin with 0 .

Class B :

This will start with **10** and Host id will have 2 bytes length.

Class C :

This will start with 110 **and** Hostid will have 1 byte length.

Class   D:

 This will start with **1110 .** This is reserved for **Multicast addresses.**

Class E :

 This is reserved for feature use and will start with **1111 .**

 Ex. for classes

   1.   01111011 10001111 11111100 11001111

                          The address is starting with 0 .Hence it is Class A.

   2.   10011101 1000111111   11111100   11001111

                         The address is starting with 10 .Hence it is Class B.

Computer Networks

3.   11011101   10001111   11111100   11001111

The address is starting with 110 .Hence it is Class C

4.   11101011   10001111   11111100   11001111

The address is starting with 1110 .Hence it is Class D.

5.   11110101   10001111   11111100   11001111

The address is starting with 1111. Hence it is Class **E.**

CLASS   A :

Byte1	Byte 2	Byte3	Byte 4
0 Netid	Hostid		

CLASS B:

Byte1	Byte 2	Byte3	Byte 4
10 Netid		Hostid	

Class C :

Byte1	Byte 2	Byte3	Byte 4
110 Netid			Hostid

Class D :

Byte1	Byte 2	Byte3	Byte 4
11110 Multicast address			

Class E :

Byte1	Byte 2	Byte3	Byte 4
1111 Reserved for future use			

Computer Networks

Dotted-Decimal Notation:

To make 32 bit form shorter and easier to read, Internet addresses are usually written in decimal form with decimal points separating the bytes – dotted – decimal notation.

```
10000000    00001011    00000011    00011111



              128.11.3.31
```
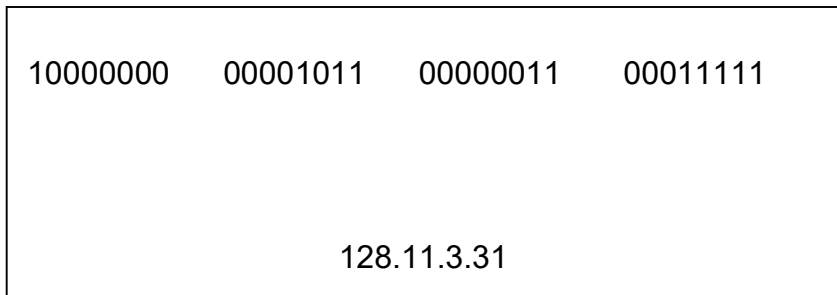
IP addresses in decimal notation

Class ranges of Internet address

From	To	
0.0.0.0	127.255.255.2555	← Class A

From	To	
128.0.0.0	191.255.255.255	← Class B

From	To	
192.0.0.0	223.255.255.255	← Class C

From	To	
224.0.0.0	239.255.255.255	← Class D

From	To	
240.0.0.0	255.255.255.2555	← Class E

Computer Networks
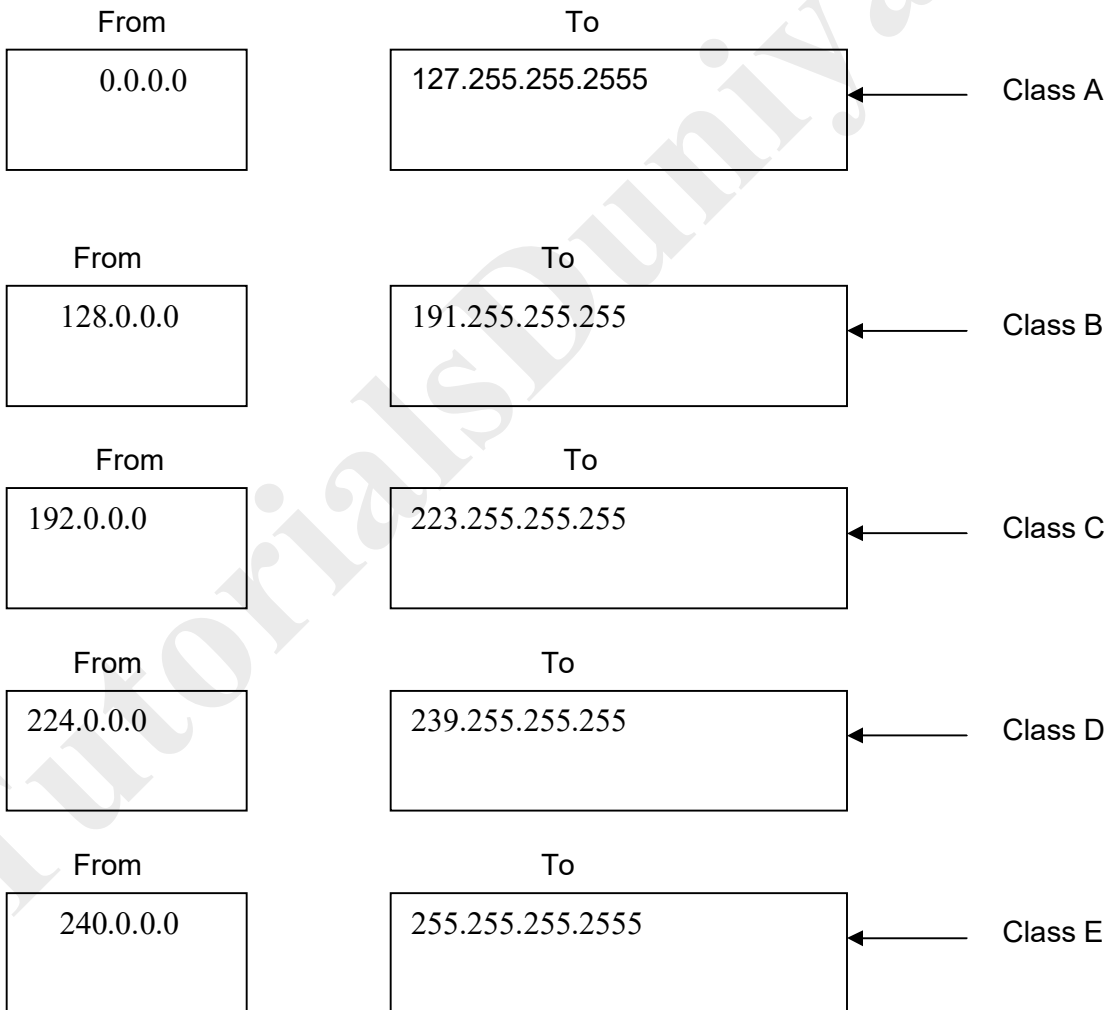
Example:

Find the class of each address

    a. 4.23.145.90
    b. 227.34.78.7
    c. 246.7.3.8
    d. 129.6.8.4
    e. 198.76.9.23

The first byte defines the class.
    a. The binary equivalent for 4 is 0000 0100. Since the first bit is 0 ,it is CLASS A.
    b. The binary equivalent for 227 is 11100011 . Since it is starting with 111 ,it is CLASS D.
    c. The binary equivalent for 246 is 11110110 . Since it is starting with 111 ,it is CLASS E.
    d. The binary equivalent for 129 is 10000001 . Since it is starting with 10,it is CLASS B.
    e. The binary equivalent for 198 is 11000110 . Since it is starting with 110 , it is CLASS C.

Example:

Find the netid and hosted for each address :

    a. 4.23.145.90
    b. 227.34.78.7
    c. 246.7.3.8
    d. 129.6.8.4
    e. 198.76.9.23

First find the class and then netid and hosted.

    a. Class A , netid :4 , hosted : 23.145.90

    b. Class D , no netid or hosted;

    c. Class E , no netid , or hosted;

    d. Class B , netid :129.6 ,hosted :8.4 ;

    e. Class C netid : 198.76.9 hostid 23 ;

TCP/IP supports four other protocols in the network layer :**ARP,RARP,ICMP,and IGMP.**

Computer Networks

Address resolution protocol (ARP)

The address resolution Protocol associates an ip address with physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address usually imprinted on the network interface card.(NIC)

Physical address have local jurisdiction and can be changed easily. For example, if the NIC on a particular machine fails, the physical address changes. The IP address, on the other hand ,have universal jurisdiction and cannot be changed. ARP is used to find the physical address of the node when its Internet address is known.

Anytime a host or a router needs to find the physical address of another host on its network, it formats an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes its internet address and sends back its physical address. The host both to its cache memory and to the datagram header, then sends the datagram on its way.

Reverse Address resolution protocol(RARP)

The RARP allows a host to discover its internet address when it knows only its physical address. The question here is ,why do we need RARP? A host is supposed to have its internet address stored on its hard disk !

RARP works much like ARP. The host wishing to retrieve its internet address broadcasts an RARP query packet that contains its physical address to every host on its physical network. A server on the network recognizes the RARP packet and returns the host's internet address.

Internet Control Message Protocol (ICMP)

The Internet control message protocol is a mechanism used by hosts and routers to send notification of datagram problems back to the sender.

IP is an unreliable and connectionless protocol. ICMP allows IP to inform a sender if a datagram is undeliverable. A datagram travels from router to router until it reaches one that can deliver it to its final destination. If a router is unable to route or deliver the datagram because of unusual conditions or due to congestion, ICMP allows it to inform the original source.

ICMP uses echo test/reply to test whether a destination is reachable and responding. It also handles both control and error message, but its sole function is ti\o report problems, not correction them. A datagram carries only source and destination address. For this reason ICMP can send message only to the source, not to an intermediate router.

Internet Group Message Protocol (IGMP)

Computer Networks

Ip addressing supports multicasting. All 32-bit IP addresses that start with 1110(class D) are multicast addresses. With 28 bits remaining for the group address, more than 250 million addresses are available for assignment. Some of these addresses are permanently assigned.

The IGMP has been designed to help a multicast router identify the hosts in a lan that are members of a multicast group. It is a companion to the IP protocol.

Expected questions

1.What is the difference between the adaptive and non-adaptive routing algorithms.

2.Explain the shortest path routing algorithm.

3.Explain the services that are provided by the network layer.

4.Explain Flooding routing algorithm.

5.Explain the Distance Vector Routing algorithm.

6.What is the count – to – infinity problem?

7.Explain link state routing algorithm.

8.Explain the Hierarchical Routing algorithm.

9.Explain Broadcast Routing and Multicast Routing.

10.What is congestion? Give the general principles of congestion control?

11.Explain Open loop and Close loop solutions for congestion.

12.How traffic shaping will be done to control congestion?

13.Explain The Leaky Bucket algorithm.

14. Explain the Token Bucket algorithm.

15.How the congestion can be controlled in Virtual Circuits?

16.What is a Choke packet? Explain when a choke packet is used.

17.Expalin the IP protocol.

18What is meant by Load shedding and Jitter control?

19. Explain the ICMP and ARP.

20.Explain the different IP address formats. For a hierarchical routing with 4800 routers, what region and cluster sizes should be chosen to minimize the size of routing table for a three-layer hierarchy?

*   *   *   *   *

Computer Networks

Review Questions

2. How is a repeater different from an amplifier?

3. What is the difference between a simple bridge and transparent bridge?

4. What is the function of router?

5. How does a router differ from a bridge?

6. Why is adaptive routing is superior to non-adaptive routing?

7. What is the function of a gateway?

8. How does a multiprotocol router differ from a traditional single – protocol router?

1. HDLC is the acronym for--------

   a. High-duplex line communication. b.high level data link control c.half-duplex digital link combination d. none of the above

2. HDLC is a ------ protocol

   a. Character-oriented b.bit-oriented c.byte – oriented d. count-oriented

3. The HDLC ----field defines the beginning and of a frame

   a. Flag bladders c. control d. FCS

4. Polling and selecting are functions of the ----in HDLC protocol

   a. P/F bit b.N(R) c.N (S) d.code bits

5. Which of the following is not an internetworking device?

   a. bridge b. gateway c. router d. all of them

6. Which of following uses the greatest number of layers in the OSI model?

   a. bridge b. gateway c. router d .repeater

7. A simple bridge does the following

   a. filters a data packet   b. forwards a data packet   c. extends Lans
   d. all the   above

8. The shortest path in routing can refer to --------

   a. the least expensive path b the latest distant path

   b. the path with the smallest number of hops d. any or combination of the above

9 In distance vector routing ,each router receives vectors from----

   a. every router in the network b. every router less than two units away

   b. a table stored by the software d. its neighbor only.

10. If there are five routers and six networks in an internet work using link state routing, how many routing tables are there?

   a. 1 b. 5 c. 6 d. 11

11. If there are five routers and six networks in an internet work using link state routing, how many data bases are there?

Computer Networks

a. 1 b. 5 c. 6   d. 1

12. Gateways function in which OSI layers?

a.the lower three b. the upper four c. all seven d. all but the physical layer

13. Repeaters function in the --- layer

a. physical b . datalink c. net work d. a and b

14.Bridges function in the -------- layer(s)

a. physical b . datalink c. net work d. a and b

Quiz Questions

1. What are the functions of Network Layer?

2. Give two differences between Adaptive and Nonadaptive routing algorithm.

3. In Shortest path routing algorithm what is the first step?

4. How the labels are measured in the above algorithm?

5. What is flooding algorithm?

6. What is meant by selective   flooding?

7. What is the disadvantage with flooding algorithm?

8. Give one method to overcome the disadvantage with flooding?

9. When the flooding algorithm will be used?

10. When we will go for hierarchical routing?

11. How the hierarchy is divided?

12. In distance vector routing, what will be the contents of table?

13. In the hierarchical routing for a N router subnet the optimal no. of   routers is _____.

14. The total no. of entries / routers = _____.

15. Give two examples of broadcast routing.

16.Give two methods of broadcast routing.

17. What is congestion?

18. Name the two congestion control algorithm.

19.What is the difference between a physical address and a logical address?

20.What are the advantages of using UDP over TCP?

21. What are the data packet at each TCP/IP protocol suite layer called?

22. Name the protocols at the network layer of the TCP/IP protocol suite.

23.What is the purpose of the time to live field in the datagram header?

24. Given an IP address in decimal – dotted notation, how can its class be determined?

25. How can a device have more than one IP address?

Computer Networks

26. What is a Hostid ?

27. What is a Netid?

28. How does a netid differ from a network address?

29. What is the purpose of subnetting?

30. What is the purpose of ARP?

31. What is the purpose of RARP?

32. What is the purpose of ICMP?

33. What is the purpose of IGMP?

34. What is the diffrence between a logical address and port address?

35. Change the following IP address from dotted-decimal notation to binary notation

  114.34.2.8

36. Change the following IP address from dotted-decimal notation to binary notation

  208.34.54.12

37. Change the following binary notation Ip address from binary notation to dotted-decimal notation .

               01111111 11110000   01100111 01111101

Multiple choice Questions

1.Which OSI layer corresponds to the TCP-UDP layer?

a. physical b. data link c.network d. transport

2.Which OSI layer corresponds to the IP layer?

a. physical b. data link c.network d. transport

3. Which OSI layer(S) corresponds to the TCP/IP application layer?

a. application b. session c. presentation d.all of the above

4.Which IP address class has few hosts per network?

   a. A b.B c.C d. D

5.For what does the data link layer look for as it sends a frame from one link to another?

   a. hosted b.Ip address c. domain name d.station address

6.The purpose of ARP on a network is to find the ------- given the ---------

   a. Intenet address, domain name

   b. Intenet address , station address

   c. Intenet address ,netid

   d. station address ,Intenet address

7.Which of the following apply to UDP?

   a. is unreliable and connectionless

   b. contains destination and source port address

   c. reports certain errors

Computer Networks

d. all the above

8.Which of the following applies to both UDP and TCP?

a. transport layer protocols

b. port – to –port communication

c. services of IP layer used

e. all the above

9.Which of the following is a class A host address?

a. 128.4.5.6

b. 117.4.5.1

c. 117.0.0.0

d. 117.8.0.0

10.which of the following is a lass b host address?

a.233.0.0.0

b.130.4.5.6

c.230.0.0.0

d.30.4.5.6

11.Which of the following is a class C host address?

a.230.0.0.0

b. 130.4.5.6

c.230.0.0.0

d.30.4.5.6

12.The data unit in the TCP/IP data link layer is called a ------

a.message

b.segment

c.datagram

d.frame

13. The data unit in the TCP/IP layer is called a ------

a.message

b.segment

c.datagram

d.frame

14. The data unit from the transport layer that uses UDP is called a -----

a. user datagram

b. message

c. segment

d. frame

Computer Networks

15.when a host knows its physical address but not its IP address,it can use-----

a.ICMP b.IGMP c. ARP d. RARP

16.This transport layer protocol is connectionless.

a.UDP b.TCP c. FTP d.NVT

17. This transport layer protocol requires acknowledgement.

a. UDP b.TCP c. FTP d.NVT

18.Which of the following is default mask for the address 98.0.46.201?

a.255.0.0.0

b.255.255.0.0

c.255.255.255.0

d.255.255.255.255

19. Which of the following is default mask for the address 98.0.46.201

a.255.0.0.0

b.255.255.0.0

c.255.255.255.0

d.255.255.255.255

20. Which of the following is default mask for the address 190.0.46.201?

a.255.0.0.0

b.255.255.0.0

c.255.255.255.0

d.255.255.255.255

21.Change the following IP address from dotted-decimal notation to binary notation

a. 114.34.2.8 b.129.14.6.8 c.208.34.54.12 d.238.34.2.1 e. 241.34.2.8

22.Find the class of the following IP address

a.208.34.54.12 b.238.34.2.1 c. 129.14.6.8 d.241.34.2.8

23.Find the netid and hosted for the following IP address.

a.114.34.2.8 b.19.34.21.5 c. 23.67.12.1 d. 126.23.4.0

24. Find the netid and hosted for the following IP address.

a.129.14.6.8 b.132.56.8.6 c.23.67.12.1 d.190.12.67.9

Computer Networks

25. Find the netid and hosted for the following IP address.

     a.   192.8.56.2 b. 220.34.8.9 c.208.34.54.12 d. 205.23.67.8

26.Find the network address of the following IP addresses.

     a. 114.34.2.8 b. 171.34.14.8 c. 192.8.56.2 d.226.7.34.5

      f.226.7.34.5 f. 225.23.6.7 g. 245.34.21.5

27.Write the following masks in binary notation:

     a.255 .255.255.0 b.255.255.224.0 c.255.255.255.240

28. Find the subnet work address for the following

     IP address : 125.34.12.56   Mask 255.255.0.0

29. Find the subnet work address for the following:

     IP address : 120.14.22.16   Mask : 255.255.128.0

30. Find the subnet work address for the following:

     Ip address 140.11.36.22   Mask : 255.255.255.0

* * * * *

Computer Networks

UNIT – IV
TRANSPORT LAYER

Introduction

The transport layer is the core of the OSI model. Protocols at this layer oversee the delivery of data from an application program on one device to an application program on another device. They act as a liaison between the upper-layer protocols (session, presentation, and application) and the services provided by the lower layers.

Duties of the transport layer:

The services provided are similar to those of the data link layer. The data link layer, however, is designed to provide its services within a single network, while the transport layer provides these services across an internetwork made of many networks. While the transport layer controls all three of the lower layers.

The services provided by transport layer protocols can be divided into five broad categories: end-to-end deliver, addressing, reliable delivery, flow control, and multiplexing.

Quality of Service

The transport protocol improves the QoS (Quality of Service) provided by the network layer. Following are the QoS parameters:

Connection establishment delay:

The connection establishment delay is the amount of time elapsing between a transport connection being requested and the confirmation being received by the user of the transport service. It includes the processing delay in the remote transport entity. As with all parameters measuring a delay, the shorter the delay, the better the service.

Connection establishment failure probability:

The connection establishment failure probability is the chance of a connection not being established within the maximum establishment delay time, for example, due to network congestion, lack of table space somewhere, or other internal problems.

Throughput:

The throughput parameter measures the number of bytes of user data transferred per second, measured over some time interval. The throughput is measured separately for each direction.

Transit delay:

The transit delay measures the time between a message being sent by the transport user on the source machine and its being received by the transport user on the destination machine. As with throughput, each direction is handled separately.

The Residual error ratio :

Measures the number of lost or garbled messages as a fraction of the total sent. In theory, the residual error rate should be zero, since it is the job of the transport layer to hide all network layer errors. In practice it may have some (small) finite value.

The Protection parameter provides a way for the transport user to specify interest in having the transport layer provide protection against unauthorized third parties (wiretappers) reading or modifying the transmitted data.

The Priority parameter provides a way for a transport user to indicate that some of its connections are more important than other ones, and in the event of congestion, to make sure that the high-priority connections get serviced before the low-priority ones.

Finally, the Resilience parameter gives the probability of the transport layer itself spontaneously terminating a connection due to internal problems or congestion.

Computer Networks

The QoS parameters are specified by the transport user when a connection is requested. Both the desired and minimum acceptable values can be given. In some cases, upon seeing the QoS parameters, the transport layer may immediately realize that some of them are unachievable, in which case it tells the caller that the connection attempt failed, without even bothering to contact the destination. The failure report specifies the reason for the failure.

The transport layer knows it cannot achieve the desired goal (e.g.600 Mbps throughput), but it can achieve a lower, but still acceptable rate (e.g.150 Mbps). It then sends the lower rate and the minimum acceptable rate to the remote machine, asking to establish a connection. If the remote machine cannot handle the proposed value, but it can handle a value above the minimum, it may make a counteroffer. If it cannot handle any value above the minimum, it rejects the connection attempt. Finally, the originating transport user is informed of whether the connection was established or rejected, and if it was established, the values of the parameters agreed upon. This process is called **option negotiation**.
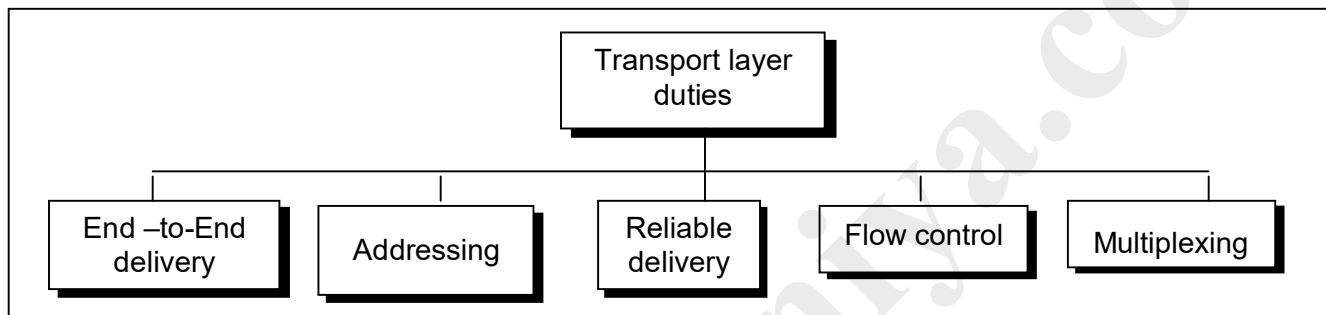
End –to –end delivery

The network layer oversees the end-to-end delivery of individual packets but does not see any relationship between those packets, even those belonging to a single message.

It treats each as an independent entity. The transport layer, on the other hand, makes sure that the entire message (not just a single packet) arrives intact. Thus, it oversees the end-to-end (source –to-destination) delivery of an entire message.

Addressing

The transport layer interacts with the functions of the session layer. However, many protocols (or protocol stacks, meaning groups of protocols that interact at different levels) combine session, presentation, and application level protocols into a single packages, called an application. In these cases, delivery to the session layer functions is, in effect, delivery to the application. In these cases, delivery to the session layer functions is, in effect, delivery to the application. So communication occurs not just from end machine to end machine but from end application to end application. Data generated by an application on one machine must be received not just by the other machine but by the correct application on that other machine.

To ensure accurate delivery from service access point to service access point, we need another level of addressing in addition to those at the data link and network levels. Data link level protocols need to know which two computers within a network are communicating. Network level protocols need to know which two computers within an internet are communicating. But at the transport level, the protocol needs to know which upper-layer protocols are communicating.

Reliable Delivery

At the transport layer, reliable delivery has four aspects: error control, sequence control, loss control, and duplication control.

Computer Networks
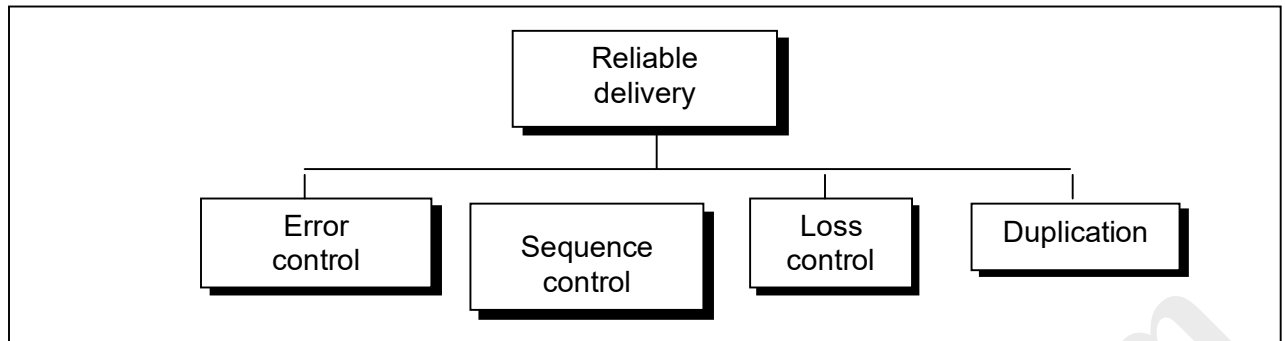
Error Control

When transferring data, the primary goal of reliability is error control.

But if we already have error handling at the data link layer, why do we need it at the transport layer? Data link layer functions guarantee error-free delivery node-to-node for each link. However, node-to-node reliability does not ensure end-to-end reliability.

Sequence Control

The second aspect of reliability implemented at the transport layer is sequence control. On the sending end, the transport layer is responsible for ensuring that data units received from the upper layers are usable by the lower layers. On the receiving end, it is responsible for ensuring that the various pieces of a transmission are correctly reassembled.

Segmentation and Concatenation

When the size of the data unit received from the upper layer is too long for the network layer datagram or data link layer frame to handle, the transport protocol divides it into smaller, usable blocks. The dividing process is called segmentation. When, on the other hand, the size of the data units belonging to a single session are so small that several can fit together into a single datagram or frame, the transport protocol combines them into a single data unit. The combing process is called concatenation.

Sequence Numbers

Most transport layer services add a sequence number at the end of each segment. If a longer data unit has been segmented, the numbers indicate the order for reassembly. If several shorter units have been concatenated, the numbers indicate the end of each submit and allow them to be separated accurately at the destination. In addition, each segment carries a field that indicates whether it is the final segment of a transmission or a middle segment with more still to come.

Loss Control

The third aspect of reliability covered by the transport layer is loss control. The transport layer ensures that all pieces of a transmission arrive at the destination, not just some of them. When data have been segmented for delivery, some segments may be lost in transit. Sequence numbers allow the receiver's transport layer protocol to identify any missing segments and request redelivery.

Duplication Control

The fourth aspect of reliability covered by the transport layer is duplication control. Transport layer functions must guarantee that no pieces of data arrive at the receiving system duplicated. Just as they allow identification of lost packets, sequence numbers allow the receiver to identify and discard duplicate segments.

Computer Networks

Flow Control

Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end-to-end rather than across a single link. Transport layer flow control also uses a sliding window protocol. However, the window at the transport layer can vary in size to accommodate buffer occupancy.

Multiplexing

To improve transmission efficiency, the transport layer has the option of multiplexing. Multiplexing at this layer occurs two ways: upward, meaning that multiple transport layer connections use the same network connection, or downward, meaning that one transport-layer connection uses multiple network connections.
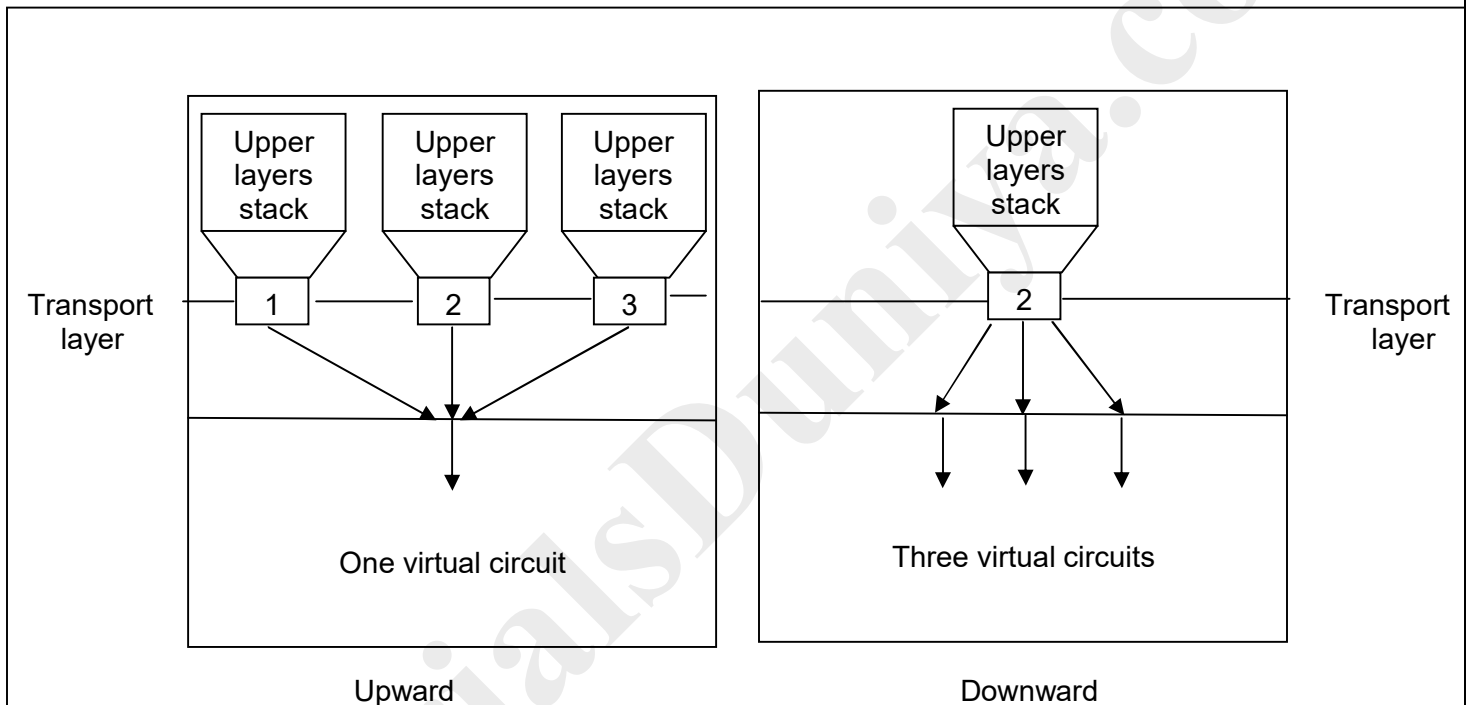
The transport layer uses virtual circuits based on the services of the lower three layers.

Normally, the underlying networks charge for each virtual circuit connection. To make more cost-effective use of an established circuit, the transport layer can send several transmissions bound for the same destination along the same path by upward multiplexing. This means if the underlying network protocol has a high throughput, for example in the range of 1 Gbps, and the user create data only in the range of Mbps, then several users can share one network connection.

Downward

Downward multiplexing allows the transport layer to split a single connection among several different paths to improve throughput (speed of delivery). This option is useful when the underlying networks have low or slow capacity. For example, some network layer protocols have restrictions on the sequence numbers that can be handled. X.25 uses a three-bit numbering code, so sequence numbers are restricted to the range of 0 to 7 (only eight packets may be sent before acknowledgment is required). In this case, throughput can be unacceptably low. To counteract this problem, the transport layer can opt to use more than one virtual circuit at the network layer to improve throughput. By sending several data segments at once, delivery is faster.
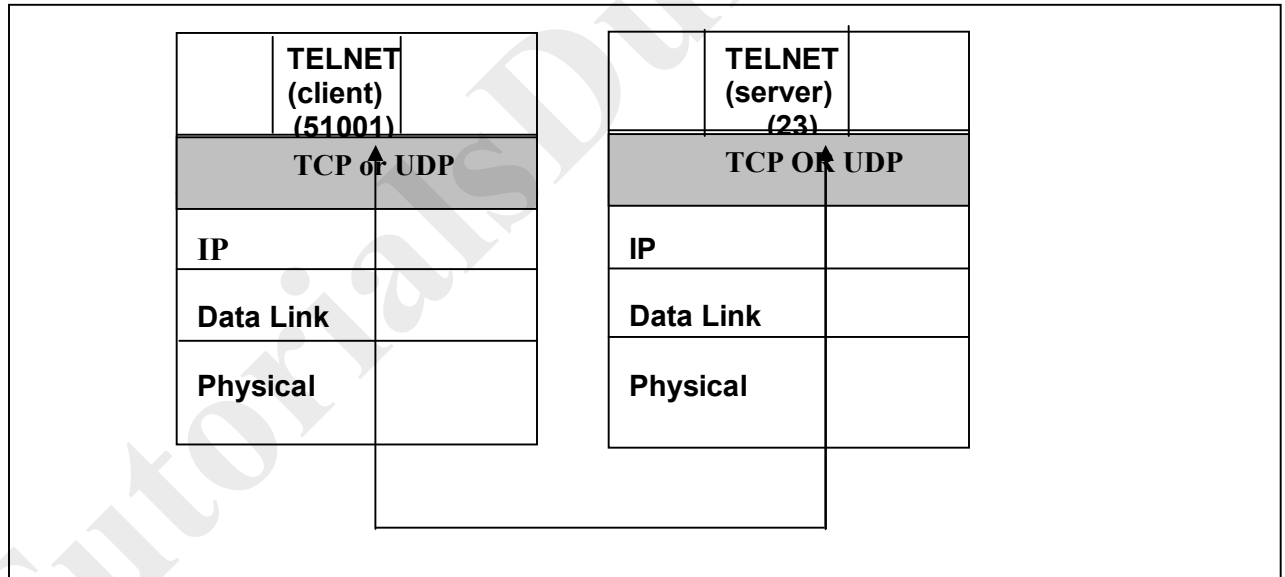
Computer Networks

TCP Protocol

ARPA established a packet-switching network of computers linked by point-to-point leased lines called Advanced Research Project Agency Network(ARPANET) that provided a basics for early research into networking. The conventions developed by ARPA to specify how individual computers could communicate across that network became TCP/IP.

The transport layer is represented in TCP/IP by two protocols:TCP and UDP. Of these, UDP is similar; it provides nonsequenced transport functionality when reliability and security are less important than size and speed.

The transport protocols of the TCP/IP suite define a set of conceptual connections to individual process called protocol ports or, more simply, ports. A protocol port is a destination point (usually a buffer) for storing data for use by a particular process.

The IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. TCP/IP's transport level protocols are port-to-port protocols that work on top of the IP protocols to deliver the packet from the originating port to the IP services at the start of a transmission, and from the IP services to the destination port at the start end.

Figure Port addresses

| TELNET (client) (51001)		TELNET (server) (23)	
TCP or UDP		TCP OR UDP	
IP		IP	
Data Link		Data Link	
Physical		Physical	

Each port is defined by a positive integer address carried in the header of a transport layer packet. An IP datagram uses the host's 32-bit Internet address. A frame at the transport level uses the process port address of 16 bits, enough to allow the support of up to 65,536(0 to 65535) ports.

USER DATAGRM PROTOCOL(UDP)

Computer Networks

The user datagram protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. It is an end-to-end transport level protocol that adds only port addresses, check sum error control, and length information to the data from the upper layer. The packet produced by the UDP is called a user datagram .

- **Source port address.** The source port address is the address of the application program that has created the message.
- **Destination port address.** The destination port address is the address of the application program that will receive the message.
- **Total length.** The total length field defines the total length of the user datagram in bytes.
- **Check sum.** The check sum is a 16-bit field used in error detection.

Figure UDP datagram format
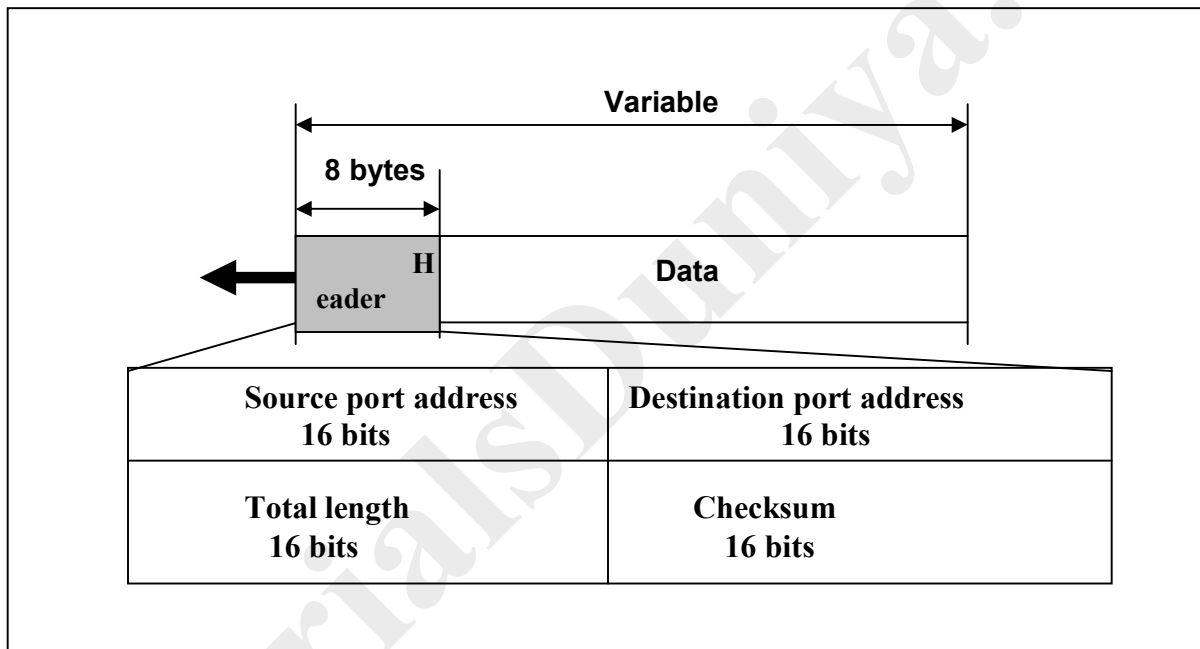
UDP provides only the basic functions needed for end-to-end delivery of a transmission. It does not provide any sequencing or recording functions and cannot specify the damaged packet when reporting an error (for which it must be paired with ICMP). UDP can discover that an error has occurred; ICMP can then inform the sender that a user datagram has been damaged and discarded. Neither, however, has the ability to specify which packet has been lost. UDP contains only a checksum; it does not contain an ID or sequencing number for a particular data segment.

Transmission Control Protocol(TCP)

Computer Networks

The Transmission Control Protocol (TCP) provides full transport layer services to applications. TCP is a reliable stream transport port-to-port protocol. The term stream, in this context, means connection-oriented: a connection must be established between both ends of a transmission before either may transmit data. By creating this connection, TCP generates a virtual circuit between sender and receiver that is active for the duration of a transmission.(connections for the duration of an entire exchange are different, and are handled by session functions in individual applications.) TCP begins each transmission by altering the receiver that datagrams are on their way (connection establishment) and ends each transmission with a connection termination. In this way, the receiver knows to expect the entire transmission rather than a single packet.
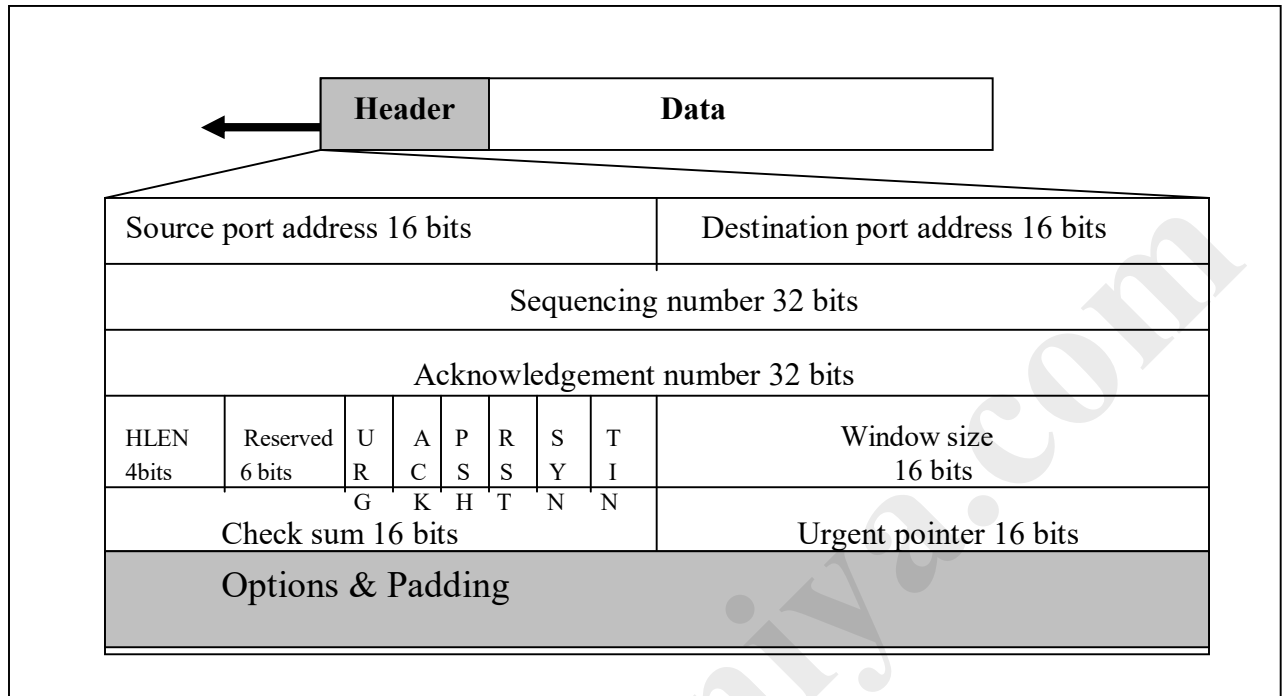
IP and UDP treat multiple datagrams belonging to a single transmission as entirely separate units, unrelated to each other. The arrival of each datagram at the destination is therefore a separate event, unexpected by the receiver. TCP, on the other hand, as a connection-oriented service, is responsible for the reliable delivery of the entire stream of bits contained in the message originally generated by the sending application. Reliability is ensured by provision for error detection and retransmission of damaged frames; all segments must be received and acknowledged before the transmission is considered complete and the virtual circuit is discarded.

At the sending end of each transmission, TCP divides long transmissions into smaller data units and packages each into a frame called a segment. Each segment includes a sequencing number for reordering after receipt, together with an acknowledgement ID number and a window-size field for sliding window ARQ. Segments are carried across network links inside of IP datagrams as it comes in and reorders the transmission based on sequence numbers.

The TCP Segment

The scope of the services provided by TCP requires that the segment header be extensive. A comparison of the TCP segment format with that of a UDP user datagram shows the differences between the two protocols. TCP provides a comprehensive range of reliability functions but sacrifices speed (connections must be established, acknowledgments waited for , etc.).Because of its smaller frame size, UDP is much faster than TCP, but at the expense of reliability. A brief description of each field is in order.

Computer Networks

Figure TCP Segment format

Header	Data

Source port address 16 bits							Destination port address 16 bits
Sequencing number 32 bits							
Acknowledgement number 32 bits							
HLEN 4bits	Reserved 6 bits	URG	ACK	PSH	RST	SYN	TIN	Window size 16 bits
Check sum 16 bits							Urgent pointer 16 bits
Options & Padding							

- **Source port address.** The source port address defines the application program in the source computer.
- **Destination port address.** The destination port address defines the application program in the destination computer.
- **Sequence number.** A stream of data from the application program may be divided into two or more TCP segments. The sequence number field shows the position of the data in the original data stream.
- **Acknowledgement number.** The 32-bit acknowledgement number is used to acknowledge the receipt of data from the other communicating device. This number is valid only if the ACK bit in the control field(explained later) is set. In this case, it defines the byte sequence number that is next expected.
- **Header Length (HLEN).** The four-bit HLEN field indicates the number of 32-bit (four-byte) words in the TCP header. The four bits can define a number up to 15.This is multiplied by 4 to give the total number of bytes in the header. Therefore, the size of the header can be a maximum of 60 bytes (4x15).Since the minimum required size of the header is 20 bytes, 40 bytes are thus available for the options section.
- **Reserved.** A six-bit field is reserved for future use.
- **Control.** Each bit of the six-bit control field functions individually and independently. A bit can either define the use of a segment or serve as a validity check for other fields. The

Computer Networks

urgent bit, when set, validates the urgent pointer field. Both this bit and the pointer indicate that the data in the segment are urgent. The ACK bit, when set, validates the acknowledgement number field. Both are used together and have different functions, depending on the segment type. The PSH bit is used to inform the sender that a higher throughput is needed. If possible, data must be pushed through paths with higher throughput. The reset bit is used to reset the connection when there is confusion in the sequence numbers. The SYN bit is used for sequence number synchronization in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement (with the ACK bit set). The FIN bit is used in connection termination in three types of segments: termination request, termination confirmation (with the ACK bit set), and acknowledgement of termination confirmation (with the ACK bit set).

- **Window size.** The window is a 16-bit field that defines the size of the sliding window.

- **Checksum.** The checksum is a 16-bit field used in error detection.

- **Urgent pointer.** This is the last required field in the header. Its value is valid only if the URG bit in the control field is set. In this case, the sender is informing the receiver that there are **urgent data** in the data portion of the segment. This pointer defines the end of urgent data and the start of normal data.

- **Options and padding.** The remainder of the TCP header defines the optional fields. They are used to convey additional information to the receiver or for alignment purposes.

Computer Networks

UNIT 5

Application Layer

Network Security

Security Attacks

Attacks on the security of a computer system or network are best characterized by viewing the function of the computer system as providing information.

There are four general categories of attack:

- **Interruption:** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, such as a hard disk, the cutting of a communication line, or the disabling of the file management system.

- **Interception:** An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program, or a computer. Examples include wiretapping to capture data in a network, and the illicit copying of files or programs.

- **Modification:** An unauthorized party not only gains access to but tampers with an asset. This is an attack or integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network.

- **Fabrication:** An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. Examples include the insertion of spurious messages in a network or the addition of records to a file.

Computer Networks

(a) Normal flow

(b) Interruption

(C) Interception

(d) Modification

(e) Fabrication
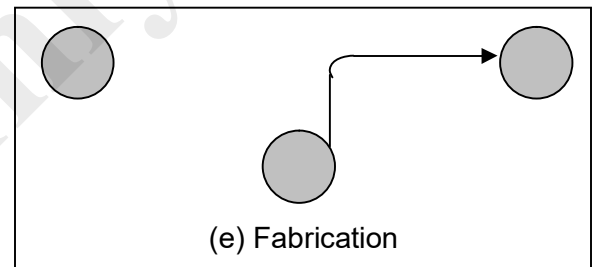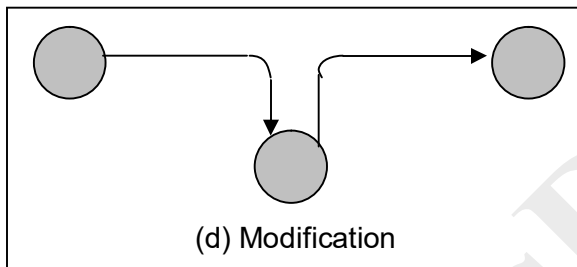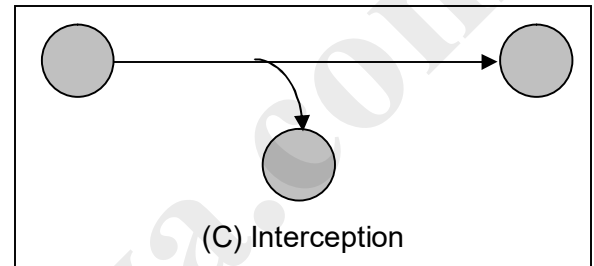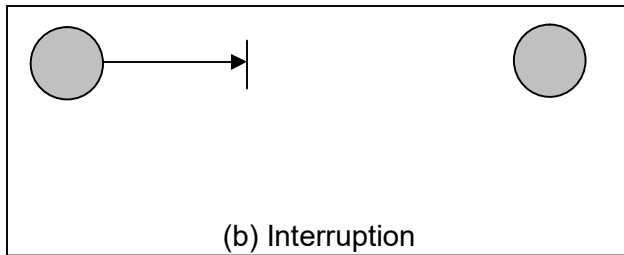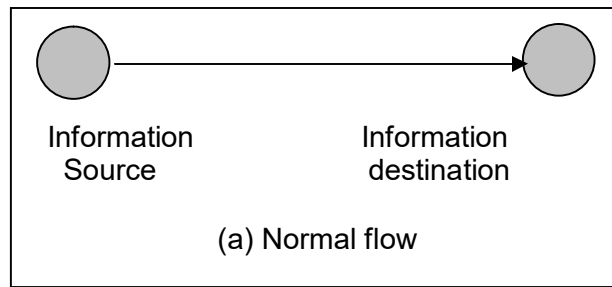
CONVENTIONAL ENCRYPTION MODEL

The original intelligible message, referred to as plaintext, is converted into apparently random nonsense, referred to as ciphertext. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext. The algorithm will produce a different output depending on the specific key being used at he time. Changing the key changes the output of the algorithm.

Once the ciphertext is produced, it may be transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

The security of conventional encryption depends on the secrecy of the key, not the secrecy of the algorithm. We do not need to keep the algorithm secret; we need to keep only the key secret. A source produces a message in plaintext, $X = [X_1, X_2, ……., X_M]$. For encryption, a key of the form $K = [K_1, K_2,……., K_J]$ is generated. If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination.

Computer Networks

With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext Y = [Y_1, Y_2,......, Y_N]. We can write this as

$$Y = E_K(X)$$

This notation indicates that Y is produced by using encryption algorithm E as a function of the plaintext X, with the specific function determined by the value of the key K.

The intended receiver, in possession of the key, is able to invert the transformation:

$$X = D_K(Y)$$

Substitution Techniques

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Caesar Cipher

The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,

plain : meet me after the toga party

cipher : PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

plain: a b c d e f g l j k l m n o p q r s t u v w x y z

cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

If we assign a numerical equivalent to each letter (a =1, b = 2, etc.), then the algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C:

$$C = E(p) = (p + 3) \bmod (26)$$

A shift may be of any amount, so that the general Caesar algorithm is

$$C = E(p) = (p + k) \bmod (26)$$

Where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$$P = D(c) = (C - k) \bmod (26)$$

Playfair Cipher

The bet-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

The Playfair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword. Here is an example, solved by Lord Peter Wimsey in Dorothy Sayers's Have His carcase.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

In this case, the keyword is monarchy. The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and then filling in the remainder of the matrix

Computer Networks

with the remaining letters in alphabetic order. The letters I and J count as one letter. Plaintext is encrypted two letters at a time, according to the following rules:
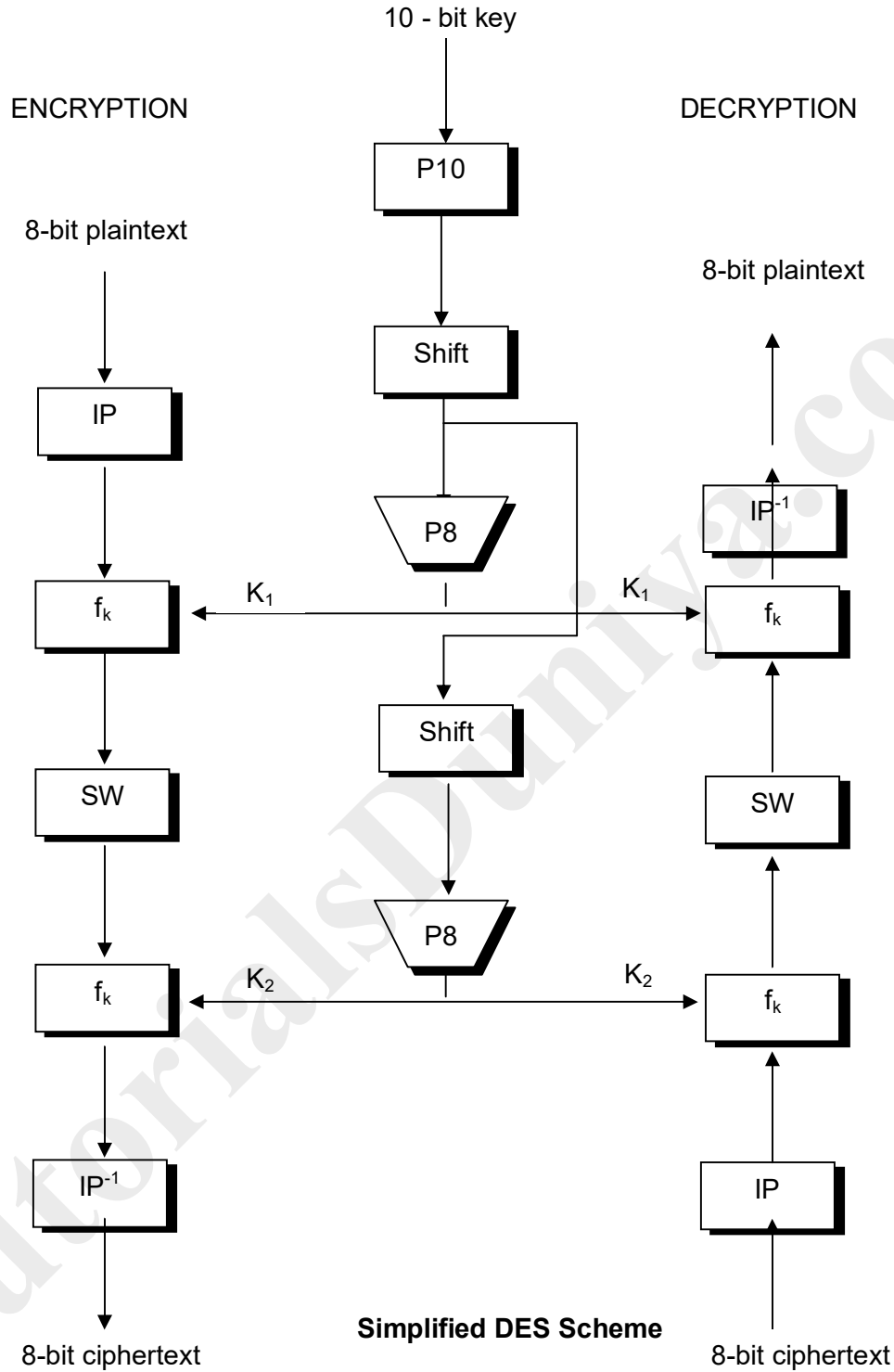
1. Repeating plaintext letters that would fall in the same pair are separated with a filler letter, such as x, so that balloon would be enciphered as ba lx lo on.

2. Plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the row circularly following the last. For example, mu is encrypted as CM.

3. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Simplified DES

The S-DES decryption algorithm takes an 8-bit block of plaintext (example: 10111101) and a 10-bit key as input and produces an 8-bit block of ciphertext as output. The S-DES decryption algorithm takes an 8-bit block of ciphertext and the same 10-bit key used to produce that ciphertext as input and produces the original 8-bit block of plaintext.

The encryption algorithm involves five functions: an initial permutation (IP); a complex function labeled f_k, which involves both permutation substitution operations and depends on a key input; a simple permutation function that switches (SW) the two halves of the data; the function f_k again, and finally a permutation function that is the inverse of the initial permutation (IP^{-1}).

The function f_k takes as input not only the data passing through the encryption algorithm, but also an 8-bit key. The algorithm could have been designed work with a 16-bit key, consisting of two 8-bit subkeys, one used for each occurrence of f_k. Alternatively, a single 8-bit key could have been used, with the same key used twice in the algorithm. A compromise is to use a 10-bit key from which two 8-bit subkeys are generated, as depicted in fig. In this case, the key is first subjected to a permutation (P10). Then a shift operation is performed. The output of the shift operation then passes through a permutation function that produces an 8-bit output (P8) for the first subkey (K_1). The output of the shift operation also feeds into another shift and another instance of P8 to produce the second subkey (K_2).

Computer Networks

10 - bit key

ENCRYPTION

DECRYPTION

P10

8-bit plaintext

8-bit plaintext

IP

Shift

IP^{-1}

f_k

P8

K_1

K_1

f_k

SW

Shift

SW

f_k

P8

K_2

K_2

f_k

IP^{-1}

IP

8-bit ciphertext

Simplified DES Scheme

8-bit ciphertext

Computer Networks

We can concisely express the encryption algorithm as a composition of functions:

$$IP^{-1} \circ f_{k2}) \; SW \;) f_{k1} \circ IP$$

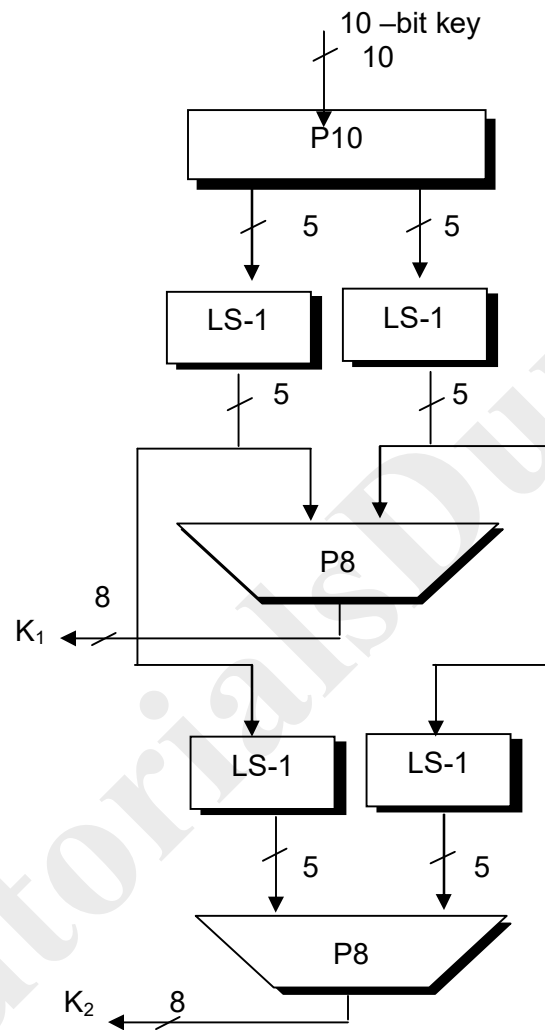Which can also be written as

$$ciphertext = IP^{-1}(f_k \,(\, SW \,(\, f_k \,(\, IP \,(\, plaintext \,)\,)\,)\,)\,)$$

Where

$$K_1 = P8 \,(Shift \,(P10 \,(key)\,)\,)$$

$$K_2 = P8 \,(Shift \,(Shift \,(P10 \,(key)\,)\,)\,)$$

Key Generation for Simplified DES

Computer Networks

Decryption is also shown in fig. and is essentially the reverse encryption:

$$\text{plaintext} = IP^{-1} (f_{k1} (SW (f_{k2} (IP (\text{ciphertext})))))$$

We now examine the elements of S-DES in more detail.

S-DES Key Generation

S-DES depends on the use of a 10-bit key shared between sender and receiver. From this key, two 8-bit subkeys are produced for use in particular stages of the encryption and decryption algorithm. Figure depicts the stages followed to produce the subkeys.

First, permute the key in the following fashion. Let the 10-bit key be designated as (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}). Then the permutation P10 is defined as P10 (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}) = (k_3, k_5, k_2, k_7, k_4, k_{10}, k_1, k_9, k_8, k_6)

P10 can be concisely defined by the display:

P10									
3	5	2	7	4	10	1	9	8	6

This table is read from left to right; each position in the table gives the identity of the input bit that produces the output bit in that position. So the first output bit is bit 3 of the input; the second output bit is bit 5 of the input, and so on. For example, the key (1010000010) is permuted to (1000001100). Next, perform a circular left shift (LS-1), or rotation, separately on the first five bits and the second five bits. In our example, the result is (00001 11000).

Next we apply P8, which picks out and permutes 8 of the 10 bits according to the following rule:

P8							
6	3	7	4	8	5	10	9

The result is subkey 1 (K_1). In our example, this yields (10100100).

We then go back to the pair of 5-bit strings produced by the two LS-1 functions and perform a circular left shift of 2 bit positions on each string. In our example, the value (00001 11000) becomes (00100 00011). Finally, P8 is applied again to produce K_2. In our example, the result is (01000011).

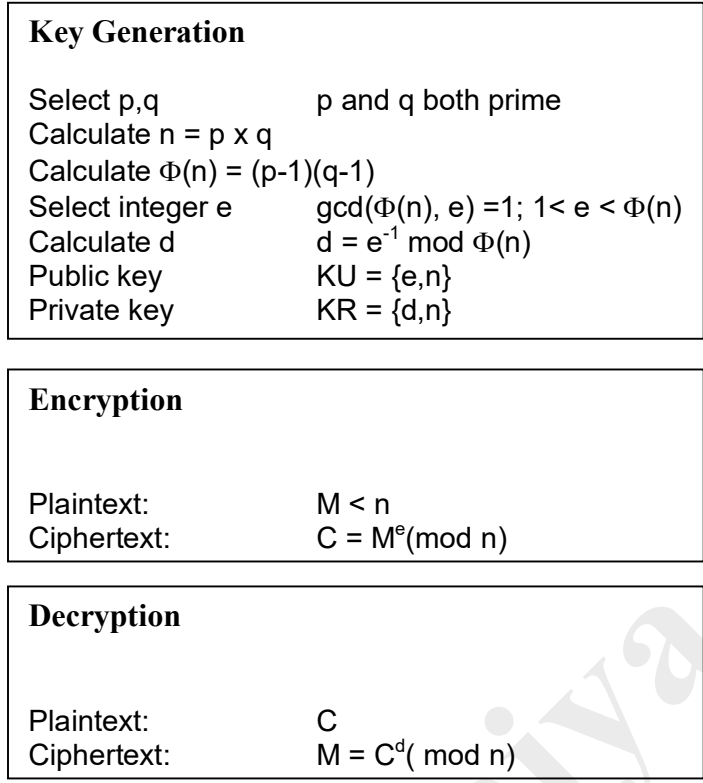### The RSA Algorithm
Description of the Algorithm
The scheme developed by Rivest, Shamir, and Adleman makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2(n)$; in practice, the block size is 2^k bits, where $2^k < n \leq 2^{k+1}$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C:

$$C = M^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of KU = {e, n} and a private key of KR = {d, n}. For this algorithm to be satisfactory for public – key encryption, the following requirements must be met:

1. It is possible to find values of e, d, n such that $M^{ed} = M \bmod n$ for all M < n.

2. It is relatively easy to calculate M^e and C^d for all values of M< n.

3. It is infeasible to determine d given e and n.

4.

Computer Networks

Key Generation

Select p,q	p and q both prime
Calculate n = p x q	
Calculate $\Phi(n) = (p-1)(q-1)$	
Select integer e	$gcd(\Phi(n), e) =1; 1< e < \Phi(n)$
Calculate d	$d = e^{-1} \bmod \Phi(n)$
Public key	KU = {e,n}
Private key	KR = {d,n}

Encryption

Plaintext:	M < n
Ciphertext:	$C = M^e (\bmod\ n)$

Decryption

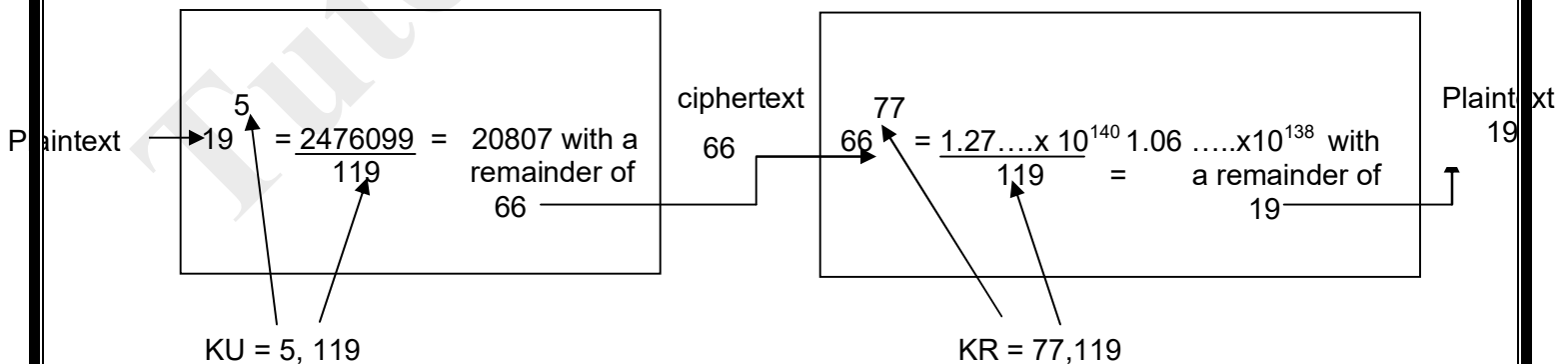|	
Plaintext:	C
Ciphertext:	$M = C^d (\bmod\ n)$

The RSA Algorithm   (a)

Fig (a) summarizes the RSA algorithm.

Example 1:

Select two prime numbers, p=7 and q = 17.

1. Calculate n = pq = 7 X 17 = 119

2. Calculate $\Phi(n) = (p-1)(q-1) = 96$

3. Select e such that e is relatively prime to $\Phi(n) = 96$ and less than $\Phi(n)$; in this case, e = 5.

4. Determine d such that de = 1 mod 96 and d < 96. The correct value is d = 77, because 77 X 5 = 385 = 4 X 96 +1.

The resulting keys are public key KU = {5,119} and private key KR = { 77,119}. The example shows the use of these keys for a plaintext input of M = 19. For

Plaintext $\rightarrow 19^5 = \dfrac{2476099}{119} = $ 20807 with a remainder of 66

ciphertext 66

$66^{77} = \dfrac{1.27....x\ 10^{140}}{119} = $ 1.06 .....$x10^{138}$ with a remainder of 19

Plaintext 19

KU = 5, 119

KR = 77,119

Example of RSA algorithm   (b)

Computer Networks

Encryption, 19 is raised to the fifth power, yielding 2476099. Upon division by 119, the remainder is determined to be 66. Hence $19^5 \equiv 66 \bmod 119$, and the ciphertext is 66. For decryption, it is determined that $66^{77} \equiv 19 \bmod 119$.

Example 2 :

p = 3, q = 11, d = 17

assume plaintext symbol M = 5

n = p*q = 33, z = = (3-1) (11 – 1) = 20

Find e such that e * d = 1 mod z (z+1)

$[d = e^{-1} \bmod z]$ k * z+1 (k =1 here)

e = 3   3 X 7 = 1 mod 20

public key = { e,n} = { 3, 33}

private key = { d, n} = { 7, 33}

Encryption M =5

C = M^e mod n

   = 5^e mod 33 = 125 /33 = 3

        with reminder 26

      ciphertext = 26

      decryption c = 26

      p =M = C^d mod n = 26^7 mod 33

       = 8031810176/33 = 243388187

                    with reminder 5

      plain text = 5

Example 3:

P = 17, q = 31, e = 7, m = 2

N = 17 X 31 = 527

z = (17-1) (31 – 1) = 16 x 30 = 480

e =7

Finding d such that e * d = 1 mod 480

and d < 480   = k * z + i

 e = 7

the value obtained is 343 1/7 x (480 x k +1)

publickey = { 7, 527} private key = { 343, 527 }

ciphertext = 2^7 mod 527
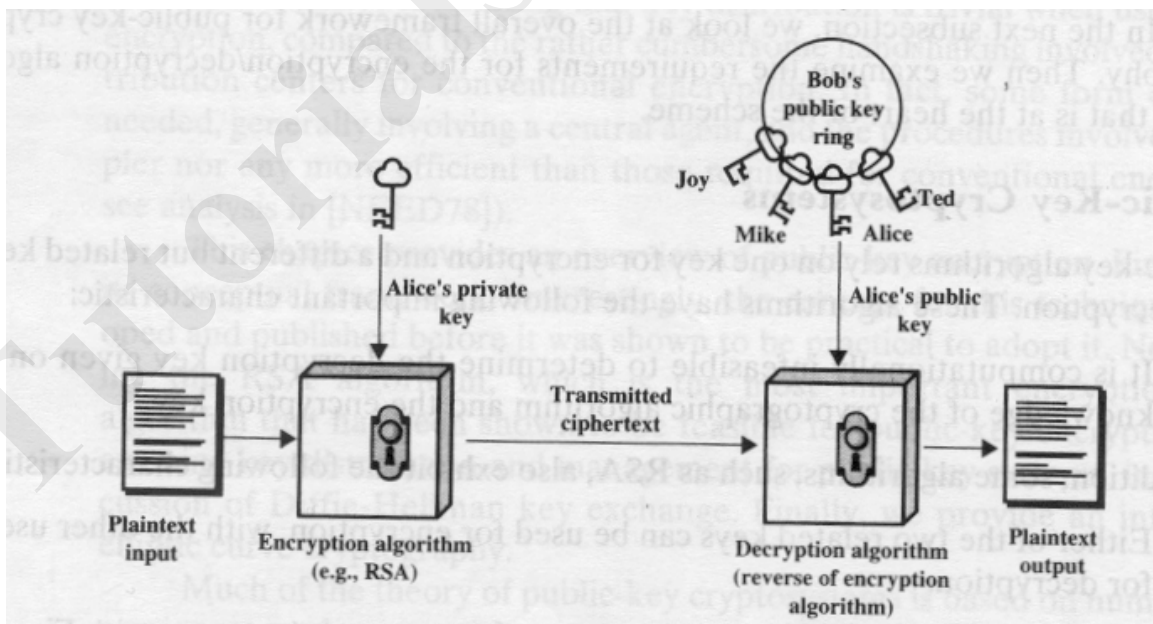
        = 128 mod 527 = 0

Computer Networks

∴ with reminder   = 128

    ciphertext   = 128

Decryption

$$128^{343} \bmod 527$$

2 is reminder

∴ plaintext = 2
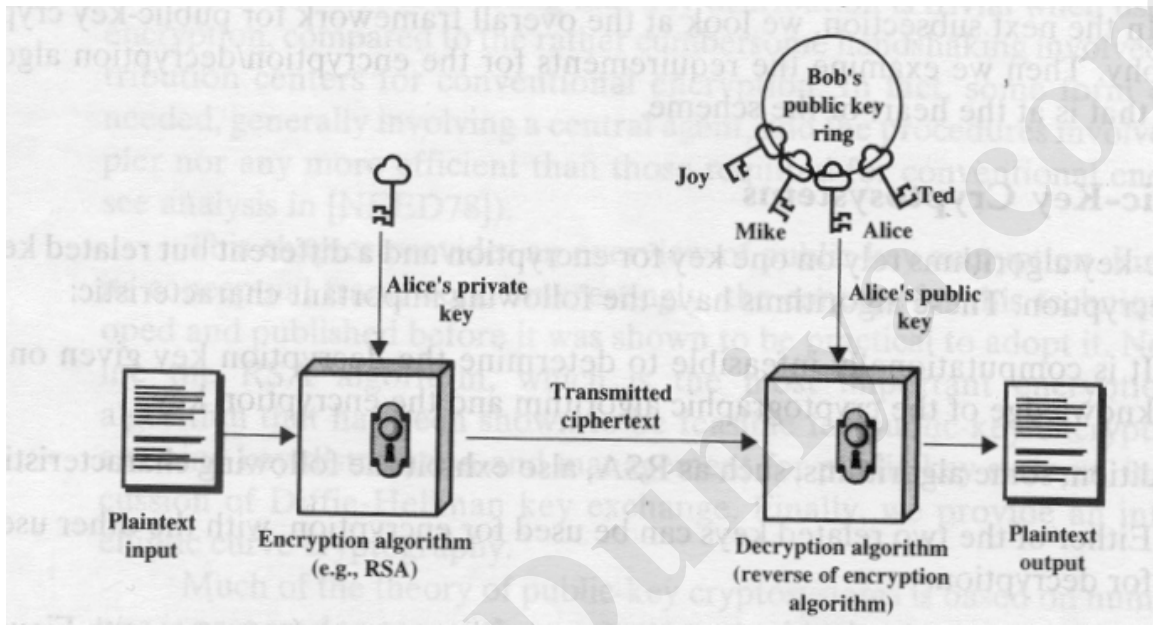
(a) Encryption

(b) Authentication

Computer Networks

Public – Key Encryption

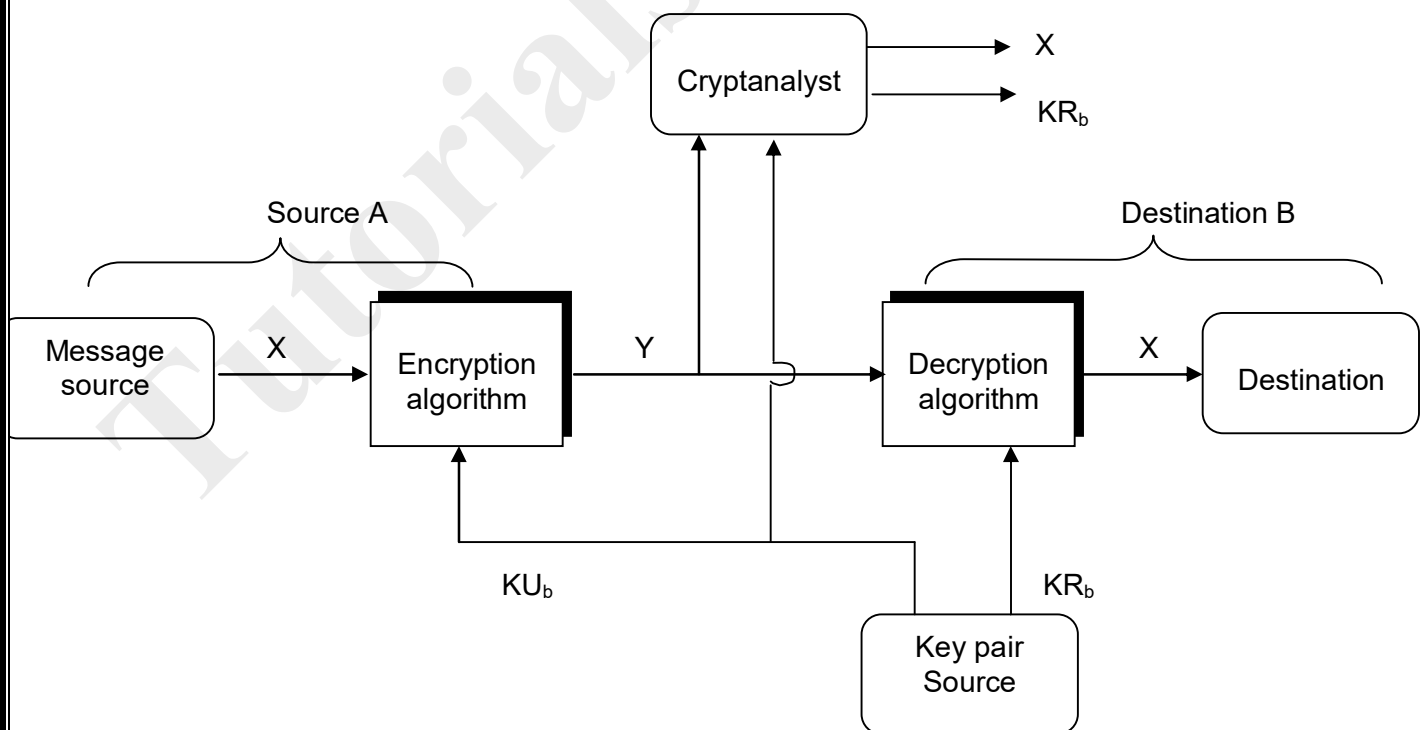| Conventional Encryption	Public-Key Encryption
Needed to work:	Needed to work:
1. The same algorithm with the same key is used for encryption and decryption.	1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
2. The sender and receiver must share the algorithm and the key.	2. The sender and receiver must each have one of the matched pair of keys (not the same one).
Need for Security:	Need for Security:
1.The key must be kept secret.	1. One of the two keys must be kept secret.
2.It must be impossible or at least impractical to decipher a message if no other information is available.	2. It must be impossible or at least impractical to decipher a message if no other information is available.
3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Cryptanalyst → X

→ KR_b

Source A

Destination B

Message source → X → Encryption algorithm → Y → Decryption algorithm → X → Destination

KU_b

KR_b

Key pair Source

Computer Networks

E-mail :

E-mail system consists of two subsystems

- the user agent, and
- the message transfer agents
- **User Agents :**

    They allow people to read and send e-mail they are local programs that provide a command based, menu based, or graphical method for interacting with e-mail system.
- **Message transfer agents :**

    They are responsible for moving the messages from the source to the destination. They are typically system daemons that run in the background and move e-mail through the system.

    Typically, e-mail system support five basic functions given below.

(i) Composition :

It refers to the process of creating messages and answers.

(ii) Transfers :

it refers to moving messages from the originator to the recipient. This requires, establishing a connection to the destination (or) some intermediate machine, outputting the message and releasing the connection.

(iii) Reporting :

It informs the originator about the status of the message, whether it is delivered, rejected(or) lost.

(iv) Displaying :

These provides the incoming messages to be read by the people. Simple conversions and formatting is performed.

(v) Disposition :

It is the final step and concerns what the recipient does with the message after receiving it.

Other Services of E-mail include:

Mailboxes :

Used for storing incoming E-mail.

Mailing List   = List of e-mail addresses to whom, identical copies of messages need to be sent.

Registered E-mail = It allows the originator to know that his mail has arrived.

High priority E-mail = Secret E-mail etc.

Computer Networks

User Agent :

A user agent is normally a program that accepts a variety of commands for composing, receiving and replying to messages as well as manipulating mail boxes.

Sending E-mail :

To send an e-mail a user must provide the message, the destination address and some other parameters. The message can be produced in any text editor (or) the one built in user agent. The destination address must be in the format that the user agent can deal with i.e., either DNS address (or) X.400 address. Most e-mail systems support mailing list, so that a user can send the same message to a list of people with a single command.

Reading E-mail :

When a user agent is started up, it will look at the user's mailbox for incoming e-mail before

displaying anything on the screen. It then announces the number of messages in the mail box(or)

a one line summary of each one.

In a sophisticated system the user can specify the fields to be displayed by providing the display

format.

Eg:

1. Message numbers
2. Flag etc.

Message format:

Message consist of a primitive envelope, some number of header field, blank line followed by message body. In normal usage, the user agent builds a message and passes it. To the message transfer agent which then uses some of the header fields to construct the actual envelope.

Principal header include:

To :

DNS address of primary recipient.

CC :

DNS address of secondary recipient.
In terms of delivery there is no distinction between primary and secondary (carbon copies).

BCC :

Similar to CC, allows people to send copies to third parties without primary and secondary

knowing it.

From :

Who wrote the message.

Sender :

The one who sent the message.

Received :

Added by each message transfers agent along the way used for finding bugs in routing system.

Return path :

Added by final message transfer agent intended to tell how to get back to the sender etc.

Explain how e-mail works?

SMTP :

Computer Networks

E-mail is delivered by having the source machine establish a TCP connection to destination. Listening to this port is an E-mail daemon that speaks SMTP. This daemon accepts incoming connections and copies messages from them to appropriate mail boxes. If the message cannot be delivered, an error message is given.

After establishing a TCP connection, the sending machine operates as a client and waits for receiving entity to talk first. The server starts by giving its identity and informing whether (or) not it is prepared to receive mail. If it is not, the client releases the connection.

If the server is ready, the client announces whom the E-mail is coming from and whom it is going to. If the recipient exists, the server gives a go-ahead to send the message. Then the client sends the message and the server acknowledges it. When the E-mail has been exchanged then the connection is released.

E-mail Gateways :

SMTP does not work, when both sender and receiver are not on internet. In order to overcome this difficulty E-mail gateways are used.

Here the sender establishes a TCP connection to the gateway and then uses SMTP to transfer the message. The daemon on the gateway then puts the message in a buffer of messages destined for host2. Late TPU (similar to TCP) is established with host2 and the message is transmitted.

Final Delivery :

Post Office Protocol (POP)

Used to fetch e-mail from a remote mail box, has commands for user to logon, logout, fetch and delete messages. If fetches the mail and stores it in local system.

Interactive mail access protocol (IMAP)

This protocol is used by a person having multiple systems (office, residence, car, etc). Here the E-mail server maintains a central repository that can be accessed from any machine. IMAP does not copy E-mail as POP.

DOMAIN NAME SYSTEM

Generally host names, mailboxes and other resources are represented by using ASCII sting such as rgm@vsnl.net.in.But the network itself only understands binary address i.e., the address written in the binary form. So we need some mechanism to convert the ASCII strings to network addresses in binary. It is easy to maintain the host names and their IP addresses in file for a network of few hundred hosts. For a network of thousand hosts it is very difficult.

The Domain Name System, DNS is a distributes data that is used by TCP/IP application to map between host names and IP addresses, and to provide electronic mail routing information. We use the term distributed because no single site on the Internet knows all the information. Each site maintains its own data base information and runs a server program that other systems (clients) across the Internet can query. It is a good example of a TCP/IP client-server application.

Computer Networks

The DNS provides the protocol that allows client and server to communicate with each other. DNS is defined in RFC's 1034 and 1035.

The DNS identifies each host on the internet with a unique name that identifies it as unambiguously as its IP address as follows. To map a name onto an IP address, an application program calls a library procedure called the resolver, passing it the name as a parameter. The 'resolver' sends a UDP packet to a local DNS server, which then looks up the name and returns the IP address to the resolver, which then returns it to the caller. To create names that are unique and at the same time decentralized and easy to change, the TCP/IP designers have chosen a hierarchical system made up of a number of labels separated by dots.

THE DNS NAME SPACE

Internet is divided it several hundred top level domains, where each domain covers many hosts. Each domain is partitioned into sub domains, these are further partitioned and so on. Thus DNS is implemented using a tree in which each node represents one possible label of up to 63 characters.

The root of the tree is a special node with new label as shown in fig. Any comparison of label considers uppercase and lower-case characters the same i.e., Domain names are case insensitive.
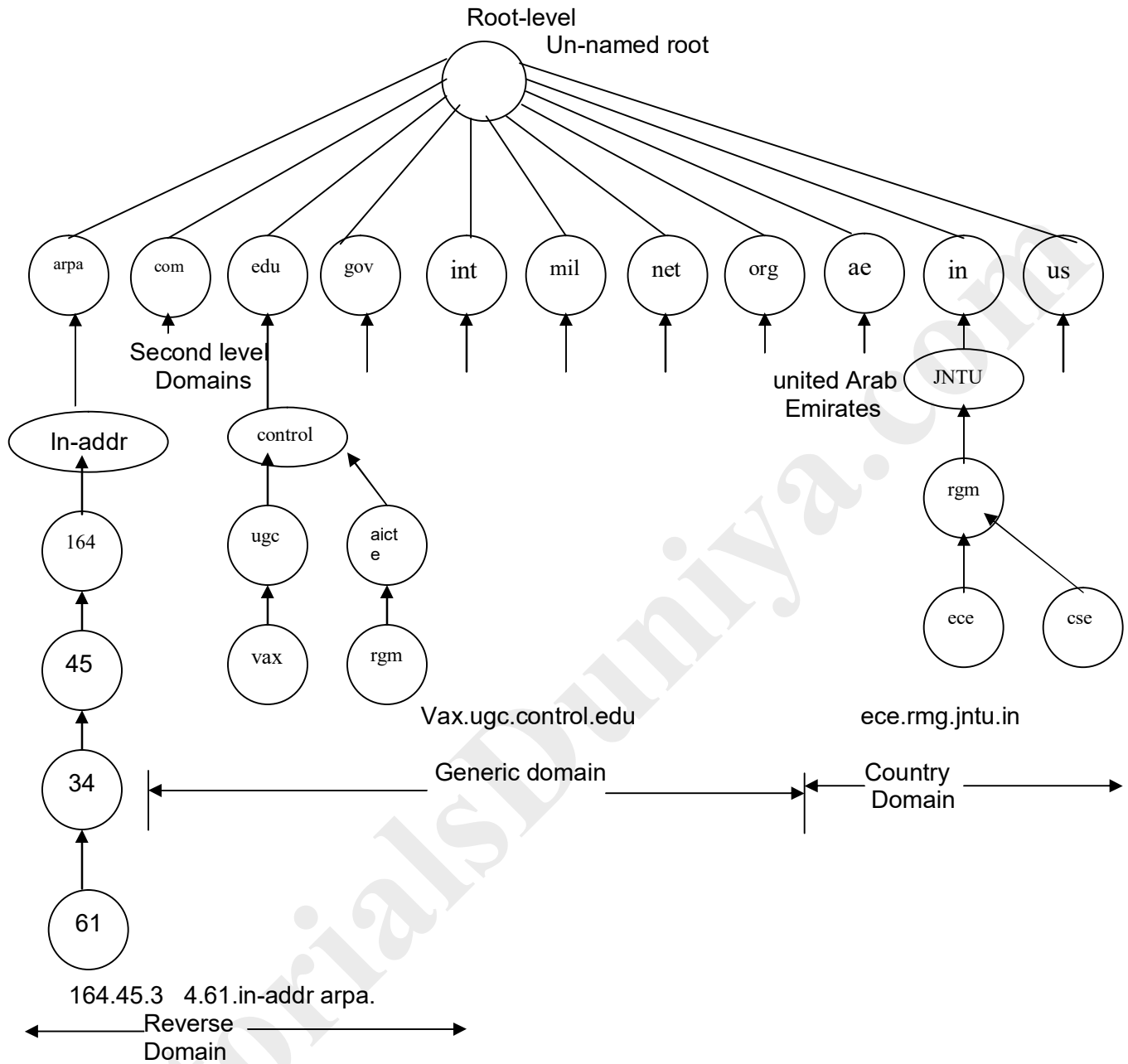
The leaves of the tree represent a company/organization and contain thousands of hosts.

Each domain is named by the path from it to the unnamed root. The components in the name are separated by periods (dots), that is domain name of any node in the tree is the list of labels starting at the node, working up to the root using the period (dot) separate the labels.

The domain names that ends with a period is called an absolute domain name or fully qualified domain name(FQDN).An example is vax.ugc,central.edu.

If domain does not end with a period, it is assumed that the name needs to be completed. How the name is completed on the DNS software being used. If the incomplete names consist of two or more labels, it might be considered to be complete. Otherwise, local addition might be added to the right of the name. The name vax might be completed by adding the local suffix.ugc.central.edu.

The right most label in the name corresponds to the level of the tree closest to the root (lowest), and left-most to the level farthest from the root(highest).The tree is divided into three domains: generic, country and reverse as shown in fig.

Computer Networks

Root-level
Un-named root

arpa   com   edu   gov   int   mil   net   org   ae   in   us

Second level
Domains

In-addr

control

164

ugc

aicte

45

vax

rgm

34

Vax.ugc.control.edu

61

164.45.3 4.61.in-addr arpa.
Reverse
Domain

united Arab
Emirates

JNTU

rgm

ece   cse

ece.rmg.jntu.in

Generic domain   Country
                                   Domain

DOMAIN NAME SYSTEM

Generic Domain: The generic domain is also called the organization domain, divides registered hosts according to their generic behaviour. Generic domain names, read left to the right , start with the most specific information about the host(e.g. the name of the workstation) and become more and more general with each label until they reach the rightmost label, which describes the broadcast affiliation of the normal host i.e., the nature of the organization.

Computer Networks

The first level of the generic domain convention allows seven possible three character labels describing organization type.

1. Com. commercial organization.
2. edu.: educational institution .
3. gov.: government institution.
4. int.: international organization.
5. mil.: military group.
6. net.: Network support center.
7. org. organizations other than listed above.

Each domain name corresponds to a particular IP address. To find the address, the resolution application begins searching with the first level. As a much is found, a pointer leads to the next level and finally to the associated IP address.

Country Domain: The country domain convention follows the same format as generic domain, but uses two character country abbreviation in place of three character organizational abbreviations at the first level shown in table. Second level labels can be organizational or they can be more specific national designations.

Table: SOME DOMAIN NAME SYSTEM COUNTRY CODE

Country Code	Country Name	Country Code	Country Name
AE	Arubeme rates	IN	India
AU	Australia	IT	Italy
BE	Belgium	JP	Japan
CA	Canada	KW	Kuwait
CH	Switzerland	NL	Netherlands
DE	Germany	NO	Norway
DK	Denmark	NZ	Newzeland
ES	Spain	SE	Sweden
FI	Finland	US	United States of America
GR	Greece		

Reverse Domain: If we have the IP address and need the domain name, you can reverse domain the functions of DNS.

The domain can be inserted onto the tree in two ways. For example ugc.control.edu could equally be listed under the country domain as cs.yale.ct.us.

Computer Networks

To create a new domain, permission is required of the domain in which it will be included. For example, rgm group was started under aicte and is known as rgm.aicte.control.edu. It needs permission from which use manages aicte.control.edu. Naming follows organizational boundaries, not physical networks.

RESOURCE RECORDS

Every domain in the DNS tree maintains a set of Resource Records, which are connected to it. For a leaf node i.e., single host, the most common resource record is its IP address. When a resolver gives a name to DNS, it gets back called as resource records associated with that name. The original function of a DNS is to map domain names on to the resource records.
A resource record is a five tuple, in ASCII text they are represented as

Domain-name Time-to live type class value.

- The domain-name tells the domain to which this record belongs. This is the primary search key used to satisfy queries.

- The time-to live field gives information regarding the stability of the record. A large value such as 86-400(number of seconds in one day) indicates that the information is highly stable. The small value such as 60(1 minute) indicates that the information is highly volatile.

- The type of field tells what kind of record it is, some of the type records are listed in table 5.3.

S.No	Type	Meaning	Value
1.	SoA	Start of Authority	Parameter for this zone
2.	A	IP address of a host	32 bit integer
3.	Mx	Mail Exchange	Priority
4.	NS	Name Server	Name of the server for this domain
5.	CNAME	Canonical name	Domain Name
6.	PTR	Pointer	Alias for an IP address
7.	TXT	Text	Uninterpreted ASCII text

1. The SOA record provides name of the primary source of information about (a) name servers zone (b) e-mail address of its administration (c) various flags and (d) various time outs.

2. The record A, holds a 32 bit IP address of the host. If a host connects two or more networks, each case it has one type of a resource record per network connection.

3. The MX record specifies the name of domain prepared to accept e-mail for the specified domain. It allows the host that is not on the internet to receive e-mail from internet sites.

4. NS record specifies Name server.

Computer Networks

5. CNAME record specifies allows the aliases to be created.

6. PTR is a regular DNS data type whose interpretation depends on the context on which it is found.

7. The TXT record allows domains to identify themselves in arbitrary way i.e., it is for user convenience.

- The fourth field in the general structure of resource record is the class. It may be Internet information, used IN and for non-internet information, other codes are used.
- The value field can be number, domain name or an ASCII string.

NAME SERVERS

The Inter network Information center (Inter NIC) manages the top level domain names. The Inter NIC delegates responsibility for assigning names to different organizations. Each organization is responsible for a specific portion of the DNS tree structure. Internet professionals refer to these areas of responsibilities as zones.

Alternatively, the Inter NIC delegates responsibility for assigning names with in a specific zone to specific organizations. Each zone contains some part of the tree and also contains name servers holding the authoritative information about the zone. Each zone contains one primary name server and one or more secondary name servers. Primary name server and one or more secondary name servers. Primary name server gets its information from a file on its disk, the secondary name server and get their information from the primary name server. One or more servers are located outside the zone, for each zone, for reliability. The number of name servers needed in a zone depends on the zone boundaries.

Let us consider an example shown in fig connected with another domain. here a resolver on "ece.rgm.jntu.in" wants to know the IP address of the host "rgm.aicte.control.edu" can be explained in 8 steps.

Step 1: It sends a query to the local name server rgm.jntu.in.This query asks a record of type A and the class IN.
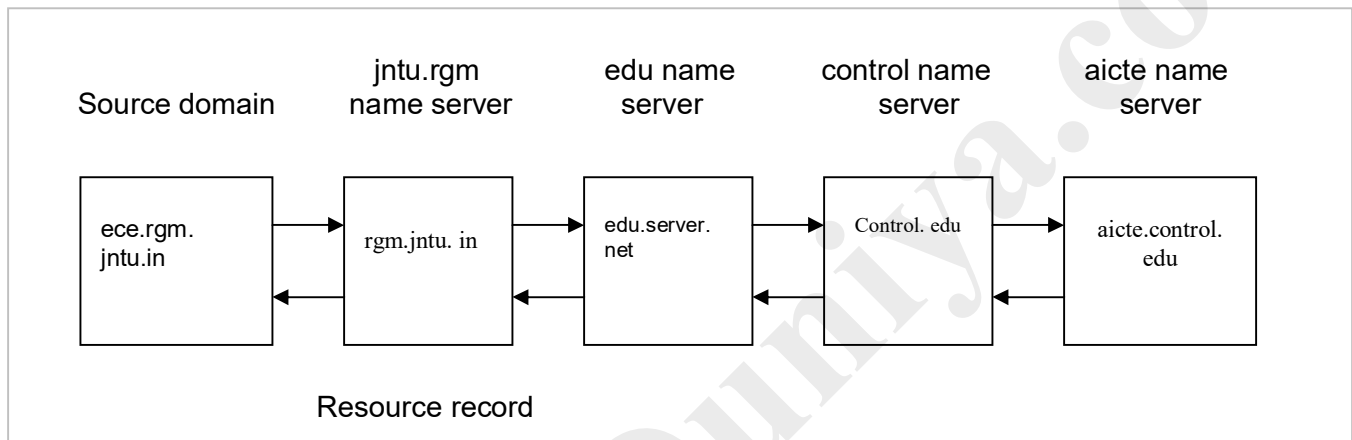
Step 2: If the local name server had no such domain and knows nothing about it, it may ask a few other near by name servers if none of them know, it sends a UDP packet to the server for "edu" given in its database (see fig) edu.server.net.

Step 3: It forwards the request to the name server control.edu.

Computer Networks

Step 4: And in turn this forwards the request aicte.control.edu, which has authoritative resource records.

This is the request from client to a server, the resource record requested will work its way back in step 5 to step 8.Once these records get back to rgm.jntu.in name server, they will be entered into a cache/memory. However this information is not authoritative, since changes made at aicte.control.edu will not be propagated to all the memories in the world. For this reason cache should not live too long, so time-to-live field is used in each resource record. It tells the name server how long to cache records.

Source domain	jntu.rgm name server	edu name server	control name server	aicte name server
ece.rgm. jntu.in	rgm.jntu. in	edu.server. net	Control. edu	aicte.control. edu

Resource record

WORKING OF A RESOLVER FOR A DOMAIN IN 8 STEPS

ELECTRONIC MAIL

Electronic mail or E-mail as it is popularly called, is a system that allows a person or a group to electronically communicate with each other through a netork. Presently people can now receive and send e-mail to:

- nearly any country in the world.
- one of millions of computer users.
- many users at once.
- computer programs.

The first e-map systems consisted of file transfer protocols, with the convention that the first line of each message contained the recipient address. Some of the complaints at that time were

1. Sending a message to a group of people was inconvenient.
2. Messages had no internal structure, making computer processing difficult.
3. The sender never knew if a message arrived or not.

Computer Networks

4. It is difficult to forward the mails.

5. It is not possible to create and send messages containing a mixer of text, drawing facsimile and voice.

After a decade of competition, email systems based on RFC822 are widely used, where all the above problems are solved.

BASIC FUNCTIONS

Email systems support five basic functions, which are: Composition, Transfer, Reporting, Displaying and Disposition.

1. **Composition** is a process for creating the messages and answers. This can be done by text editor, outside the mailer, the system will provide assistance in addressing and numerous header fields attached to each message. For eample:when answering a message, the e mail system can extract the originator's address from the incoming e-mail and automatically insert it into the address space in reply.

2. **Transfer** refers to moving of messages from the source to the recipient. In some cases, connection establishment is needed with the destination, outputting the message and releasing the connection. The e-mail system should do automatically this.

3. **Reporting** is used to indicate the originator what happened to the message i.e., confirmation of the message delivery. Was it delivers successfully? Was it rejected? Was it lost? Did errors occur?

4. **Displaying** It refers to read the incoming e-mail by the person. Sometimes conversion is required or a special viewer must be invoked.

5. **Disposition** It concerns what the recipient does with the message after receiving it. The possibilities are

   (a) Throwing it away before reading

   (b) Throwing it away after reading.

   (c) Saving it and so on. It is also possible to forward them or process them in other ways.

In addition to these basic services, most of e-mail systems provide a large variety of advanced features such as

   (a) It allows to create a mailbox to store incoming e-mail.

   (b) It allows to have a mailing list, to which the e-mail messages have to send.

   (c) Carbon copies, high priority email, secret email, registered email etc.

Computer Networks

THE USER AGENT

The user agent is a program that allows users to read reply to, forward, save and compose messages. User agents for electronic mail are sometimes called mail readers. Some user agents have menu or icon driven interface that requires a mouse, some other requires only 1 character command from keyboard.

Sending e-mail: To send an email message the user must provide

    (a) message

    (b) destination address and

    (c) priority or security levels (options).

- Message can be produced with a free standing text editor, a word processing program or by using a text editor built into the user agents. The format of an e-mail message is similar to that of a conventional letter.

There are two main parts: Header and body.

The header contains out name and address, the name and address of the person it's being sent to, the name and address of the person who is being sent a copy, the date of the message and the subject when we receive an e-mail from someone, the header tells us where it came from, what it is about, how it was sent and when.

The body is the place where we write the contents of what we want to communicate. The message sent should be simple and direct. Body is entirely for human recipient.

- The designation address must be in a format that the user agent can deal with. The basic form of e-mail address is

    User name @host name.subdomain.domain.

The text before the sign @(pronounced "at") specifies the user name of the individual, the text after the @ sign indicates how the computer system can locate that individual's mailboxes.

    For example

    mvs@cs.colorado.edu

Here cs is a sub domain of Colorado is a sub domain of edu.the edu specifies the top-level domain name.

The number of periods (pronounced as dots) varies from e-mail address.

Reading e-mail: On connecting to the net, the first thing a user usually does is check his mail, it's like checking the mailbox when we go home. The display like fig 5.28 appears on the screen.

Computer Networks

Each line refers to one message. In the fig, the mailbox contains 4 (four) messages. The display line contains several fields, which provides user profile.

S.No	Flag	Bytes	Sender	Subject
1.	K	1000	n / p	Got the job
2.	KA	2000	Smer	Request for MP
3.	KF	4000	Vimicro	Repair of controller
4.		1536	hiq	Enquiry of the book

- The first field is the message number.
- The second field is flags, can contain,

    K-means that, message was read previously and kept in mail box.

    A-means the message has already answered and

    F-message has been forwarded to someone else.

- The third field indicates the length of the message in bytes.
- Fourth field tells who sent the message, this field is simple extracted from the message, so this field contains initials, log in name, first name etc.
- The last field is a 'subject field' gives brief summary of the message.

MESSAGE FORMATS

The e-mail message format was defined in RFC 822.There are two types: ASCII e-mail and multimedia extensions.

ASCII e-mails using RFC 822: The e-mail message consists of a primitive envelope, some number of header fields, a blank like and then message body.

Each header field consists of a single line of ASCII text containing the field name, a colon, and a value of RFC.

The list of header fields related to message transport are

- A recipient's address or "To"
- A sender's address or "From"
- A subject.

The email header may additionally contain.

- **A List of "C_d":** This is a list of e-mail or 'carbon copies' addresses to whom a copy of the message is to be delivered. Multiple e-mail addresses in the "C_c" field are separated by a comma.

Computer Networks

- **A List of "B$_c$":** This is same as "C$_c$" except that this is a carbon copy. The list of recipients is not visible to the person who receives this message.
- **Attached:** This is a convenient method to share both data and programs. These files may be attached or enclosed with an e-mail message.
- **Signature:** It contains sender's full name and address or whatever information the sender wishes to send.

Instead of creating a message from the scratch, we may choose to reply or forward the messages.

- **Replying:** When we reply a message, the sender's address is automatically put in the "To" header and subject of the original message is reduced proceeded by Re, for the reply.
- **Forwarding:** When we forward a message, the subject of the original message is reused, with prefix "FW".We must specify the e-mail address of the recipient of the forward message.
- **Redirecting:** Some e-mail programs allow to redirect messages. It is similar to forwarding a message, except that the message retains the original sender in the form header and adds a notation that the message comes through you.

Multipurpose Internet Mail Extensions(MIME):

This is the solution defined in 1341 and updated in 1521 for the following problems.

1. Messages in languages with accents.
2. Messages in non Latin alphabets.
3. Messages in languages with out alphabets.
4. Messages not containing text at all.

The basic idea of MIME is to continue the use of RFC 822 format, but to add structure to the message body defined encoding rules for non ASCII formats. The MIME messages can be sent using the existing mail programs, and protocols.
The MIME defines five new message header

- **MIME-Version:** It tells the use agent receiving the message that it is dealing with a MIME message, and which version of MIME it uses.
- **Content-Description:** It tells what is there in the message, this header helps the recipient whether it is worth decoding and reading the message.

Computer Networks

- **Content-Transfer Encoding:** It tells how the body is wrapped for transmission through a network that may object to most characters other than letters, numbers and punctuation marks.

- **Content-Type:** It specifies the nature of the message body. Seven types are defined in RFC 1521, each of which has one or more sub types. The type and sub type are separated by a slash. The sub type must be given explicitly in the header, no defaults are provided. Table 5.4 shows the list of types and sub types.

TYPE AND SUB TYPE FIELDS DEFINED IN RFC 1521

S.No	Type	Sub Type	Meaning
1.	Text	Plain HTML Rich text	Unformated text Hyper text mark up language Allows a simple mark up language to the included in the text (standardized general mark up language (SGML)
2.	Image	GIF JPEG PNG	To transmit still pictures in GIF format To transmit still pictures in JPEG format To transmit still pictures in portable network graphics
3.	Audio	au Basic aiff	Sun micro systems sound Audiable sound Apple sound
4.	Video	sgi.movie MPEG avi	Silicon graphics movie Visual information, the video format is moving picture experts group MPEG Microsoft audio video interleaved
5.	Application	Octet stream Post Script tex	It is a sequence of uninterrupted bytes Which refers the postscript language produced by Adobe systems and widely used for describing printed pages. TEX document.
6.	Message	RFC822 Partial External	A MIME RFC-822 message (ASCII characters message) Break and encapsulated message up into pieces and send them separately. Used for very long message (i.e., video films)
7.	Multiport	Mixed Alternative Parallel Digest	Each part to be different with no additional structure imposed Each part must contain the same message but expressed in a different medium or encoding. All parts must be viewed simultaneously Many messages are packed together into composite message.

Computer Networks

MESSAGE TRANSFER

The message Transfer system, MTS is concerned with relaying messages from originator to the recipient.The simplest way to do this is to establish a transport connection from source machine to the destination machine and just transfer the message.

Mail servers are from the core of the e-mail infrastructure.Each recipient has a mail box, located in one of the mail servers.A typical message starts its journey in the sender's user agent, travels to the sender's main server, and then travels to the recipient mail server where it is deposited in the recipient mail box.

A mail server needs to be running all the time, waiting for e-mail messages and routing them approximately.If a mail server crashes or down for an extended period(3-4 days), e-mail can be lost.There may be a limitation on the size of mail box.Generally once this limit is reached, new incoming messages are refused until you free up space by deleting some messages.

SIMPLE MAIL TRANSFER PROTOCOL-SMTP

The simple mail transfer protocol (SMTP) is the principal application layer protocol for internet e-mail. It is simple ASCII protocol. It uses the reliable data transfer service of TCP to transfer mail from the sender's mail server to the recipient's mail server. In most application protocols SMTP has two sides: a client side, which executes on the sender's mail server and a server side-which executes on the recipient mail server. When a mail server sends a mail (to other mail server), it acts as a client SMTP.When a mail server receives a mail (from other mail server), it acts as an SMTP server.

The SMTP defined in RF821, is at the heart of Internet e-mail.SMTP is much older than HTTP.To illustrate the basic operation of SMTP, let's walkthrough a common scenario. Suppose Ramu wants to send Raju a simple ASCII message.

- Ramu invokes his user agent for e-mail, provides Raju's e-mail address(example Raju@some school.edu) composes a message, and instructs the user agent to send the message.
- Ramu's user agent sends the message to his mail server, where it is placed in a message queue.
- The client side of SMTP, running on Ramu's mail server, sees the message in the message queue.It opens a TCP connection to a SMTP running Raju's mail server.
- After some initial SMTP hand shaking, the SMTP client sends Ramu's message into the TCP connection.
- At Raju's mail server host, the server side of SMTP recives the message.Raju's mail server then places the message in Raju's mail box.
- Raju invokes his user agent to read the message at his convenience.
  The scenario is summarized in fig.5.29

Computer Networks

SMTP

Ramu's mail server

Internal
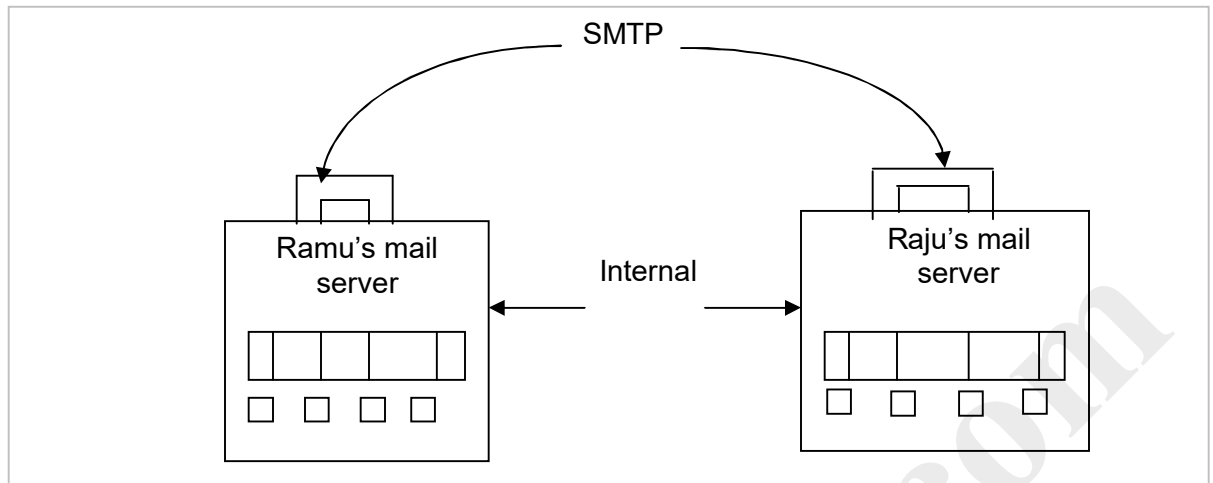
Raju's mail server

RAMU'S MAIL SERVER TRANSFERS RAMU'S MESSAGE TO RAJU'S MAIL SERVER

Let us now take closer look at how SMTP transfers a message from a sending mail server to a receiving mail server.

We will see that the SMTP protocol has many similarities with protocols that are used for face-to-face human interaction.

- The client SMTP has TCP to establish a connection on port 25 to server SMTP.If server is down, the clients tries again later. Once the connection is established, the server and client perform some application layer handshaking. During this SMTP handshaking phase, the SMTP client indicates the e-mail address of the sender and the e-mail address of the recipient. Once the SMTP client and server have introduced themselves to each other, the client sends the message, SMTP can count on the reliable data transfer service of TCP to get the message to the server without errors. The client then repeats this process over the same TCP connection if it has other message to send to the server; otherwise it instructs TCP to close the connection.

Even though the SMTP protocol is well defined, a few problems can still arise. These are.

1. **Related to the Message Length :** Some older implementations cannot handle messages exceeding 64kB.

2. **Related to Time Outs :** If the client and server have different time-outs, one of them may give up while the other is still busy, unexpectedly terminating the connection.

3. Infinite mail storms can be triggered .

To get around some of these problems, extended SMTP (ESMTP) has been defined in RFC1425.

E-mail Gateways: E-mail using SMTP works best when both the sender and receiver on the internet and can support TCP connections between sender and receiver.However many

Computer Networks

machines that are not on the internet)because of security problem) still want to send and recive e-mail from internet sites.

Another problem occurs when the sender speaks only RFC822 and the receiver speaks only X.400 or some proprietary vendor specific mail protocol.

Both these problems can be solved using application layer e-mail gateways fig.5.30 shows the gateway.
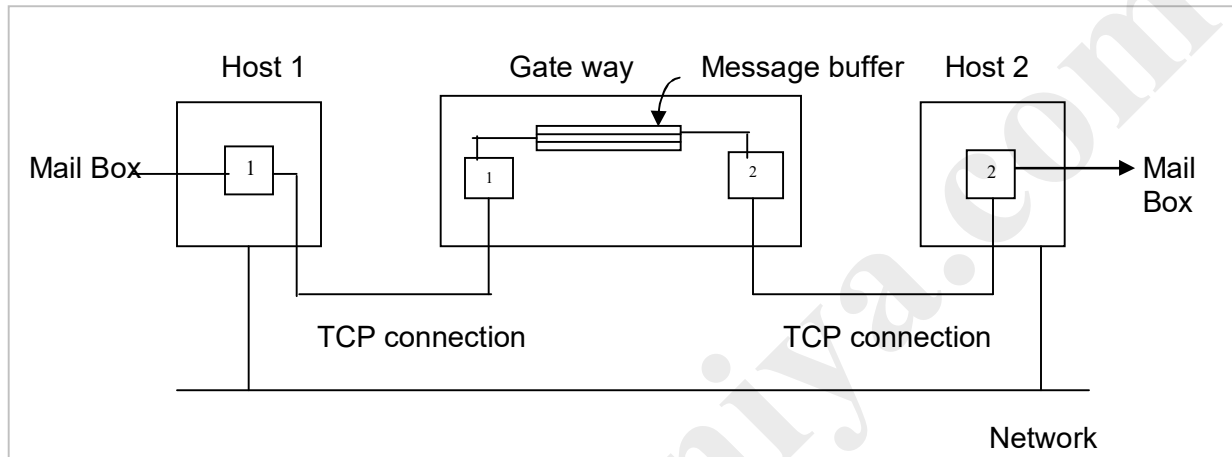
- Here Host1 speaks only TCP/IP and RFC822, where as host 2 speaks only OSITP$_4$ ans X.400.

   They can exchange e-mail using an e-mail gateway.

Procedure:

1. Host 1 establishes a TCP connection to gateway and then use SMTP to transfer message there.
2. The gateway then puts the message in a buffer of messages destened to host 2.
3. A TP$_4$ connection is established between host 2 an the gateway.
4. The message is transferred using OSI equivalent of SMTA.

The problems here are

   (a) The Internet address and X.400 address are totally different. Need of elaborating mapping mechanism between them.
   (b) Envelope and header fields are present in one system and are not present in the other.

MAIL ACCESS PROTOCOL

Till now we have assumed that an users work on machines that are capable of sending and receiving e-mail. Sometimes this situation is false. For example in an organization, users work on desktop PCs that are no in the internet and are capable of sending and receiving e-mail from outside. Instead the organization has one or more e-mail servers that can send and receive e-

Computer Networks

mail. To sned and receive e-mails, a PC must talk to an e-mail server using some kind of delivery protocol.

There are currently two popular mail access protocols:POP_3(Post office Protocol version3) and 1 MAP (internet mail access protocl)

POP_3 : POP_3 defined in RFC 1939, it is an extremely simple amil access protocol.POP_3 begins when the user agents (clients) opens a TCP connection to the mail server (the server) on port 100.With the TCP with TCP connection established, POP_3 progress through three phases.

1. **Authorization:** The user agent sends a user name and a password to authenticate the user downloading the mail.

2. **Transaction:** The user agent receives messages. In this phase the user agent can also mark messages for deletion, remove deletion marks, and obtain mail statistics.

3. **Update:** During the third phase, update occurs after the client has issued the quit command, ending the POP_3 session. This time the mail server deletes the messages that were marked for deletion.

IMAP: The Internet Mail Access Protocol (IMAP), is defined in RFC 2060.It has many features than POP_3 , but it is also significantly maore complex. It was designed to help the user whi uses multiple computers, perhaps a workstation in the office, a PC at a home and laptop on the road.The basic idea behind IMAP is for the e-mail server to maintain a central reposition that can be accessed from any machine.Thus unlike POP_3 , IMAP does not copy email to the user's personal machine because the user may have several.

The IMAP has many features.

a) It has commands that permit a user agents to obtain components of messages. This feature is useful when there is a low bandwidth connection between the user agent and mail server.

b) An IMAP session consists of a client command, server data and a server completion result response.

The IMAP server has four states.

1. **Non Authenticated State:** Initial state whenthe connection begins, the user must supply a user name and password before most commands will be permitted.

2. **Authenticated State:** The user must select a folder before sending commands that affect messages.

3. **Selected State:** The user can issue commands that affect messages.

4. **Log Out State:** Here the session is terminated.

✳ ✳ ✳ ✳ ✳

Computer Networks

REVIEW QUESTIONS

1.What is a secure communication and what are its features?

2.What is the need of cryptography?

3.Define the following terms

  a. plain text b.cipher text c.encryption   d.decrytion e.crypt analysis f.cryptology

4.With the help of suitable examples, explain transposition cipher and substitutional cipher.

5.Draw the block diagram of cryptography. Explain it.

6.Write about the services provided by the application layer.

6. Explain DES algorithm.

7.Explain the public key cryptography. Explain the MIT algorithm for public key encryption.

8.Distinguish between private and public key.

9. What is the diffrence between authentication protocol and digital signature?Give an example

for each.

10. What is the purpose of DNS, explain?

11. explain e-mail system

12.What are the different types of messages formats used in e-mail?

13.Write short notes on world wide web.
14.Write short notes on multimedia.

16.Write short notes on network security and privacy.

17.Using RSA algorithm with A = 1, B = 2 , ………,Z = 26

    taking a.) p =5,q =11 and d =27,find 'e' and encrypt 'ECE'

Computer Networks

Quiz Questions

1. What are the properties of secure communication?

2. An intruder who can listen to and record the content and data messages on the channel is called -----------

3. An intruder who can remove message from the channel and/or add message into the channel is called -----------

4. The key which is available to every one is called --------------

5. The message to be encrypted is known as ----------------

6. The output of encryption process is known as --------------

7. In a------- each letter or group of letters is replaced by another letter or group of letters to disguise it.

8. In ---------- type of cryptography, the messages do not disguise.

* * * * *

Computer Networks